17.12.2025

# Gemeinsamer Schlussbericht

Projektlaufzeit: 01.01.2022 – 30.06.2025

Projektkoordinator: Sebastian Völl, MAN Truck & Bus SE

**Förderkennzeichen: 19A21048 A-L**

## Beteiligte Partner

BTC Embedded Systems AG
Die Autobahn GmbH des Bundes
Fernride GmbH
Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC
Knorr-Bremse Systeme für Nutzfahrzeuge GmbH
LEONI Bordnetz-Systeme GmbH
MAN Truck & Bus SE
Robert Bosch Automotive Steering GmbH
Technische Universität Braunschweig
Technische Universität München
TÜV SÜD Auto Service GmbH
WIVW GmbH

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

**Autoren:**

Anderle, Dominik – MAN Truck & Bus SE

Lippert, Lars – MAN Truck & Bus SE

Dr. Schechner, Korbinian – MAN Truck & Bus SE

Schenkel, Torben – Die Autobahn GmbH des Bundes

Stollfuß, Lavinia – MAN Truck & Bus SE

Taye, Nebiyat – MAN Truck & Bus SE

Dr. Teige, Tino – BTC Embedded Systems AG

Völl, Sebastian – MAN Truck & Bus SE

Dr. Voll, Ulrich – MAN Truck & Bus SE

Wagner, Patrick – Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC)

Wulf, Leonie – MAN Truck & Bus SE

# Inhaltsverzeichnis

# Tabellenverzeichnis



# Abbildungsverzeichnis

# Alphabetisch sortierte Abkürzungen und Bedeutungen

| Abkürzung | Bedeutung |
|---|---|
| ABE | Allgemeine Betriebserlaubnis |
| AD | Automated Driving (automatisiertes Fahren) |
| ADAS | Fahrerassistenzsysteme (Advanced Driver Assistance Systems) |
| ADS | Automatisiertes Fahrsystem (Automated Driving System) |
| AFGBV | Autonome-Fahrzeuge-Genehmigungs- und Betriebsverordnung |
| AI | Artificial Intelligence (Künstliche Intelligenz) |
| AP | Arbeitspaket |
| API | Application Programming Interface |
| ARB | Advanced Redundant Brake (redundantes Bremssystem) / Autonomous Redundant Brake |
| ASC | Absicherungskonzept |
| ASIL | Automotive Safety Integrity Level |
| AWS | Amazon Web Services |
| BEA | Betriebsbereichs- und Ereignismanagement auf Autobahnen |
| BDSG | Bundesdatenschutzgesetz |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BTC | BTC Embedded Systems AG |
| CAN | Controller Area Network (Fahrzeug-Bussystem) |
| CI/CD | Continuous Integration / Continuous Deployment |
| C-ITS | Cooperative Intelligent Transport Systems (kooperative intelligente Verkehrssysteme) |
| CNN | Convolutional Neural Network |
| CVM | Central Vehicle Module (zentrales Fahrzeugsteuergerät) / Zentralsteuergerät – Central Vehicle Management |
| CTA | Cause-tree analysis |
| DATP | Driver-Assistive Truck Platooning |
| DDT | Dynamic Driving Task (dynamische Fahraufgabe) |
| DENM | Decentralized Environmental Notification Message |
| DHW | Distance Headway / Distance Head Way |
| DLR | Deutsches Zentrum für Luft- und Raumfahrt |

| Abkürzung | Bedeutung |
|---|---|
| DoF | Degree of Freedom |
| DSGVO | Datenschutz-Grundverordnung |
| ECU | Electronic Control Unit (elektronisches Steuergerät) / Steuergerät (Electronic Control Unit) |
| EG | Europäische Gemeinschaft |
| ePDB | Intelligenter Leistungsverteiler |
| FCEV | Fuel Cell Electric Vehicle |
| FoV | Field of View |
| FTA | Fault-tree analysis |
| FuSi | Funktionale Sicherheit |
| GNSS | Global Navigation Satellite System / Globales Navigationssatellitensystem |
| GSN | Goal Structuring Notation / Goal-Structuring-Notation |
| HAD | Hochautomatisiertes Fahren / Highly Automated Driving |
| HIL | Hardware-in-the-Loop / Hardware in the Loop |
| HMI | Human-Machine Interface |
| IaC | Infrastructure as Code |
| ICP | Iterative Closest Point |
| IEC | International Electrotechnical Commission |
| IMU | Inertial Measurement Unit |
| ISO | International Organization for Standardization |
| KBA | Kraftfahrt-Bundesamt |
| KPI | Key-Performance-Indicator |
| L2 | Automatisierungslevel 2 / Level 2 (SAE J3016) |
| L4 | Automatisierungslevel 4 / Level 4 (SAE J3016) |
| LiDAR | Light Detection and Ranging |
| LKW | Lastkraftwagen |
| MAN | MAN Truck & Bus SE |
| MDM | Messdatenmanagement |
| ML | Machine Learning |
| MoRA | Modular Risk Assessment |
| MPC | Model Predictive Control |
| MRC | Minimum Risk Condition / Minimal Risk Condition |
| MRM | Minimum Risk Manoeuvre / Minimal Risk Maneuver |
| MS | Meilenstein |
| mAP | mean average precision |
| OBU | On-Board Unit |

| Abkürzung | Bedeutung |
|---|---|
| ODD | Operational Design Domain |
| OT | Operational Technology |
| PETs | Privacy Enhancing Technologies |
| PKW | Personenkraftwagen |
| PMT | Projektmanagementteammeeting |
| RADAR | Radio Detection and Ranging |
| RCP | Rapid-Control Prototyping |
| RGB | Rot-Grün-Blau |
| RL | Reinforcement Learning |
| RM | Risk Management |
| RMSE | Root Mean Square Error / Root-Mean-Square-Error |
| RWW | Road Works Warning |
| S3 | Simple Storage Service |
| SAE | Society of Automotive Engineers |
| SAST | Static Application Security Testing |
| SbB | Steer-by-Brake |
| SCS | Supply Chain Services |
| SMC | Systems, Man, and Cybernetics |
| SNMPC | Stochastic Nonlinear Model Predictive Control |
| SOTIF | Safety of the Intended Functionality / Safety Of The Intended Functionality (ISO 21448) |
| SPI | Safety-Performance-Indicator |
| SSD | Solid State Drive |
| STPA | Systems Theoretic Process Analysis |
| StVG | Straßenverkehrsgesetz |
| StVO | Straßenverkehrsordnung |
| StVZO | Straßenverkehrs-Zulassungs-Ordnung |
| SUT | System Under Test |
| TARA | Threat Analysis and Risk Assessment |
| THW | Time Headway / Time Head Way |
| TRL | Technology Readyness Level |
| TSV | Traffic Simulation Vehicle |
| TTC | Time to Collision |
| TUM | Technische Universität München |
| TÜV | Technischer Überwachungsverein |
| UN R.155 | UN Regulation No. 155 |
| V2V | Vehicle-to-Vehicle |
| V2X | Vehicle-to-Everything |
| VDE | Verband der Elektrotechnik Elektronik Informationstechnik e. V. |
| VDI | Verein Deutscher Ingenieure e.V. |
| VHB | Vorhabenbeschreibung |
| VV | Verifikation und Validierung |
| WD | Weakness Detection |

| Abkürzung | Bedeutung |
|---|---|
| WIVW | Würzburger Institut für Verkehrswissenschaften |
| WVTA | Whole Vehicle Type Approval |
| XBR | eXternal Brake Requests |

Hinweis:

Ausschließlich zum Zweck der besseren Lesbarkeit wird auf eine geschlechterspezifische Schreibweise sowie auf eine Mehrfachbezeichnung verzichtet. Alle Personenbezeichnungen sollen dennoch als geschlechtsneutral angesehen werden.

# 1 Einleitung und Ausgangssituation

*Projektleitung: Sebastian Völl. MAN Truck & Bus SE*

Lkw transportieren weltweit die meisten Güter, in Europa beträgt ihr Anteil am Güterverkehr etwa 70 Prozent. Gleichzeitig stehen die Transport- und Logistikbranche wie auch die Nutzfahrzeughersteller unter Druck: Trends wie autonom[1] fahrende Lkw, Elektroantriebe, Digitalisierung, zunehmender Mangel an Fahrern oder schärfere Abgasnormen sorgen für einen massiven Wandel, auf den sich die Unternehmen frühzeitig vorbereiten müssen

Zahlreiche Statistiken und Studienergebnisse untermauern die schwierigen Rahmenbedingungen für die Logistik:

- In Deutschland verursachen Staus Kosten in Höhe von 33 Mrd. Euro (INRIX/2014)
- 90 % der Unfälle resultieren aus menschlichem Versagen (DeStatis 2019)
- 44,3 % der Fernfahrer würden ihren Beruf nicht wieder wählen (ZF-Zukunftsstudie Fernfahrer 2012)
- 94 % Prozent der Unternehmen haben aktuell mit Fahrermangel zu kämpfen („Top 100 der Logistik 2018/2019“, Fraunhofer Arbeitsgruppe für Supply Chain Services (SCS))

Die Transport- und Logistikbranche steht unter enormem Druck, sich frühzeitig auf Trends wie autonomes Fahren, Elektroantriebe, Digitalisierung und Fahrermangel vorzubereiten. Autonome Lkw sind die Antwort auf viele großen Herausforderungen, denen sich die moderne Lkw-Branche stellen muss: Verlängerung der Betriebszeiten von Lkw, Fahrerproduktivität, Fahrermangel, Sicherheit und Umweltfreundlichkeit. Bei der Betrachtung von drei verschiedenen Anwendungen (Fernverkehr, Regionalverkehr auf Straßen mit hohem Verkehrsaufkommen und Regionalverkehr auf Straßen mit geringem Verkehrsaufkommen) kam Roland Berger (Zukunftsstudie Lkw / Roland Berger 2018) zu dem Ergebnis, dass automatisierte Systeme der Stufen 1 bis 3 die durchschnittlichen Gesamtkosten pro Meile nicht verbessern. Signifikante Verbesserungen der Gesamtbetriebskosten treten erst in der Automatisierungsstufe 4 auf, in der die Fahrerkosten sinken.

Das Projekt ATLAS-L4, das den automatisierten Transport zwischen Logistikzentren auf Schnellstraßen im Level 4 untersucht, zielt darauf ab, den autonomen Warentransport auf der Straße zu ermöglichen und somit die Logistik 4.0 voranzutreiben. Durch die Erweiterung der technischen Potenziale soll der autonome Transport auf Autobahnen realisiert werden. Dabei müssen Sensorik, Perzeption, Planung und Regelung mit den Herausforderungen des Mischverkehrs, hohen Geschwindigkeiten und geringen Merkmalstiefen umgehen. ATLAS-L4 setzt auf neue Ansätze und Konzepte wie die inkrementelle szenarienbasierte Validierung und die Überarbeitung aller Funktionsmodule im Automatisierungs-Stack. Eine sichere Fahrzeugarchitektur, die Fehler erkennt und kompensiert, sowie die Entwicklung eines Control Centers für die technische Aufsicht des automatisierten Lkw-Betriebs sind zentrale Bestandteile des Projekts.

[1] In diesem Dokument ist sowohl von autonomen als auch automatisiertem Fahren die Rede. Mit beidem ist das Automatisierungslevel 4 nach SAE-Standard J3016 gemeint, welches in dem Standard als „High Driving Automation“ bezeichnet wird.

Das Projekt ATLAS-L4 hat zum Ziel, die notwendige Technologie für das automatisierte Fahren im Automatisierungslevel 4 auf Autobahnen zu spezifizieren. Dabei müssen noch zahlreiche Herausforderungen bewältigt werden, wie die Anpassung der Architektur und Software, um sicherzustellen, dass fahrerlose Lkw sicher auf Autobahnen unterwegs sein können. Die Bereitstellung neuer rechtlicher Rahmenbedingungen durch den Gesetzentwurf der Bundesregierung zum autonomen Fahren ermöglicht in naher Zukunft die Zulassung automatisierter Fahrzeuge unter definierten Rahmenbedingungen. Technische Hürden wie die Fahrzeugüberwachung und die Systemdegradation müssen jedoch noch gelöst werden. Eine wissenschaftliche Betrachtung der Themen Sicherheit und simulationsgestützte Validierung soll gangbare Wege für einen leistbaren Homologationsnachweis aufzeigen und experimentell nachweisen.

Mit der Bereitstellung neuer rechtlicher Rahmenbedingungen in Form des Gesetzes zum autonomen Fahren von 2021 der Bundesregierung ist es bereits heute möglich, für autonome Fahrzeuge unter definierten Rahmenbedingungen eine Zulassung für den Straßenverkehr zu erlangen. Dies ebnet den Weg für autonome Transporte. Gleichwohl sind die mit dem Gesetz einhergehenden technischen Hürden, wie die technische Fahrzeugüberwachung und die definierte Systemdegradation, zu lösen. Diese Hürden sind ebenfalls ein zentrales Thema im Projekt ATLAS-L4. Eine wissenschaftliche Betrachtung der Themen Sicherheit und simulationsgestützte Validierung soll helfen, gangbare Wege hin zu einem leistbaren Homologationsnachweis aufzuzeigen und experimentell nachzuweisen.

# 2 Ziele und methodisches Vorgehen

Bis automatisierte Systeme des SAE Levels 4 eingesetzt werden können, muss noch eine Reihe von großen Herausforderungen bewältigt werden. Zum Beispiel sind Architektur- und Softwareanpassungen erforderlich, um sicherzustellen, dass fahrerlose Lkw sicher auf Autobahnen unterwegs sein können. Das Projekt ATLAS-L4 hatte zum Ziel, die dafür notwendige Technologie für das automatisierte Fahren im Automatisierungslevel 4 auf Autobahnen zu spezifizieren.

Das übergeordnete Ziel des Projekts war die Realisierung autonomen Fahrens von Lkw in realen Autobahnszenarien mit Mischverkehr

Im Vordergrund standen die Entwicklung von Technologien, wie z.B. hochgenaue Lokalisierung des Fahrzeugs, Trajektorienplanung und präzise Umsetzung des Bewegungsvektors für den Einsatz auf Autobahnen, sowie deren Umsetzung auf einer L4-tauglichen Fahrzeugarchitektur. Flankiert wurden diese Aufgaben durch die Betrachtung der einzuhaltenden Rahmenbedingungen, die sich aus dem Gesetz zum autonomen Fahren ergeben, sowie der Umsetzung von Prozessen zur Vorbereitung eines Betriebs im Umfeld von Logistik 4.0.

Die wissenschaftlichen Arbeitsziele des Verbundprojekts ATLAS-L4 erstreckten sich auf einen erfolgreichen Wissenstransfer aus dem Forschungsbereich in die betriebliche Praxis.

In der Entwicklung automatisierter Fahrzeuge lag bisher der Fokus primär auf dem Ersetzen eines Menschen in Bezug auf die Fahraufgabe. Menschliche Fahrer und Fahrerinnen absolvieren beim Führen eines Fahrzeugs im Straßenverkehr jedoch deutlich mehr Aufgaben, wie etwa die Überwachung der Fahrtüchtigkeit des Fahrzeugs sowie das Erkennen von Einflüssen, die diese Fahrtüchtigkeit beeinträchtigen können. Im Projekt ATLAS-L4 wurde daher erstmalig ein ganzheitliches Konzept für ein automatisiertes Straßenfahrzeug mit (technischer) Self-Awareness entwickelt. Ausgewählte Aspekte des Konzepts wurden zudem praktisch umgesetzt und so deren Anwendbarkeit und Nutzen für die Fahrzeugautomatisierung demonstriert

Zur Verifikation entwickelter Sicherheitskonzepte für automatisierte Fahrzeuge (mit einem SAE Level 3+) und zur Validierung ihres sicheren Betriebs sind neue Testansätze erforderlich. Szenarienbasierte Entwicklungs- und Testansätze in Kombination mit einer (zumindest teilweisen) Testfalldurchführung in der Simulation sind mögliche Lösungsansätze. Hierfür sind geeignete Testkonzepte zu entwickeln, die heute nur bedingt existieren. Teile eines solchen Testkonzepts sind beispielsweise Testaktivitäten, Teststrategien und Testentwurfsverfahren. Im Projekt ATLAS-L4 wurde die Erstellung und Umsetzung dieser Testkonzepte wissenschaftlich untersucht und deren Praxistauglichkeit sichergestellt. Zum einen wurde ein Testkonzept für die Gesamtfahrzeugverifikation und Sicherheitsvalidierung eines Level-4-Prototyps (im Level-2-Betrieb mit einem Sicherheitsfahrer) erforscht; zum anderen wurde ein entsprechendes Testkonzept für ein Level-4-Fahrzeug untersucht. Das Testkonzept für den Level-4-Prototyp sollte im Projekt vollumfänglich umgesetzt werden, um eine Basis für die Freigabe des Level-4-Prototyps (im Level-2-Betrieb) für den realen Straßenverkehr zu bieten.

Bezüglich der Security-Umfänge wurde angestrebt, bestehende, wissenschaftlich fundierte Methoden zur Security-Risikoanalyse auf den Vorhabenkontext zu adaptieren, um Security-Anforderungen von Beginn an in die Entwicklung des vollautomatisierten Fahrens von Lkw in realen Autobahnszenarien mit Mischverkehr einzubringen. Mittels einer wissenschaftlichen,

übergreifenden Analyse von Security-Standards sollten Automobilhersteller und -zulieferer eine Übersicht der Security-Anforderungen aus Standards und rechtlichen Rahmenbedingungen für die Bereiche IT/Control Center, Produktion, Fahrzeugentwicklung und Werkstatt erhalten, um Standardkonformität zu erreichen und Bereiche hinsichtlich Security zu vernetzen. Ferner sollte für die langfristige Integration der Security ein prototypisches Werkzeug als bereichsübergreifendes Wissensbasis- und Incident-Management-Tool für den gesamten Produktlebenszyklus entwickelt werden

Aus industrieller Perspektive zielte das Projekt ATLAS-L4 auf die Weiterentwicklung der verschiedenen Komponenten des Level-4-Prototyps ab, wie in Tabelle 1 dargestellt

Tabelle 1 Kerninnovationen im Projekt ATLAS-L4

| **Kerninnovation** | **Beschreibung** |
|---|---|
| Lkw mit Automatisierungsgrad 4 | Lkw mit Level-4-Sicherheitskonzept in Hardware, Architektur und Software; durch im Projekt entwickeltes Validierungsverfahren geprüft |
| Konzept für technische Überwachung automatisierter Fahrzeuge | Aufbau einer technischen Überwachung gemäß den Anforderungen aus dem Gesetz zum automatisierten Fahren |
| Testlösungen und -werkzeuge für das szenarienbasierte Testen | Szenarien-Editor zur Formalisierung von Verkehrssituationen, Szenarienvariation zur Ableitung von konkreten Testfällen, Ausführung der Testfälle in einer Simulationsumgebung |
| Erstellung und Umsetzung Testkonzepte (Level-4-Prototyp mit Sicherheitsfahrer) | Testkonzepte für die Gesamtfahrzeugverifikation und die Sicherheitsvalidierung eines Level-4-Prototyps (mit einem Sicherheitsfahrer) |
| Erstellung und Umsetzung Testkonzepte (Level-4-Fahrzeug) | Testkonzepte für die Gesamtfahrzeugverifikation und die Sicherheitsvalidierung eines Level-4-Fahrzeugs im Hinblick auf eine potentielle Serienentwicklung (welche im Projekt ATLAS-L4 jedoch nicht angestrebt wird) |

## 2.1 Methodisches Vorgehen

Aus den Zielen und dem Zielbild eines autonomen Lkws auf der Autobahn ist unter Zuhilfenahme des V-Modells und unter Berücksichtigung des bereits vorhandenen Vorwissens zur Entwicklung autonomer Lkw die in Abbildung 1 dargestellte Arbeitspaketstruktur entstanden. Für die Fahrzeug- und Komponentenentwicklung wurde von den jeweiligen Industriepartnern jeweils ihre eigene Entwicklungsmethodik angewandt (siehe unten).

AP 1 bis AP 3 beschäftigten sich insbesondere mit der Modellierung, Analyse und Konzeption von Safety, Security und Anforderungen. Hier ist insbesondere die intensive Zusammenarbeit zwischen Industrie, Wissenschaft, SW-Entwicklung und Straßenbetreiber herauszustellen, um die Arbeiten nach neuesten und wissenschaftlich anerkannten Prozessen, Methoden und Vorgehen durchzuführen. AP 4 beschäftigte sich mit Test- und Validierungsmethoden. Auch hier gab es eine starke Zusammenarbeit zwischen Softwareentwicklung, Industrie und Wissenschaft, um neueste Methoden, teils in anderen Förderprojekten erarbeitet, mit in ATLAS-L4 einfließen zu lassen. AP 5 und AP 6 vervollständigten den linken Ast des V-Modells mit Konzeption und Definition sowie Umsetzung einer Software- und Hardware-Architektur für das Automatisierungssystem inklusiver der jeweiligen redundanten Komponenten Bordnetz, Lenkung und Bremssystem. Diese Arbeitspakete waren sehr stark industriegetrieben.

In den Unter-APs von AP 6 haben die jeweiligen Industriepartner für die Komponentenentwicklung jeweils nochmal ihre eigene Entwicklungsmethodik angewandt. AP 7 und AP 8 bildeten den Rahmen für die Integration der Sensorik und für die Implementierung eines Umfeldmodells sowie für die komplette Funktionsentwicklung des Automatisierungssystems. Diese beiden Arbeitspakete waren ebenfalls nahezu komplett in der Hand eines Industriepartners.

Das AP 9 mit der Entwicklung eines Control Centers beinhaltete ebenfalls die Entwicklungsschritte nach V-Modell, da das Control Center eine eigene Anwendung ist, die via Kommunikationslink mit einem autonomen Lkw verbunden ist. Aufgrund der Neuartigkeit eines solchen Control Centers wurde in diesem AP ebenfalls sehr stark zwischen Industrie, Wissenschaft und Straßenbetreiber zusammengearbeitet, um ein grundlegendes Konzept für die Technische Aufsicht sowie für das teleoperierte Fahren zu entwickeln.

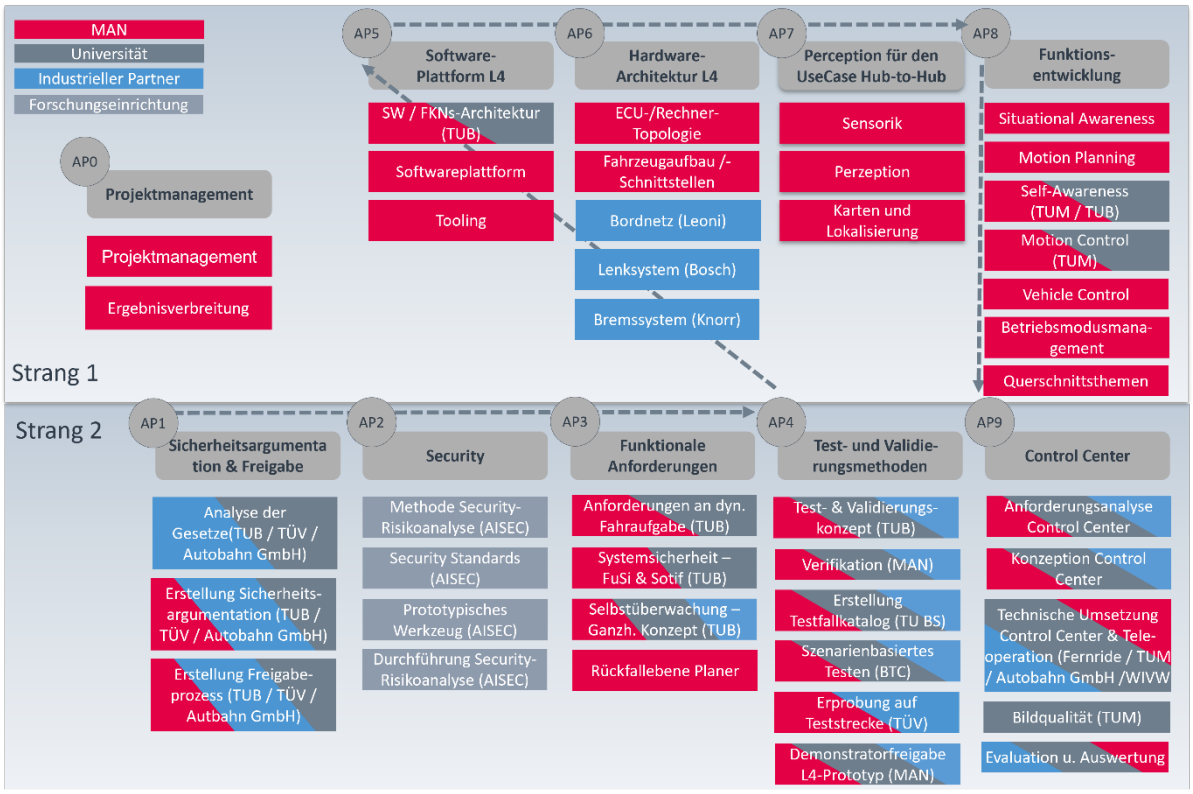



Abbildung 1 Übersicht der Arbeitspakete

Abbildung 2 zeigt die Projekt-Meilensteine. Nahezu alle Arbeitspakete konnten parallel beginnen und liefen auch komplett parallel. Einzig die Implementierung in AP 8 startete etwas später, aber trotzdem noch frühzeitig, als die ersten Konzeptarbeiten vorlagen. Hier konnte mit grundlegender Arbeit an Fahrzeugschnittstellen begonnen werden.

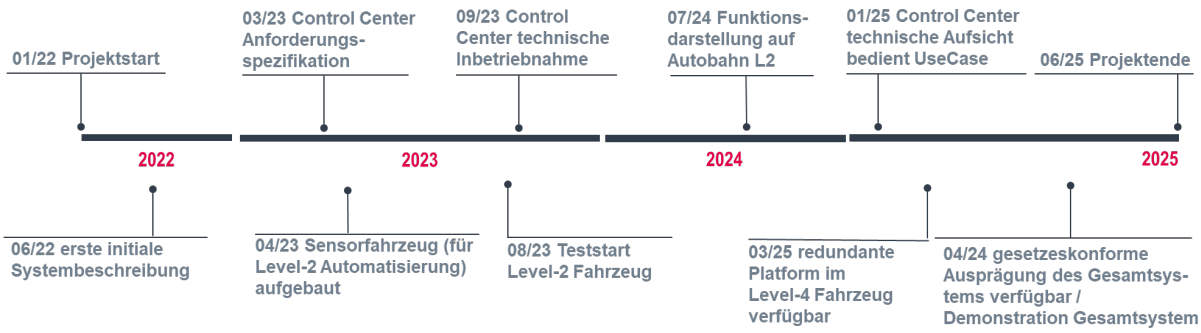



Abbildung 2 Meilensteinplan

Das parallele Arbeiten war auch dem agilen Entwicklungsprozess geschuldet, der für dieses Projekt vom Partner MAN angewendet wurde. Hier wurden u. a. inkrementell einzelne Funktionsteile konzeptioniert, implementiert, getestet und anschließend optimiert. So ergab sich

innerhalb eines Arbeitspakets aber auch zwischen den verschiedenen Arbeitspaketen eine wiederkehrende Entwicklungsschleife (vgl. Abbildung 3).

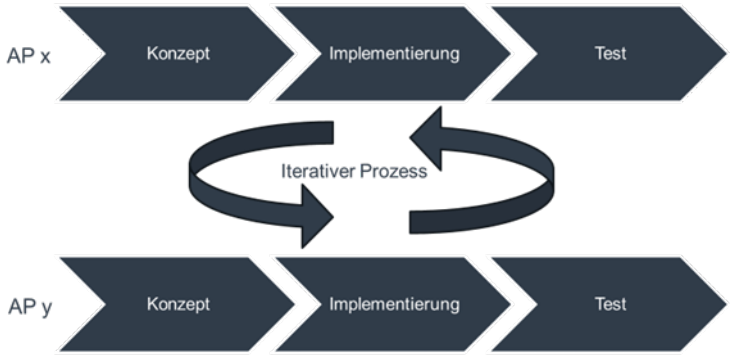



Abbildung 3 Iterativer Entwicklungsprozess zwischen den Arbeitspaketen

Dies stellte sicher, dass sich der Gesamtfunktionalität des Gesamtsystems in kleinen Schritten zielgerichtet angenähert werden konnte, jedoch auch Änderungen möglich waren, wenn Testergebnisse konzeptionelle Anpassungen erforderlich machten.

Zur Koordinierung wurde ca. einmal im Quartal ein sogenanntes Projektmanagementteam-Meeting abgehalten, an dem die jeweiligen Leiter der Arbeitspakete, Gesamtprojektleiter sowie alle Firmenprojektleiter über den aktuellen Stand sowie den Fortschritt in den jeweiligen Arbeitspaketen berichtet hatten. So wurde sichergestellt, dass Wissen zwischen den Arbeitspaketen transferiert wird und Abhängigkeiten identifiziert und entsprechend aufgelöst werden konnten.

## 2.2 Projektübersicht

Nachfolgend befindet sich die Präsentation von der ATLAS-L4-Abschlussveranstaltung (Partner, Projektstruktur, Darstellung der Ergebnisse im Überblick)


## DIE ATLAS-L4 PARTNER

ATLAS-L4

**Laufzeit:** 01.01.2022 bis 30.06.2025
**Projektvolumen:** 59,1 Mio. Euro
**Förderung:** 53 %

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages

**12 Projektpartner aus Industrie – Wissenschaft – Softwareentwicklung – Infrastrukturbetreiber**

MAN · Die Autobahn · BOSCH Invented for life · BTC embedded systems · FERNRIDE DRIVING LOGISTICS AUTOMATION · Fraunhofer AISEC · KNORR-BREMSE · LEONI · Technische Universität Braunschweig · Technische Universität München · TÜV SÜD · WIVW

ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Sebastian Völl, MAN Truck & Bus SE 3

## PROGRAMM

ATLAS-L4

**Vorträge am Vormittag**

| | |
|---|---|
| **Das Projekt im Überblick** | *Sebastian Völl, MAN Truck & Bus SE* |
| **Rechtliche Rahmenbedingungen, Sicherheit und Freigabe, funktionale Anforderungen** | *Susanne Schulz, Autobahn GmbH*<br>*Patrick Wagner, Fraunhofer-Institut AISEC*<br>*Dominik Anderle, Clear Motive GmbH* |
| **Fahrzeugaufbau: Fahrzeugkonzepte, Sensorfahrzeug, Demofahrzeuge** | *Lars Lippert, MAN Truck & Bus SE* |
| **Perzeption** | *Dr. Ulrich Voll, MAN Truck & Bus SE* |
| **Funktionsentwicklung, Tooling, Test und Validierungsmethoden** | *Leonie Wulf, MAN Truck & Bus SE*<br>*Nebiyat Taye, MAN Truck & Bus SE*<br>*Dr. Tino Teige, BTC Embedded Systems AG* |
| **Control Center und Teleoperation** | *Lavinia Stollfuß, MAN Truck & Bus SE* |

ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Sebastian Völl, MAN Truck & Bus SE 6

## ATLAS-L4:
## DAS PROJEKT IM ÜBERBLICK

Sebastian Völl
MAN Truck & Bus SE
ATLAS-L4 Projektkoordinator

## PROJEKTZIEL UND TECHNOLOGIEN

**Projektziel:** Level-4 automatisierter Hub2Hub Transport unter Beachtung der Rahmenbedingungen aus dem Gesetz zum automatisierten Fahren als Enabler für das Ökosystem Logistik 4.0


**Nötige Technologien:**

- Level-4-Konzepte für Safety, Architektur des Automatisierungs-system und ihrer Komponenten inkl. Sensorik
- Security-Betrachtung dieser Konzepte
- Redundante Basiskomponenten Bordnetz, Lenkung und Bremssystem
- Redundanz- und Degradationskonzepte für die Automatisierungsfunktion
- Validierungskonzept für Level-4-Systeme
- Realisierung einer technischen Aufsicht inkl. Teleoperation
- Realisierung des Zulassungsprozess nach AFGBV für Erprobungs- und folgend auch als Betriebsgenehmigung

**Projektziele zum Erleben:**

- LKW im Automatisierungslevel 4 (mit Sicherheitsfahrer) für die Autobahn
- Betrieb des automatisierten LKW unter Nutzung einer Technischen Aufsicht auf der Autobahn
- Fail-Safe Strategien für Basiskomponenten, Funktionen und Gesamtsystem
- Einsatz von Teleoperation bei Erreichen von Systemgrenzen

## VERNETZUNG IM PROJEKT

- Rechtliche Rahmenbedingungen und Freigabe (AP 1)
- Security (AP 2)
- Funktionale Anforderungen (AP 3)

- Perzeption (AP 7)
- Fahrzeugaufbau: Fahrzeugkonzepte Sensorfahrzeug, Demofahrzeuge (AP 6)

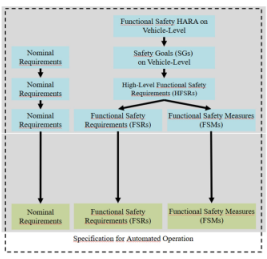
- Funktionsentwicklung (AP 8)
- Tooling (AP 5)
- Test und Validierung (AP 4)

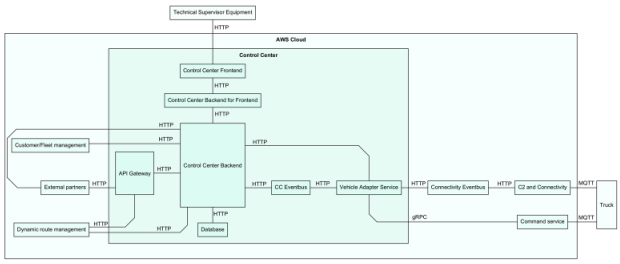
- Control Center und Teleoperation (AP 9)



## PROJEKTERGEBNISSE IM ÜBERLICK

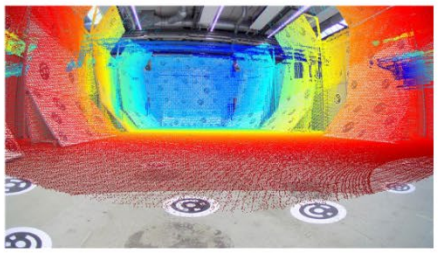
- **Normenanalyse** und konzeptionelle **Level 4 Sicherheitsargumentation**
- Gesetzesanalyse und Software für digitale Betriebsbereichsgenehmigung
- **Erprobungsgenehmigung nach AFGBV** für Demonstrationsfahrzeug erhalten
- **Security-Risikoanalyse und Schutzkonzept zum Control Center** abgeschlossen
- **Risikoanalyse (HARA) für L4-Betrieb** durchgeführt
- **Funktionale Architektur** inkl. Abbildung aller Safety relevanten Aspekten

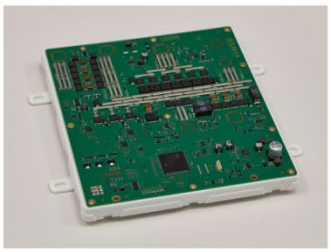



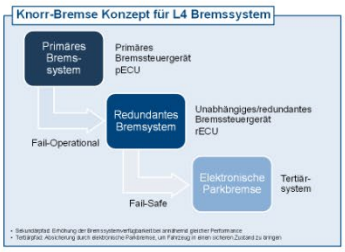



## PROJEKTERGEBNISSE IM ÜBERLICK

- **Bestätigtes Energiebordnetzkonzept**
- **Red. Bremssystem** in B-Musterstand mit Straßenfreigabe
- Hochgenaues **Verfahren zur Offline Kalibrierung** in Kalibrierhalle erstellt.
- **Public Dataset MAN TruckScenes** veröffentlicht
- ARB- und Demonstrationsfahrzeug aufgebaut



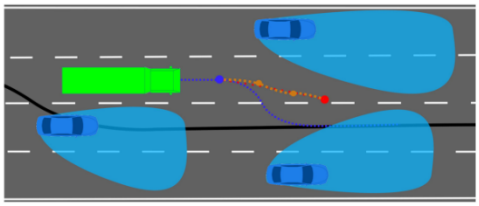


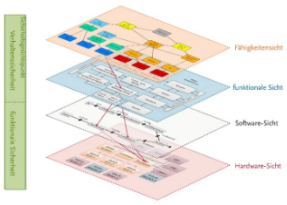



ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Sebastian Völl, MAN Truck & Bus SE 9

## PROJEKTERGEBNISSE IM ÜBERLICK

- **Manöver zur Erreichung eines risikominimalen Zustands** erfolgreich mit der technischen Aufsicht kombiniert
- Implementierung einer Notfalltrajektorienplanung als Rückfallebene für die Bewegungsplanung, Fahrzeugintegration und Integration mit Offboard-Modulen zur Ausführung eines Minimum Risk Maneuvers
- Abbildung der Funktionen in einer funktionalen Schicht
- Aufbau einer durchgängigen Software-Toolchain vom Funktions-Build bis zum Fahrzeug-Deployment
- Prototypische **Toolkette zum szenarienbasierten Testen** des L4-Planers in virtueller Simulationsumgebung
- Umsetzung eines exemplarischen **Vergleichs zwischen Realfahrten auf dem Prüfgelände** und Simulationen zur Validierung

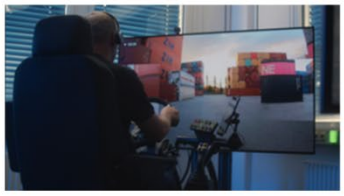


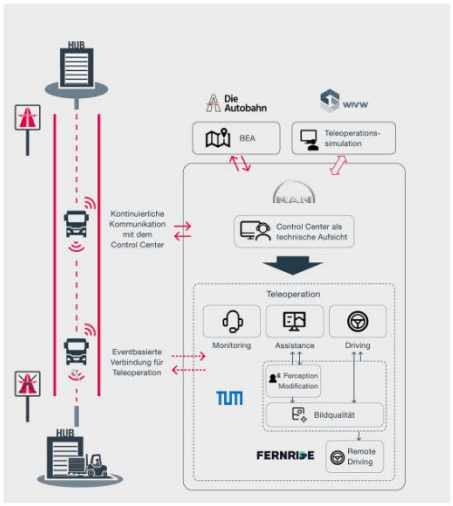



ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Sebastian Völl, MAN Truck & Bus SE 12

## PROJEKTERGEBNISSE IM ÜBERLICK

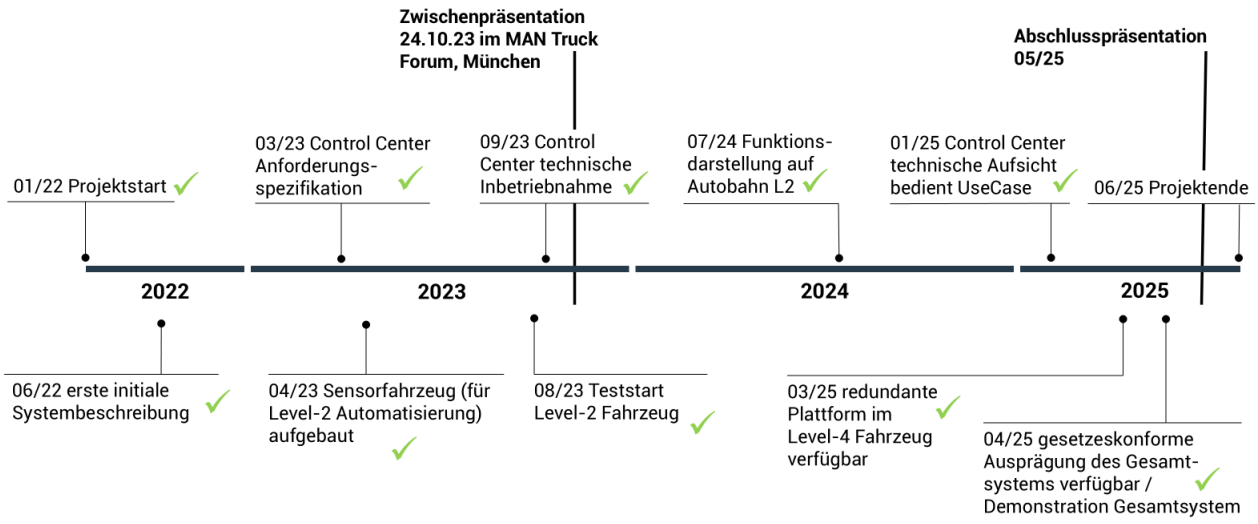
- **Control Center mit technischer Aufsicht** für Live Monitoring Fahrzeug & Mission
- **Teleoperationssimulation** als Werkzeug für Forschung/Entwicklung und Training von Teleoperatoren
- **Teleoperation als Remote-Driving-Konzept für Control Center entwickelt** und in Lkw integriert






ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Sebastian Völl, MAN Truck & Bus SE 13

## MEILENSTEINE IM PROJEKT

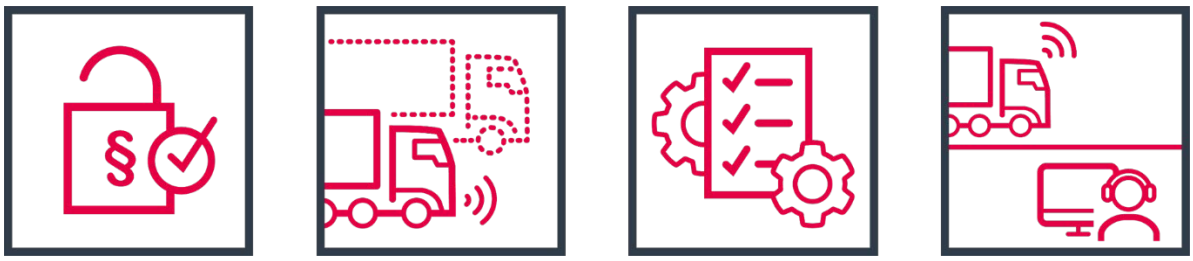



ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Sebastian Völl, MAN Truck & Bus SE 14

# 3 Projektergebnisse nach Arbeitspaketen

Im Folgenden werden die Ergebnisse der neun Arbeitspakete detailliert dargestellt.

- AP 1: Sicherheitsargumentation und Freigabe
- AP 2: Security
- AP 3: Funktionale Anforderungen
- AP 4: Test und Validierungsmethoden
- AP 5: Softwareplattform L4
- AP 6: Hardwarearchitektur L4
- AP 7: Perzeption für den Use Case Hub-to-Hub
- AP 8: Funktionsentwicklung
- AP 9: Control Center und Teleoperation



# AP 1:
# Sicherheitsargumentation und Freigabe

Torben Schenkel, Die Autobahn GmbH des Bundes

## 3.1 AP 1: Sicherheitsargumentation und Freigabe

*Arbeitspaketleitung: Torben Schenkel, Die Autobahn GmbH des Bundes*

Damit Fahrzeuge im öffentlichen Straßenverkehr betrieben werden dürfen, muss einem definierten Freigabeprozess gefolgt werden. Während für konventionelle Fahrzeuge mit menschlichem Fahrer etablierte Freigabeprozesse zum Stand der Technik gehören, sind vergleichbare Prozesse für automatisierte und autonome Straßenfahrzeuge noch nicht etabliert. Mit dem „Gesetz zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren“ vom 12.07.2021 und der „Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung“ (kurz: AFGBV) vom 24.06.2022 hat Deutschland als erstes Land weltweit die gesetzlichen Rahmenbedingungen für den Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion im öffentlichen Straßenraum geschaffen. Es ist dabei vorgeschrieben, dass der Betrieb solcher Fahrzeuge genehmigungspflichtig ist, auf dafür freigegebenen Betriebsbereichen durchgeführt und von einer technischen Aufsicht überwacht werden muss. Das Gesetz unterscheidet zwischen einer zeitlich begrenzten Erprobungsgenehmigung für Testfahrzeuge und einer Regelgenehmigung für Serienfahrzeuge. Das Arbeitspaket 1 beschäftigt sich mit diesen beiden Freigabeprozessen sowie mit der Sicherheitsargumentation, die eine wesentliche Voraussetzung für die Erteilung einer Freigabe darstellt. Im Rahmen einer Sicherheitsargumentation ist nachzuweisen und zu dokumentieren, wieso sich das Fahrzeug im Betrieb sicher verhält. Dabei ist u.a. zu dokumentieren, dass nach geltenden Sicherheitsstandards und Gesetzen entwickelt wurde. Daher wurden im Arbeitspakt 1.1 zunächst die einzuhaltenden Gesetze und Sicherheitsnormen analysiert. Arbeitspaket 1.2 wurde die Sicherheitsargumentation erstellt. Darauf aufbauend wurde Arbeitspaket 1.3 an den Freigabeprozessen gearbeitet und schließlich erfolgreich eine Erprobungsgenehmigung erlangt.

Das Arbeitspaket 1 wurde von der Autobahn GmbH geleitet. Für die Zusammenarbeit und Koordination wurden regelmäßige Online-Treffen durchgeführt und von der Autobahn GmbH moderiert. Neben der Autobahn GmbH arbeiteten MAN, TU Braunschweig und TÜV Süd im AP 1.

### 3.1.1 Analyse der einzuhaltenden Gesetze und Sicherheitsnormen (AP 1.1)

**Normenanalyse**

Im Kontext der Sicherheitsargumentation sind im Projekt verschiedene Fragestellungen untersucht worden. Zunächst wurden die für die Entwicklung automatisierter Fahrzeuge (implizit[2] oder explizit) relevanten normativen Dokumente betrachtet. Abbildung 4 zeigt exemplarisch die differenzierte Auswahl normativer Dokumente im Kontext der Funktionalen Sicherheit.

[2] Implizit relevant meint Normen, deren Berücksichtigung nicht zwangsläufig erfolgen muss, aber Vorteile bringen kann. So handelt es sich dabei etwa um technologieoffene Normen. Diese behandeln nicht das Fahrzeugführungssystem als Entwicklungsgegenstand, präsentieren jedoch teilweise etablierte Konzepte und Prozesse für den Umgang mit sicherheitskritischen Systemen, die auf die Entwicklung eines SAE-Level-4-Fahrzeugs übertragbar sind.


Abbildung 4 Ausschnitt aus der Analyse für domänenspezifische und technologieneutrale normative Dokumente; zugeordnet zur Sicherheitsdisziplin „Funktionale Sicherheit“

Zentrale Ergebnisse der Analyse wurden in einem umfassenden Bericht festgehalten, der unter anderem folgende Aspekte beinhaltet:

- Definition von inhaltlichen Kategorien zur Verortung normativer Dokumente
- Zusammenfassung der Prinzipien, Prozesse und Anforderungen einer Vielzahl an normativen Dokumenten
- Identifikation ausgewählter Defizite, Widersprüche oder Synergien der normativen Dokumente
- Identifikation von unterrepräsentierten Themenkomplexen in der Normenlandschaft (z. B. wertebasierte Entwicklung)

Die zuvor genannten inhaltlichen Kategorien dienen der Beherrschung von Komplexität für die breite und dynamische Normenlandschaft. Die Definition der Verortungskategorien erfolgte vor dem Hintergrund unterschiedlicher Gefährdungsursachen („Sicherheitsdisziplinen“, etwa Verhaltenssicherheit) sowie durchgängigen Aspekten, die mehrere Sicherheitsdisziplinen betreffen, etwa der Terminologie. Die Kategorien sind Abbildung 5 zu entnehmen.


Abbildung 5 Übersicht der definierten Verortungskategorien

Der Stand der Technik ist maßgeblich durch Standardisierungsaktivitäten geprägt. Daher liefert das Vorhandensein einer detaillierten Erklärung, welche normativen Anforderungen zu berücksichtigen oder vernachlässigen sind, einen entscheidenden Beitrag zur Argumentation hinreichender Entwicklungssorgfalt. Dies ist eine entscheidende Grundlage der Erstellung einer Sicherheitsargumentation, die insbesondere im Produkthaftungsfall von zentraler Bedeutung ist.

**Gesetzesanalyse**

Grundlage für die Gesetzesanalyse ist der nationale Rechtsrahmen, der aus dem Gesetz zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren vom 12.07.2021 und der zugehörigen Autonome-Fahrzeuge-Genehmigungs-und-Betriebsverordnung (AFGBV) vom 24.06.2022 besteht. Mit diesem Rechtsrahmen hat Deutschland als erstes Land weltweit die gesetzlichen Rahmenbedingungen für den Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion im öffentlichen Straßenraum geschaffen. Der neue Rechtsrahmen ermöglicht:

- Erprobungsgenehmigung für automatisierte und autonome Testfahrzeuge
- Regelgenehmigung für autonome Serienfahrzeuge
- Nachträglich aktivierbare automatisierte und autonome Fahrfunktionen

Die Erprobungsgenehmigung wird federführend vom Kraftfahrtbundesamt (KBA) erteilt. Wenn Bundesautobahnen oder Bundesstraßen in Bundesverwaltung zum Erprobungsbereich gehören, wird die Autobahn GmbH angehört und hat so die Möglichkeit Hinweise oder Einwände einzubringen.

Die Regelgenehmigung ist ein dreistufiger Prozess:

- Im ersten Schritt prüft das KBA, ob das autonome Fahrzeug die notwendigen technischen Voraussetzungen erfüllt; daraufhin erteilt es die EU-Typgenehmigung oder die Allgemeine Betriebserlaubnis (ABE). Antragsteller ist der Fahrzeughersteller.
- Im zweiten Schritt wird geprüft, ob der beantragte Betriebsbereich für den Betrieb des autonomen Fahrzeugs geeignet ist, bzw. ob das Fahrzeug alle Besonderheiten im Betriebsbereich sicher bewältigen kann. Für den Bereich der Autobahnen ist die Autobahn GmbH die zuständige Behörde, für Bundes-, Land- und Kreisstraßen ist dies die jeweils zuständige Landesbehörde. Antragsteller ist der Fahrzeughalter.
- Im letzten Schritt wird von der Zulassungsstelle die Fahrzeugzulassung erteilt. Antragsteller ist hier ebenfalls der Fahrzeughalter.

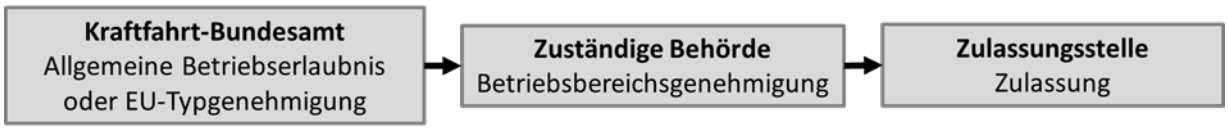



Abbildung 6 Dreistufiger Prozess der Regelgenehmigung

Die Betriebsbereichsgenehmigung für alle Autobahnen in Deutschland ist also eine neue Aufgabe für die Autobahn GmbH. Um zu erarbeiten, welche gesetzlichen Rechte und Pflichten für die Autobahn GmbH bei dieser neuen Aufgabe bestehen, wurde ein Unterauftrag zur Gesetzesanalyse an eine Anwaltskanzlei vergeben. Der Zuschlag fiel im Rahmen des Vergabeprozesses an die Kanzlei GSK Stockmann. Innerhalb eines Jahres wurden von der Kanzlei zahlreiche rechtliche Fragestellungen in Bezug auf das Gesetz zum autonomen Fahren und die Betriebsbereichsgenehmigung bearbeitet. Das Ergebnis ist ein ca. 60-seitiges Gutachten, in dem u. a. folgende Themen adressiert werden:

- Das Hinzuziehen von begutachtenden Stellen für die Betriebsbereichsgenehmigung: Bei welchen Prüfgegenständen eine begutachtende Stelle notwendig ist und was von der zuständigen Behörde selbst geprüft werden kann
- Die Sonderregeln für die Erprobung von autonomen Fahrfunktionen im Straßenbetriebsdienst (§1k StVG „Ausnahmen“)
- Welche gesetzlichen Anforderungen es für eine Digitalisierung der Betriebsbereichsgenehmigung gibt (eGovernment)
- Wie genau die im Gesetz beschriebene Zuverlässigkeitsprüfung für Fahrzeughalter und technische Aufsicht in der Praxis ablaufen kann
- Wie eine digitale Kommunikation zwischen Fahrzeughalter, technischer Aufsicht und zuständiger Behörde ablaufen kann und welche Fristen und Vorgaben dabei eingehalten werden müssen
- Welche gesetzlichen Möglichkeiten die zuständigen Behörden für das Beschränken von autonomem Fahren in ihren Betriebsbereichen haben, z. B. bei Arbeitsstellen oder Wetterereignissen
- Wie die Amtshaftung bei Fehlern bei Erlass der Betriebsbereichsgenehmigung geregelt ist
- Wie bei autonomen Fahrzeugen mit der Forderung aus §15 StVO umzugehen ist, dass im Pannenfall ein Warndreieck aufgestellt werden muss
- Welche Gesetzestexte ggf. noch angepasst werden müssen, wenn autonome Fahrzeuge im Regelbetrieb eingesetzt werden

Insbesondere die gesetzlichen Möglichkeiten zur Beschränkung des autonomen Fahrens sind für die Autobahn GmbH ein sehr wichtiges Thema, da sie als Straßenbetreiberin ihrer Verkehrssicherungspflicht nachkommen muss. Aus Sicht der Autobahn GmbH muss daher bei bestimmten dynamischen Ereignissen die Möglichkeit bestehen das autonome Fahren temporär und streckenabschnittsscharf zu einzuschränken. Gemäß dem Gutachten von GSK Stockmann gibt es die in der Abbildung 7 gezeigten gesetzlichen Möglichkeiten zur Beschränkung einer erteilten Betriebsbereichsgenehmigung.

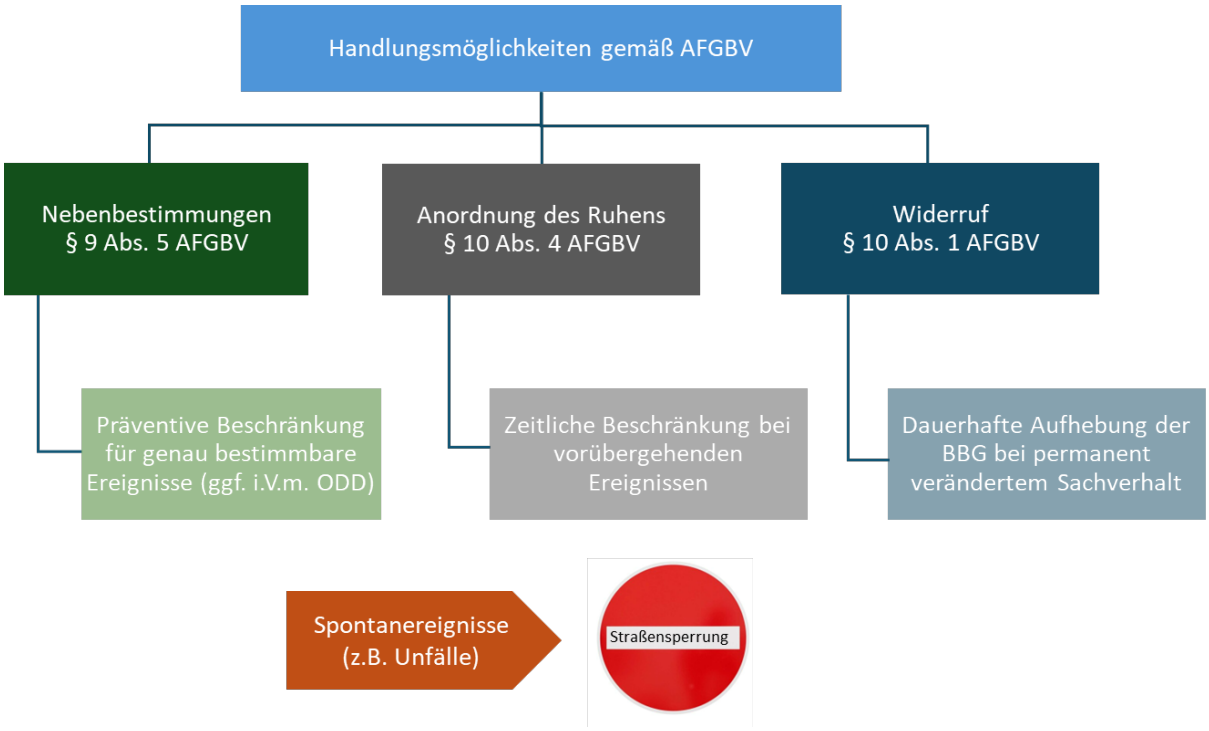



Abbildung 7 Gesetzliche Möglichkeiten zur Beschränkung von autonomem Fahren in einem Betriebsbereich

Bei Genehmigungserteilung können Nebenbestimmungen in die Betriebsbereichsgenehmigung mitaufgenommen werden, die z. B. autonomes Fahren bei definierten Ereignissen einschränken. Außerdem gibt es gemäß §10 Abs. 4 AFGBV die Möglichkeit die Betriebsbereichsgenehmigung temporär ruhen zu lassen. Bei dauerhaft verändertem Sachverhalt ist es auch möglich eine Betriebsbereichsgenehmigung dauerhaft zu widerrufen. Schließlich gibt es noch die Möglichkeit der Straßensperrung, dies gilt dann allerdings für den gesamten Verkehr und nicht nur für autonome Fahrzeuge. Diese Erkenntnisse und auch die weiteren Erkenntnisse aus dem Gutachten sind u.a. in die Entwicklung des digitalen Managementsystems BEA (Betriebsbereichs- und Ereignismanagement auf Autobahnen) eingeflossen, das die Autobahn GmbH entwickelt hat, um Betriebsbereiche digital zu genehmigen und zu verwalten (siehe auch Abschnitt 3.1.3 und Abschnitt 3.9).

Der neue gesetzliche Rahmen ist natürlich nicht nur für die Autobahn GmbH als genehmigende Behörde, sondern auch für Fahrzeughersteller relevant. Daher hat auch MAN eine Gesetzesanalyse durchgeführt. Hierbei wurden sowohl die Anforderungen für eine Freigabe nach AFGBV analysiert als auch die späteren Anforderungen für ein L4-Fahrzeug. Die relevanten Prozesse und Dokumente für die Prototypen-Freigabe nach AFGBV sind in die Sicherheitsargumentation für die Prototypen eingeflossen (siehe Beschreibung Kapitel 3.1.2.). Zusätzlich wurde der neu in Kraft getretene Prozess analysiert (siehe entsprechender Absatz in Kapitel 3.1.3).

Die Anforderungen für ein L4-Fahrzeug wurden im Rahmen der Erhebung der Anforderungen für das Nominalverhalten in AP 3 durchgeführt und sind dort genauer beschrieben.

### 3.1.2 Erstellung der Sicherheitsargumentation (AP 1.2)

Bei der Sicherheitsargumentation ist zwischen der konzeptionellen Sicherheitsargumentation für SAE-Level-4-Serienfahrzeuge und der praktischen Sicherheitsargumentation, die als Grundlage für die Freigabe der ATLAS-L4-Prototypenfahrzeuge, dient, zu unterscheiden.

**Sicherheitsargumentation SAE-Level-4-Fahrzeug**

Der Sicherheitsnachweis für den Betrieb automatisierter Fahrzeuge stellt das Feld bis heute vor große Herausforderungen. Im Produkthaftungsfall muss plausibel argumentiert werden können, dass die Entwicklung und Absicherung mit der notwendigen Sorgfalt und nach Stand der Wissenschaft und Technik stattgefunden haben. Die hohe Komplexität der Systeme und ihrer Aufgabe, sich in einer offenen Welt zu bewegen, führt unweigerlich zu Restrisiken, zu hoher Entwicklungs- und damit einhergehend maßgeblicher Rechtsunsicherheit.

Es ist daher zwingend erforderlich, einen strukturierten Nachweis zu führen, dass eine Reduktion des Risikos auf ein akzeptables Maß erfolgt ist. Bei einer „Sicherheitsargumentation“ handelt es sich um ein anerkanntes Mittel, das diesem Ziel Rechnung trägt. Eine solche Sicherheitsargumentation soll diese Risikoreduktion mithilfe von Evidenzen, die im Entwicklungsprozess erzeugt werden, nachvollziehbar belegen. Wie eine umfassende Sicherheitsargumentation für automatisierte Straßenfahrzeuge geführt werden kann, ist Gegenstand aktueller Forschung.

Im Projekt wurde daher das Ziel verfolgt, die Erstellung einer Sicherheitsargumentation für ein SAE-Level-4-Fahrzeug zu konzeptualisieren und im Modell exemplarisch umzusetzen. Dabei erfolgte die Arbeit im AP 1.2 in enger Zusammenarbeit durch Mitarbeiter der TU Braunschweig und von MAN. Es ist entscheidend, die Argumentationskomplexität zu beherrschen. Hier können Konzepte wie Modularisierung oder Hierarchisierung helfen. Im Projekt wurde daher, wie in der Praxis etabliert, eine semi-formale Notation (Modellierung in Goal Structuring Notation, GSN) verfolgt.

Anforderungen an die Struktur einer Sicherheitsargumentation für automatisierte Straßenfahrzeuge wurden aus dem publizierten Stand der Technik erhoben. Die systematische Anforderungserhebung sowie die Instanziierung einer generischen Argumentationsstruktur, die aus der Anforderungsimplementierung hervorgeht, wurde entsprechend publiziert [1]. Abbildung 8 visualisiert die übergeordnete Argumentationsstruktur.

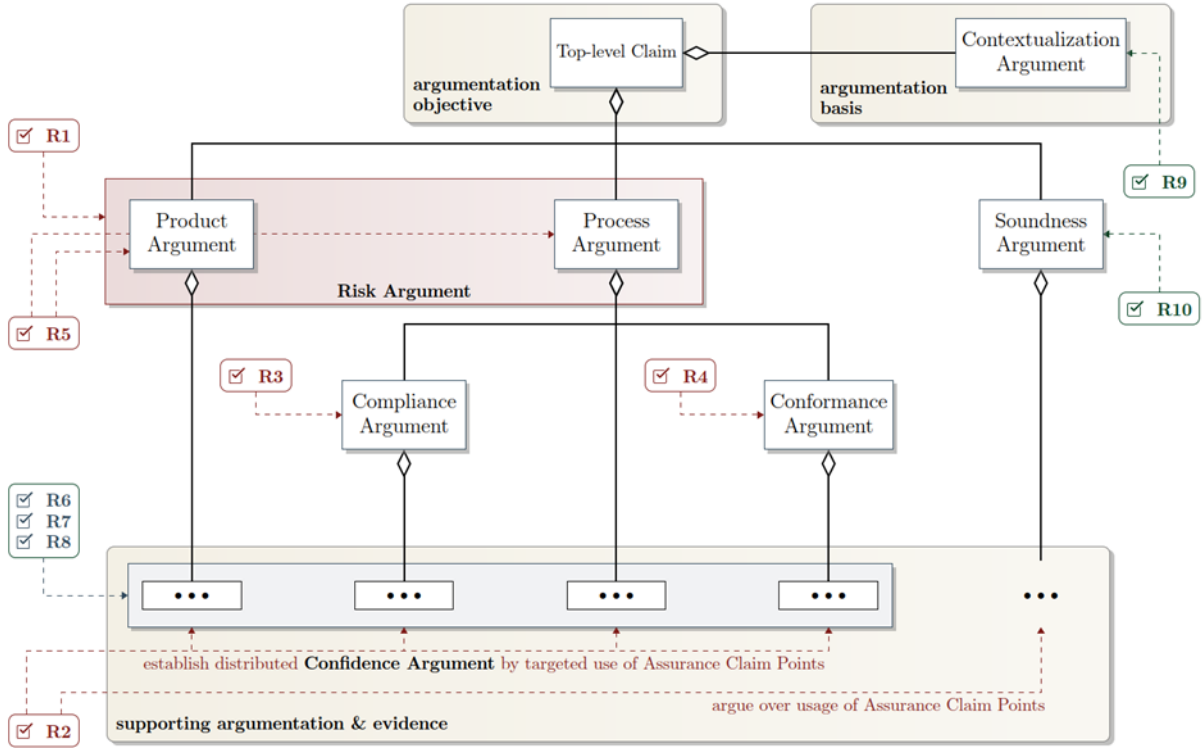



Abbildung 8 Argumentationsstruktur,
die sich aus Implementierung der literaturbasierten strukturellen Anforderungen ergibt;
siehe Loba et al. (2025) für eine detaillierte Diskussion der Anforderungserhebung
und -umsetzung.

Die sukzessive Erarbeitung einer konkreten GSN-Argumentation ist dabei im Einklang mit der dargestellten Argumentationsstruktur erfolgt. Dabei stellt die Abwesenheit unzumutbarer Risiken als Definition der Sicherheit das Argumentationsziel dar, während eine entsprechende Kontextualisierung des Argumentationsgegenstands die Argumentationsbasis bereitet. Das Risikoargument wird über zwei Teilargumentationen weiter heruntergebrochen: Einerseits gilt es über die Eigenschaften des implementierten (Sub-)Systems (Produktargument) und andererseits über den dahinter liegenden Entwicklungs- und Bewertungsprozess (Prozessargument) zu argumentieren. Dabei beinhaltet das Prozessargument neben der Argumentation über den lebenszyklusbezogenen Entwicklungsprozess dedizierte Betrachtungen für die Normenkonformität (Konformitätsargument) und Gesetzes-Compliance (Compliance-Argument). Dies meint, dass darüber argumentiert wird, ob und wie die normativen/rechtlichen Anforderungen durch den Prozess adressiert werden. Somit fand hier unmittelbar eine Verknüpfung der Arbeiten zur Normen- und Gesetzesanalyse im AP 1.1 statt. Das sogenannte Soundness-Argument adressiert Maßnahmen, um die gesamte Argumentation kritisch zu hinterfragen und die Konfidenz in deren Stichhaltigkeit durch geeignete (qualitative und quantitative) Bewertungsmethoden zu erhöhen.

Die entwickelten Prinzipien und Argumentationen wurden von TÜV Süd in enger Zusammenarbeit mit TU Braunschweig und MAN gereviewed. Das Review erfolgte in mehreren Iterationen und Feedbackschleifen und konzentrierte sich inhaltlich darauf

- Einen Abgleich mit State-of-the-Art Erkenntnissen aus vorherigen Projekten (z. B. VV-Methoden) sowie eine Berücksichtigung des relevanten normativen Rahmens sicherzustellen
- Die präzise Verwendung von Begriffen und Definitionen z. B. für Ziele, Restrisiken und Evidenzen zu garantieren (u. a. durch Einbeziehung FUSE-Framework)
- Die Nachvollziehbarkeit der Argumentation sowie der Risikobewertungen zu überprüfen

Die resultierenden Argumentationsprinzipien wurden während der Projektlaufzeit ebenfalls durch Mitarbeitende der TU Braunschweig und von MAN auf einschlägigen Fachkonferenzen präsentiert und diskutiert – wobei eine exemplarischer Tiefbohrung die Argumentation über die adäquate Definition der Einsatzumgebung (Operational Design Domain) war [2]. Abbildung 9 zeigt exemplarisch die höchste Argumentationsebene als Ausschnitt aus dem im Projekt entworfenen GSN-Modell, das konsistent mit der zuvor beschriebenen Argumentationsstruktur ist.

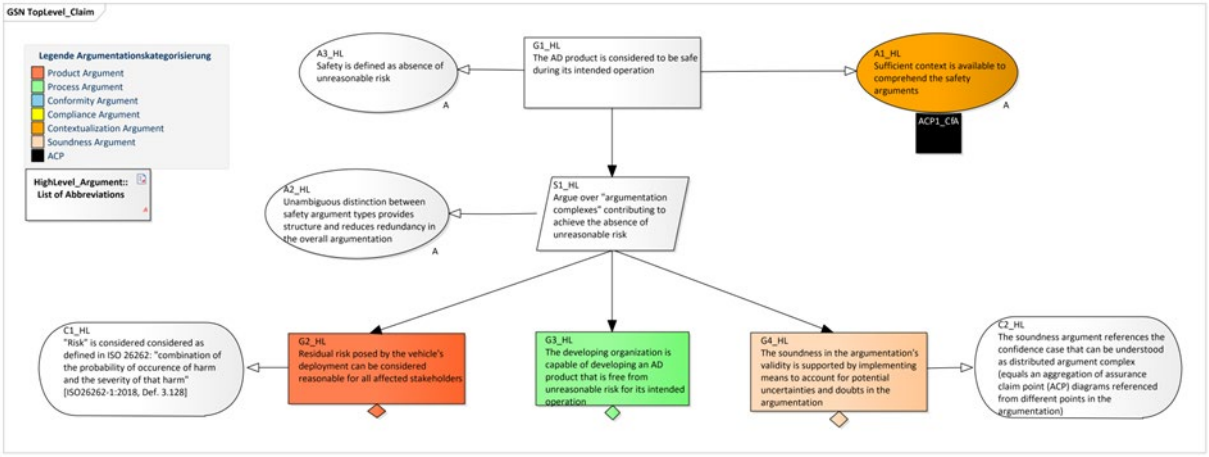



Abbildung 9 Höchste Argumentationsebene als Ausschnitt aus GSN-Modell.

### Sicherheitsargumentation Prototypen-Fahrzeuge

Neben der beschriebenen konzeptuellen Sicherheitsargumentation für ein L4-Fahrzeug, war auch die Freigabe der Testfahrzeuge, siehe Übersichts-Poster „Hardware-Architektur“ (mit Sicherheitsfahrer im Fahrzeug) Gegenstand des Projekts. Durch das Inkrafttreten der AFGBV während der Projektlaufzeit, hat sich der Gesetzesrahmen für dieses Vorhaben geändert und wurde deutlich komplexer.

Um die neuen Anforderungen aus der AFGBV zu erfüllen, wurde im Projekt ein Set an sicherheitsrelevanter Dokumentation (z. B. Entwicklungskonzept, Risikoanalyse, funktionales und technisches Sicherheitskonzept, Verifikation & Validierung, Schulung & Training Sicherheitsfahrer ...) auf Basis eines Frameworks des TÜV Süd für die Prototypen-Fahrzeuge erstellt und mit den zuständigen Behörden (Kraftfahrtbundesamt, BSI, Autobahn GmbH) abgestimmt. Als Ergebnis konnte eine der ersten Freigaben von automatisierten Nutzfahrzeugen auf öffentlichen Straßen nach AFGBV erreicht werden. Der Durchlauf dieses Prozesses hat viele wertvolle Erfahrungen für die Zulassung automatisierter Fahrzeuge bei allen beteiligten Partnern generiert und eine Vielzahl weiterer Schritte ermöglicht.

Auf dieser Grundlage konnten im Projektverlauf weitere Fahrzeuge mit erweitertem Funktionsumfang (z. B. Verbindung zu dem Control Center) und damit einhergehenden Herausforderungen (Cybersecurity) freigegeben werden.

### 3.1.3 Erstellung und Durchführung des Freigabeprozesses (AP 1.3)

**Freigabe Prototypen-Fahrzeuge**

Voraussetzung zur Beantragung einer AFGBV-Erprobungsgenehmigung war die EG-Gesamtbetriebserlaubnis (WVTA) für das Sensorfahrzeug. Nach der Ausrüstung des Basisfahrzeugs mit der AD-Sensorik und -Hardware wurden dieses im ersten Schritt vom Technischen Dienst (TÜV SÜD) als Versuchsfahrzeug nach StVZO §19(6) als „Datensammler im Shadow-Mode“ zugelassen, wozu verschiedene Ausnahmegenehmigungen bei der zuständigen Bezirksregierung (Regierung der Oberpfalz) eingeholt werden mussten. Nach Vorstellung des ATLAS-L4-Projekts beim Kraftfahrt-Bundesamt (KBA) und der gemeinsamen Abstimmung der Anforderungen, wurde ein offizieller Antrag auf Erteilung einer Level-4-Erprobungsgenehmigung gestellt und das Entwicklungskonzept nach Muster des KBA als wesentlicher Punkt der Erprobungsgenehmigung erarbeitet. In enger Anlehnung an dieses Entwicklungskonzept wurde der Beschreibungsbogen für das Fahrzeug erstellt. Schwerpunkte in den folgenden Besprechungen mit dem KBA waren u. a. die Punkte des Sicherheitskonzepts, die technische Überwachung, bzw. die Rolle des Sicherheitsfahrers und dessen Schulungsprogramm, die Datenspeicherung, -sicherung und -übermittlung an das KBA, sowie die Softwareversionen und die Cybersicherheit auch hinsichtlich der Funkschnittstellen.

Die beim KBA eingereichten Unterlagen wurden vom KBA zur Anhörung an die für den Betriebsbereich (ODD) zuständige Behörde – in diesem Fall die Autobahn GmbH – und bezüglich der Datensicherheit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) weitergeleitet. Die Stellungnahmen im Rahmen der Anhörung fielen positiv aus. Abschließend wurden im Rahmen einer Fahrzeugbegutachtung inkl. der AD-Sensorik und Hardware, Prüfungsfahrten auf dem Testgelände mit KBA-Testingenieuren durchgeführt. Im März 2024 wurde dann die erste AFGBV-Level4-Erprobungsgenehmigung für das ATLAS-L4 Sensorfahrzeug vom KBA erteilt. Es folgte eine Verlängerung der Erprobungsgenehmigung bis zum 30.06.2027.

**Freigabeprozess Level-4-Serienfahrzeuge**

Wie in Abbildung 6 gezeigt und in Abschnitt 3.1.1 beschrieben, besteht der Freigabeprozess für Level 4-Serienfahrzeuge aus drei Schritten. Während der erste (EU-Typgenehmigung) und letzte Schritt (Fahrzeugzulassung) grundsätzlich bereits aus den Freigabeprozessen für herkömmliche Fahrzeuge bekannt sind, ist der zweite Schritt (Betriebsbereichsgenehmigung) erst mit der Einführung des Gesetzes zum autonomen Fahren und der AFGBV entstanden. Die Autobahn GmbH ist im gesamten deutschen Autobahnnetz für die Betriebsbereichsgenehmigung zuständig. Auf diese neue Aufgabe der Betriebsbereichsgenehmigung hat sich die Autobahn GmbH durch die Entwicklung eines digitalen Managementsystems vorbereitet. Dieses System namens BEA (Betriebsbereichs- und Ereignismanagement auf Autobahnen) ermöglicht die initiale Genehmigung von Betriebsbereichen sowie deren anschließende Verwaltung. Zur Genehmigung können Antragsteller in einem Webportal die erforderlichen Nachweise und Informationen einreichen. Die Prüfpunkte basieren auf den Regelungen in der AFGBV zur Betriebsbereichsgenehmigung sowie einem Mustergenehmigungsbogen, der im Rahmen des

Arbeitskreises „Adhoc AG Betriebsbereichsgenehmigung“ entwickelt wurde. Teilweise müssen Nachweise hochgeladen werden, andere Prüfpunkte enthalten Hinweise, die nur als „zur Kenntnis genommen“ abgehakt werden. Anschließend können die Verantwortlichen der Autobahn GmbH die Nachweise prüfen und daraufhin Nachforderungen stellen sowie die Genehmigung erteilen oder ablehnen. Tabelle 2 zeigt eine Übersicht der einzureichenden Dokumente.

Tabelle 2 Antragsdokumente für die Betriebsbereichsgenehmigung (Quelle: Mustergutachten Betriebsbereichsgenehmigung aus Arbeitskreis „Adhoc AG Betriebsbereichsgenehmigung“)

| **Thema** | **Einzureichende Unterlagen** |
|---|---|
| Antragsdokumente (Unterlagen, Planunterlagen, gemäß § 8 AFGBV) | • Antrag seitens des Halters<br>• Betriebserlaubnis<br>• Beschreibung des Betriebsbereichs<br>• Beschreibung des Betriebszwecks<br>• Bestätigung des KBA bzgl. der Gleichwertigkeit als Nachweis zur Gültigkeit/Übertragbarkeit von nationalen ausländischen Betriebserlaubnissen |
| Deaktivierbarkeit / Reaktivierbarkeit der autonomen Fahrfunktion | • Betriebsstrategie des Fahrzeugs<br>• Netzabdeckungskarte(n)<br>• Ergebnis: Prüfbericht zur Deaktivier-/Reaktivierbarkeit der AF-Funktion (über die Technische Aufsicht) |
| Gültigkeit/Übertragbarkeit von nationalen ausländischen Betriebserlaubnissen | • Betriebserlaubnis<br>• Bestätigung des KBA bzgl. der Gleichwertigkeit |
| Technische Aufsicht | • Führungszeugnis (Belegart O)<br>• Auskunft aus dem Fahreignungsregister<br>• die für den Betriebszweck erforderlichen Nachweise der eingesetzten Personen<br>• Ausbildungsnachweis im Sinne des § 14 Abs. 1 AFGBV<br>• Ergebnis: Prüfbericht zur Eignung der eingesetzten Personen |

Im Sinne der Benutzerfreundlichkeit wurden die Prüfpunkte im Antragformular so aufbereitet, dass sie für Antragstellende möglichst schnell und bequem auszufüllen sind. Auch auf Barrierefreiheit wurde geachtet. In Abbildung 10 ist beispielhaft die Auswahl des Betriebsbereichs gezeigt. Neben der in der Abbildung gezeigten Auswahl durch Anklicken eines Start- und Endabschnitts auf der Karte kann der Betriebsbereich auch durch die Pfeiltasten in einer Baumstruktur ausgewählt werden.

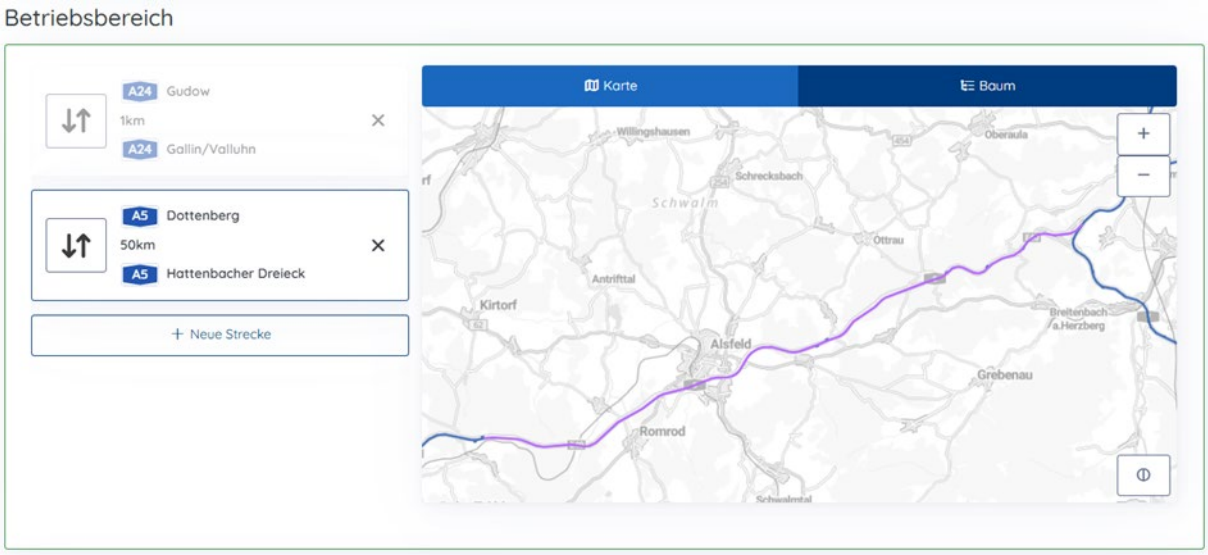



Abbildung 10 Antragsformular: Auswahl des Betriebsbereichs über die Karte

Das Antragsformular in BEA bietet zudem eine Fortschrittsübersicht mit der Möglichkeit zu den noch auszufüllenden Punkten zu springen, die Möglichkeit eigene bereits in der Vergangenheit eingereichte Anträge als Basis für einen neuen Antrag zu nutzen sowie E-Mail-Benachrichtigungen für Statusupdates zu eingereichten Anträgen.

Einzelne Prüfpunkte wurden im Rahmen des bereits in Abschnitt 3.1.1 beschriebenen rechtlichen Unterauftrags einer genauen Betrachtung unterzogen, mit dem Ziel auch den Antragsprüfenden eine möglichst genaue Hilfestellung bei der Prüfung zu bieten. Beispielsweise wurde erörtert, wann genau ein Führungszeugnis als „in Ordnung“ und wann als „Mangelhaft“ zu bewerten ist. Auf diese Weise soll eine möglichst unkomplizierte, objektive und einheitliche Prüfung sichergestellt werden.

Insgesamt konnten somit im AP 1 zum einen die Erprobungsgenehmigungen für die ATLAS-L4-Prototypen-Fahrzeuge erlangt und zum anderen wichtige Grundlagen für Sicherheitsargumentation und Freigabeprozess von Level-4-Serienfahrzeugen geschaffen werden.

### 3.1.4 AP 1 – Vortrag und Poster der Abschlusspräsentation

## AP1: SICHERHEITSARGUMENTATION UND FREIGABE

ATLAS-L4

**Übersicht**

**Motivation**

Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren sowie Autonome-Fahrzeuge-Genehmigungs-und-Betriebsverordnung (AFGBV)

-Neue Prozesse für die Erprobungsgenehmigung

-Prozesse für die Regelgenehmigung:

**Kraftfahrt-Bundesamt** Allgemeine Betriebserlaubnis oder EU-Typgenehmigung → **Zuständige Behörde*** Genehmigung Betriebsbereich → **Zulassungs-stelle**

*nach Bundes- oder Landesrecht zuständige Behörde oder auf Bundesfernstraßen, soweit dem Bund die Verwaltung zusteht, die Gesellschaft privaten Rechts im Sinne des Infrastrukturgesellschaftserrichtungsgesetzes

**Arbeitsschwerpunkte**

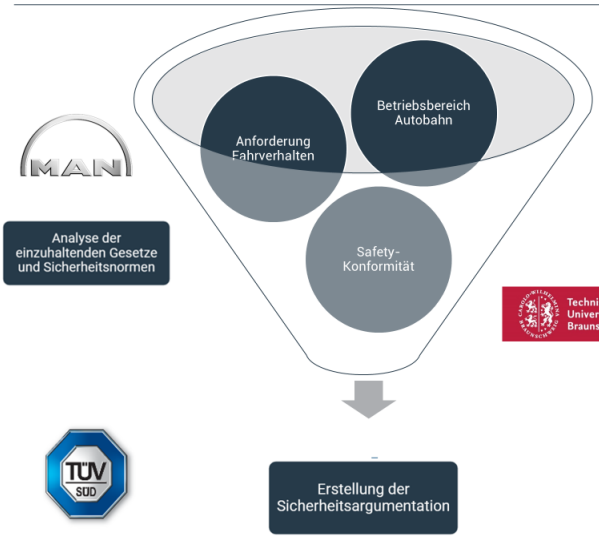
- Analyse der einzuhaltenden Gesetze und Sicherheitsnormen
- Erstellung der Sicherheitsargumentation
- Erstellung und Durchführung des Freigabeprozesses

ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Susanne Schulz, Die Autobahn GmbH des Bundes 15

## AP1: SICHERHEITSARGUMENTATION UND FREIGABE

ATLAS-L4

**Übersicht**




Die Autobahn

**Sicherheitsargumentation für Demonstrationsfahrzeug (Baustein Erprobungsgenehmigung):**

Mit vor Ort anwesender, in Bezug auf technische Entwicklungen für den Kraftfahrzeugverkehr zuverlässige Technische Aufsicht. (§16 AFGBV)

**Sicherheitsargumentation für konzeptionelles Level 4 Fahrzeug (Baustein Regelgenehmigung):**

Risikobasierte Argumentation → Nachweis für Risikoreduktion auf ein zumutbares Niveau

Detailargumentation im GSN-Modell

ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Susanne Schulz, Die Autobahn GmbH des Bundes 16

## AP1: SICHERHEITSARGUMENTATION UND FREIGABE

**Erstellung und Durchführung des Freigabeprozesses**

Erstellung und Durchführung des Freigabeprozesses

### Erprobungsgenehmigung (erteilt):

- **Erteilung der Erprobungsgenehmigung** an MAN durch das KBA im April 2024 → Erprobungsfahrten im öffentlichen Straßenverkehr
- Autobahn GmbH und Bundesamt für Sicherheit in der Informationstechnik wurden durch das Kraftfahrt-Bundesamt angehört

### Teil der Regelgenehmigung:

- Grundlage für die die Entwicklung des digitalen Managementsystems BEA (Betriebsbereichs- und Ereignismanagement auf Autobahnen) für die Genehmigung und Verwaltung von Betriebsbereichen auf Autobahnen


Demonstrationsfahrzeug bei Erprobungsfahrt im öffentlichen Straßenverkehr

ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Susanne Schulz, Die Autobahn GmbH des Bundes 19

# SICHERHEITSARGUMENTATION UND FREIGABE
## Übersicht

### MOTIVATION UND ZIELE

- Rechtsrahmen für Einführung von Kraftfahrzeugen mit autonomen Fahrfunktionen (SAE Level 4) wurde geschaffen → Neue Aufgaben sowohl auf Infrastruktur- als auch auf Fahrzeugseite
- Während für konventionelle Fahrzeuge Sicherheitsargumentation und Zulassung etablierte Prozesse sind, müssen diese für autonome Fahrzeuge noch entwickelt werden

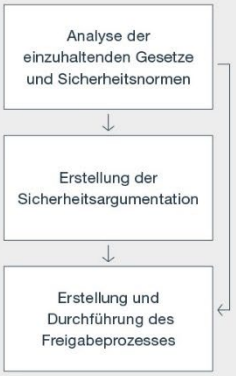
**Rechtsrahmen**

UNECE · EUROPEAN COMMISSION · §

**Normative Dokumente**

Automated Vehicle Safety Consortium · bsi · IEEE SA STANDARDS ASSOCIATION · ISO · SAE INTERNATIONAL · UL Standards & Engagement

### ARBEITSSCHWERPUNKTE




Arbeitsschwerpunkte und Vorgehensweise

- Analyse der einzuhaltenden Sicherheitsnormen
- Gesetzesanalyse
  - Gesetz zum autonomen Fahren und AFGBV zur Klärung des Freigabeprozesses mit Fokus Betriebsbereichsgenehmigung
  - Straßenverkehrsordnung zur Ableitung von Fahrverhaltensanforderungen
- Erstellung Sicherheitsargumentation und Freigabeprozess
  - Für Demonstrationsfahrzeug
  - Für konzeptionelles Level 4 Fahrzeug

### ERGEBNISSE/HIGHLIGHTS

- Erprobungsgenehmigung nach AFGBV für Demonstrationsfahrzeug erhalten
  → Testfahrten im Realverkehr auf der Autobahn seit April 2024
- Konzeptionelle Level 4 Sicherheitsargumentation entwickelt
- Software für digitale Beantragung und Prüfung von Betriebsbereichsgenehmigungen entwickelt: BEA (Betriebsbereichs- und Ereignismanagement auf Autobahnen)


April 2024: Öffentlichkeitswirksame erste Testfahrt auf der Autobahn

# ÜBERSICHT ZULASSUNG AUTONOMER FAHRSYSTEME

## Sicherheitsargumentation und Freigabe

| INTERNATIONALER RECHTSRAHMEN (EU UND UNECE): | | |
|---|---|---|
| | **LEVEL 3** | **LEVEL 4** |
| Erprobung | Genehmigung erfolgt nach nationalem Rechtsrahmen | |
| Regelbetrieb | **UN Regulation No. 157**<br>■ Fahrzeugklassen M, N, O<br>■ Betrieb auf Autobahnen und ähnlichen Straßen bis 130 km/h<br>■ System muss manuell aktiviert und deaktiviert werden können<br>■ Fahrer muss übernahmebereit sein<br>■ Genehmigung des Fhzg nach VO(EU) 2018/858 → keine Betriebsbereichsgenehmigung | **VO(EU) 2022/1426**<br>■ Genehmigung für autom. Fahrsystem bei Fahrzeugklassen M und N in Kleinserie (1500 Fhzg /Jahr)<br>■ Anwendungsfälle: Shuttle-/Goods-Mover, Hub-to-Hub, AVP[3]<br>■ Kleinseriengenehmigung nach VO(EU) 2018/858<br>■ Betrieb und Zulassung der Kfz in Deutschland in AFGBV[2] geregelt |

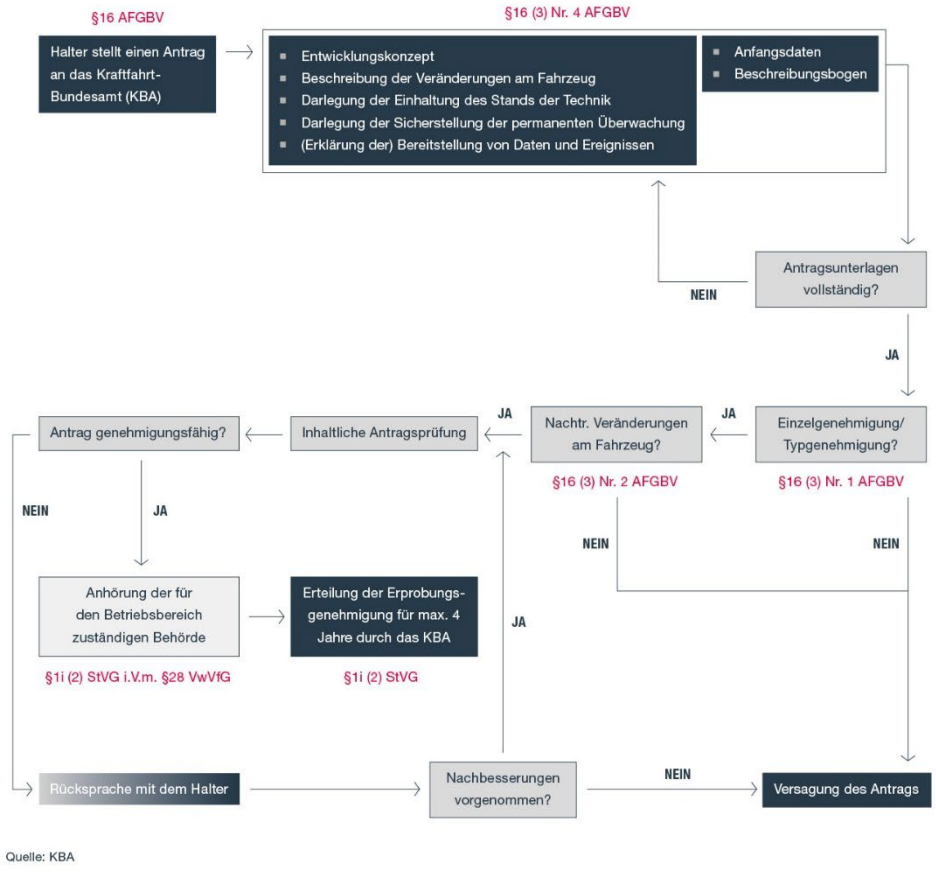
| NATIONALER RECHTSRAHMEN (DEUTSCHLAND): | | |
|---|---|---|
| | **LEVEL 3** | **LEVEL 4** |
| Erprobung | **Erprobungsgenehmigung**<br>■ § 1i StVG[6] und §16 AFGBV<br>■ KBA[5] ist genehmigende Behörde<br>■ Zuständige Landesbehörde / Autobahn GmbH und BSI[4] werden angehört<br>■ Automatisiertes Fahrsystem muss zu jedem Zeitpunkt deaktivierbar und vor Ort durch Fahrzeugführer bzw. Technische Aufsicht übersteuerbar sein | |
| Regelbetrieb | **Gesetz zum automatisierten Fahren (2017) – StVG**<br>■ Nationale Typengenehmigung für Kfz nach StVZO (KBA) → Zulassung<br>■ Fahrfunktion bewältigt Fahraufgabe (Längs- und Querführung)<br>■ Fahrzeugführer darf sich vom Verkehrsgeschehen abwenden, muss aber übernahmebereit bleiben | **Gesetz zum autonomen Fahren (2021) – StVG und AFGBV (2022)**<br>■ Anwendbar für Fahrzeuge aller Art<br>■ Dreistufiges Verfahren: ABE[1] (alle Fhzg außer M & N) oder Kleinserie (M & N)*<br>→ Betriebsbereichsgenehmigung<br>→ Zulassung<br>■ Technische Aufsicht notwendig |

1: Allgemeine Betriebserlaubnis
2: Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung
3: Automated Valet Parking
4: Bundesamt für Sicherheit in der Informationstechnik
5: Kraftfahrtbundesamt
6: Straßenverkehrsgesetz

*: EG-Fahrzeugklassen:
M = Für die Personenbeförderung ausgelegte und gebaute Kraftfahrzeuge mit mindestens vier Rädern
N = Für die Güterbeförderung ausgelegte und gebaute Kraftfahrzeuge mit mindestens vier Rädern

# ERPROBUNGSGENEHMIGUNG NACH AFGBV

## Sicherheitsargumentation und Freigabe




Quelle: KBA

### ANHÖRUNG DER FÜR DEN BETRIEBSBEREICH ZUSTÄNDIGEN BEHÖRDE:

Die Autobahn GmbH wird im Rahmen der Erprobungsgenehmigung auf Autobahnen vom KBA angehört

- Möglichkeit, Hinweise einzubringen
- Information über Besonderheiten, die auf Autobahnen auftreten können. z. B.:
  - Vom aktuellen Regelwerk (RAA[1]) abweichende Straßengeometrie
  - Großraum- und Schwertransporte und Konvois
  - Nicht StVO-konformes Verhalten

[1]: Richtlinien für die Anlage von Autobahnen

# SICHERHEITSARGUMENTATION FÜR EIN SAE-L4-FAHRZEUG

## Sicherheitsargumentation und Freigabe

### MOTIVATION

Die Komplexität automatisierter Straßenfahrzeuge und ihrer Umwelt führt unweigerlich zu Restrisiken im Betrieb. Der Wegfall eines Menschen, der die Fahraufgabe bisher verantworten musste, bedingt somit eine hohe Entwicklungsunsicherheit. Um zukünftig Lkw nach SAE-Level-4 in Verkehr bringen zu können, bedarf es einer strukturierten Argumentation der Systemsicherheit. Diese soll mithilfe gesammelter Evidenzen einen Nachweis für die Risikoreduktion auf ein zumutbares Niveau liefern. Das Erzeugen einer kohärenten Argumentation, die sämtliche etablierte Absicherungsprozesse ganzheitlich betrachtet, stellt dabei eine zentrale Herausforderung dar.

### ANSATZ

- Gesetzes- und Normenanalyse unterstützt die Erstellung der Sicherheitsargumentation
- unabhängiges Review erhöht Konfidenz in Validität der Argumentation
- Komplexitätsbeherrschung durch Strukturierung, Modularisierung & Hierarchisierung

→ Modellierung mittels semi-formaler Notation (Goal Structuring Notation)

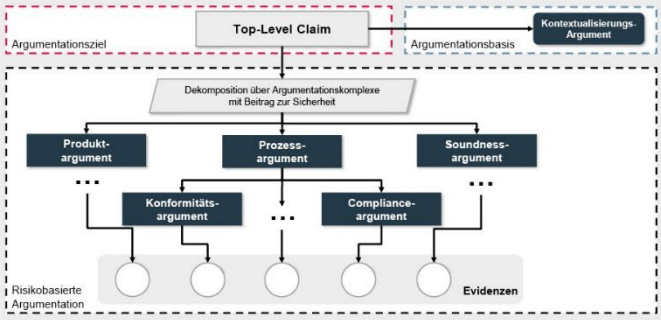



Abb. 1: Übergeordnete Struktur der Argumentation

↓ MODELLIERUNG

### ARGUMENTATIONSSTRUKTUR

Systematische Dekomposition über Argumentationskomplexe

- Kontextualisierungsargument
- Produktargument
- Prozessargument
  - Konformitätsargument
  - Compliance-Argument
- Soundness-Argument

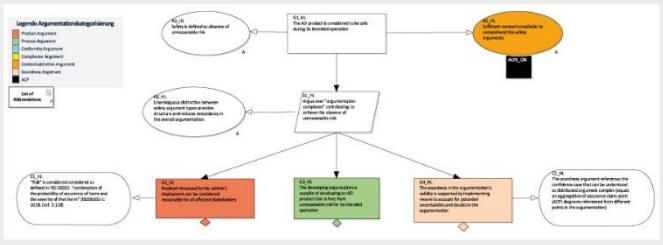


Abb. 2: Ausschnitt aus konkreter Modellierung

# ERPROBUNGSGENEHMIGUNG NACH AFGBV PRAKTISCHER ANTEIL

## Sicherheitsargumentation und Freigabe

### MOTIVATION

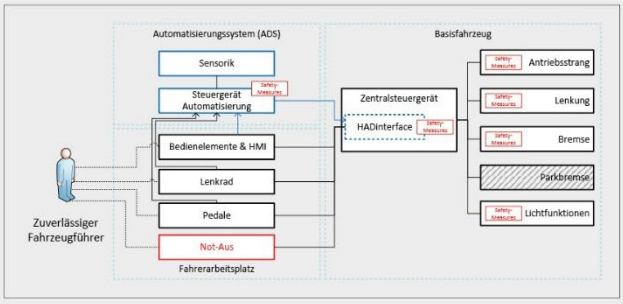
Mit dem Inkrafttreten der AFGBV am 01.07.2022 wurde durch den Gesetzgeber ein Rahmen für die Erprobung von Fahrzeugen mit autonomer Fahrfunktion erstellt. Da ein Teil der Fahrzeuge im ATLAS-Projekt davon betroffen ist, wurde der Prozess zur Erlangung einer Erprobungsgenehmigung nach AFGBV anhand des Demonstrationsfahrzeugs und des Sensorfahrzeugs in AP1.2. durchgeführt.

### ÜBERBLICK FAHRZEUGAUFBAU

- Ausgestattet mit prototypischem ADS und zusätzlichen Komponenten (Sensorik, HMI, Connectivity, ...)
- Keine Redundanz im Fahrzeug
- Erweiterung durch Control-Center-Verbindung (Stichwort: Security)

### KURZBESCHREIBUNG SICHERHEITSKONZEPT

- Zuverlässiger Fahrzeugführer muss das Fahrzeug jederzeit beherrschen können, u. a. durch:
  - Übersteuerung des ADS (z.B. via Bremspedal, Gaspedal, Lenkrad,...)
  - Limitierung der ADS-Anforderungen im Basisfahrzeug
  - Not-Aus-und Mode-Management-Konzept
- Organisatorische Maßnahmen:
  - Entwicklung weitestgehend orientiert an "Stand der Technik"
  - Fahrertraining in Theorie und Praxis (fahrzeug-spezifisch, reduzierte ODD, Fahrzeitbegrenzung, ...)
  - Sicherstellung, dass nur befugte Personen die Fahrzeuge führen können




### DOKUMENTATION

- Entwicklungskonzept inkl. Entwicklungsplan, Fahrzeugaufbau, Fahrfunktionen, ...
- Weitere erstellte Dokumentation: Item-Definition, Risikoanalyse, Sicherheitskonzept, Sicherheitsanalysen, Teststrategie, Testspezifikation, Fahrertraining, ....

# NORMENANALYSE ZUR SICHERHEIT AUTOMATISIERTER FAHRZEUGE

## Sicherheitsargumentation und Freigabe

### MOTIVATION

Die Entwicklung automatisierter Straßenfahrzeuge stellt Hersteller vor große Herausforderungen. Im Kontext einer offenen Welt bedingen die hohe Komplexität der Systeme selbst und ihrer Fahraufgabe inhärente (Rest-)Risiken. Während die Konformität mit Normen keine hinreichende Grundlage für eine Freigabeargumentation ist, stellt sie dennoch eine wichtige Grundlage für die Gestaltung des Entwicklungsprozesses dar. Zudem trägt diese im Sinne des Produkthaftungsgesetzes, das eine Entwicklung nach geltendem Stand der Technik fordert, zur Rechtssicherheit bei.

### VORGEHEN

**1. Definition von Verortungskategorien**

- Sicherheitsdisziplinen mit Schnitt über jeweils zugrundeliegende Gefährdungsursache (z. B. „Funktionale Sicherheit“ → Hard- und Softwarefehler)
- übergeordnete Kategorien mit Konsequenzen für mehrere Sicherheitsdisziplinen (z. B. „Terminologie“)

**2. Identifikation relevanter Dokumente**

- ISO, IEEE SA, IEC, SAE (AVSC), BSI & UL
- AD-spezifische normative Dokumente
- technologieneutrale Dokumente mit übertragbaren Konzepten/Prinzipien

**3. Kategorienspezifische Fokusanalysen**

- inhaltliche Zusammenfassung & Übersicht
- dokumentenindividuelle & ganzheitliche Betrachtung für Evaluierung von Synergien, Limitationen, Reifegrade, Widersprüchen …


Abb. 1: Übersicht der Kategorien

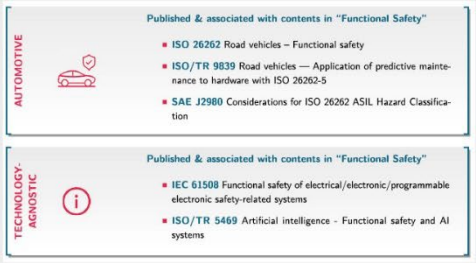



Abb. 2: Ausschnitt aus der Analyse für domänenspezifische und technologieneutrale normative Dokumente; zugeordnet zur Sicherheitsdisziplin „Funktionale Sicherheit“

### ERGEBNISSE

- hohe Dynamik der Normenlandschaft mit unterschiedlicher Reife der Dokumente
- Normungsbedarf für unterrepräsentierte Aspekte, etwa hinsichtlich der systematischen Berücksichtigung von Ethik sowie der nachverfolgbaren Auflösung von Wertekonflikten
- Normung unterliegt Interessen → kritische Prüfung normativer Dokumente notwendig
- Verwertung der Analyse im „Konformitätsargument“ der Sicherheitsargumentation

# C-ITS UND AUTONOMES FAHREN: EIN ECOSYSTEM ENTSTEHT

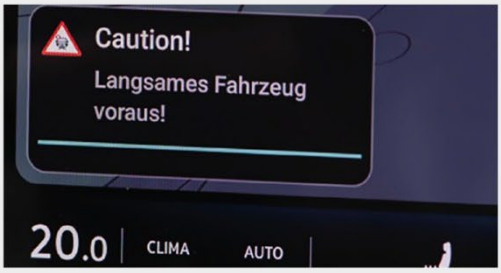
## WAS IST C-ITS?

C-ITS steht für „kooperative intelligente Verkehrssysteme“ und setzt auf die Vernetzung von Fahrzeugen, Dienste-anbietern und Infrastruktur. Das Ziel ist es, die Verkehrs-sicherheit auf den Autobahnen zu erhöhen. Mit C-ITS erhalten Verkehrsteilnehmende durch Direktkommunikation (IEEE 802.11p/WLANp) in ihren Fahrzeugen Informationen aus erster Hand und können darauf reagieren.

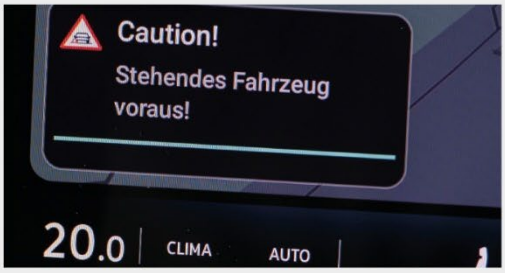

Warnmeldung vor einer Baustelle im VW ID.3

## USE CASE MINIMUM RISK MANOEUVRE / CONDITION (MRM / MRC)

Das Minimum Risk Manoeuvre stellt beim autonomen Fahren eine Rückfallebene für kritische Ereignisse dar, bei der das Fahrzeug an einer möglichst sicheren Stelle anhält. C-ITS-Nachrichten sind eine sichere Kommunikationsmöglichkeit, um Verkehrsteilnehmende in der Nähe zu warnen und über den MRM-Status zu informieren. Es handelt sich quasi um ein „digitales Warndreieck“. Ein Ecosystem aus verschiedenen innovativen Technologien entsteht.




Warnmeldung vor einem langsam fahrenden Fahrzeug




Warnmeldung vor einem stehenden Fahrzeug

## USE CASE ROAD WORKS WARNING

Nähert sich ein (autonomes) Fahrzeug einer Baustelle, erhält es bis zu 800 Meter davor über WLANp die Information „Achtung, Baustelle voraus“. Damit bleibt dem Fahrzeug genügend Zeit, um entsprechend auf die Situation zu reagieren, noch bevor diese von der Sensorik erfasst werden kann.

Ein autonomer Lkw passiert eine Tagesbaustelle


Exemplarische Darstellung der C-ITS-Nachricht im LKW

# AP 2: Security

Patrick Wagner, Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC)

## 3.2 AP 2: Security

*Arbeitspaketleitung: Patrick Wagner, Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC)*

Für die Entwicklung neuer, sicherer Fahrzeugarchitekturen inkl. eines Control Centers für die technische Aufsicht vollautomatisierter Lkw müssen Security-Anforderungen vollumfänglich und nachvollziehbar ermittelt und berücksichtigt werden. Security-Risikoanalysen ermöglichen hierfür Security-by-Design durch die Ableitung von Anforderungen für eine sichere Systementwicklung. Allerdings berücksichtigten bisherige Methoden zur Security-Risikoanalyse in der Automobilentwicklung noch nicht die spezifischen Gegebenheiten des autonomen Warentransports auf Schnellstraßen. Daher wurde während der Projektlaufzeit eine in der Automobilentwicklung etablierte Methode zur Security-Risikoanalyse auf den speziellen Kontext vollautomatisierter Lkw erweitert und angepasst. Konkret wurden hierfür Bewertungsmodell, Schadenskriterien sowie Annahmen-, Bedrohungs- und Maßnahmenkataloge der Modular Risk Assessment (MoRA) Methode auf die Spezifika vollautomatisierten Fahrens adaptiert. Nach Entwicklung der Methode konnten damit Security-Anforderungen für den autonomen Lkw und sein Control Center ermittelt werden. Somit wurde Security frühzeitig in die Entwicklung der neuen Fahrzeugarchitektur und des Control Centers integriert, um Sicherheitsvorfälle und negative Auswirkungen zu vermeiden sowie gesetzliche Anforderungen zu erfüllen.

Um den Schutz von Fahrzeugen und deren Insassen bestmöglich sicherzustellen, müssen sich Automobilhersteller und -zulieferer mit vielen Security-Standards und Regularien für verschiedene Bereiche befassen. Beispiele hierfür sind die ISO/IEC-27000-Reihe und der BSI Grundschutz für die Office-IT, IEC 62443 für die Produktion, ISO/SAE 21434 und UN Regulation No. 155 für das Automotive Engineering sowie viele Querschnittsthemen wie Software Testing (ISO 29119), Safety (ISO 26262) oder Datenschutz (DSGVO, BDSG). Gerade in der Automobilentwicklung bestehen viele Reibungspunkte zwischen den Bereichen und somit auch bei den Security-Standards. Dabei besteht die Gefahr, dass bei einer unabhängigen Betrachtung der Standards bereichsübergreifende Risiken nicht erkannt werden. Daher wurden während der Projektlaufzeit Security-Standards für die Bereiche IT/Control Center, Produktion, Fahrzeugentwicklung und Werkstatt in einer übergreifenden Sicht analysiert und miteinander verglichen. Konkret wurden hierfür Gemeinsamkeiten und Unterschiede bzgl. Terminologien, Konzepten und Secure Development Lifecycles identifiziert. Zudem wurden Abhängigkeiten und Schnittstellen zwischen den Security-Standards bestimmt. Somit können Anforderungen, Bedrohungen und Risiken für Automobilhersteller und -zulieferer holistisch während des gesamten Entwicklungsprozesses bestimmt werden, die nur in einer übergreifenden Sicht auf die Security-Standards erkannt werden konnten.

Ferner ist es notwendig, dass die bereichsübergreifende Ermittlung von Anforderungen, Bedrohungen und Risiken vollständig und nachvollziehbar dokumentiert wird. Dabei ist es analog zu den Standards so, dass für die einzelnen Bereiche verschiedene Software-Tools eingesetzt werden. Dies verhindert beispielsweise, dass für die Auswirkungen eines Security-Incidents, der in der Produktion stattgefunden hat, unmittelbar ersichtlich ist, welche weiteren Bereiche (Entwicklung, Werkstatt etc.) negativ beeinflusst werden. Daher wurde ein prototypisches Werkzeug für ein bereichsübergreifendes Security-Management konzipiert und ein Proof of Concept entwickelt. Dieses Werkzeug kann als bereichsübergreifendes Wissensbasis- und Incident-Management-Tool für den gesamten Produktlebenszyklus fungieren. Konkret wurden hierfür funktionale und Security-relevante Anforderungen/Use Cases aus Sicht

der Automobilhersteller und -zulieferer und Anforderungen der UN Regulation No. 155 für das Tool definiert. Weiterhin wurde ein übergreifendes Risiko- und Maßnahmeninventar (Template) für alle Bereiche entwickelt, um eine Verknüpfbarkeit sowie eine einheitliche Bewertung und Behandlung von Schutzzielen, Bedrohungen und Maßnahmen zu erreichen. Schließlich wurden Anknüpfungspunkte für die Integration einer solchen Plattform in die Systemlandschaft von Automobilherstellern erarbeitet.

### 3.2.1 Methode Security Risikoanalyse (AP 2.1)

Für die Anpassung der Modular Risk Assessment Methode auf den Kontext von ATLAS-L4 wurden in der Projektlaufzeit mehrere Workshops zwischen Fraunhofer AISEC und MAN abgehalten. Nach einer Abgleichung der Erwartungshaltungen der beteiligten Partner wurde die Terminologie für die Security-Risikoanalysen bestimmt. Die Projektpartner haben sich im Wesentlichen auf die Terminologie des ISO/SAE 21434:2021 Standards festgelegt. Als Methodenkern für die Security-Risikoanalyse wurde Modular Risk Assessment (MoRA) festgelegt, da sich diese bereits für die Ermittlung von Security-Anforderungen für Lkw Funktionen und Steuergeräte bei MAN bewährt hat, ISO/SAE 21434 konform ist und am Fraunhofer AISEC entwickelt wurde. Während der Projektlaufzeit wurde ein Paper zur MoRA-Methode bei den ACM Transactions on Cyber-Physical Systems veröffentlicht [3]

Die grundlegenden Definitionen und Stufen des Bewertungsmodells sowie die resultierende Risikomatrix wurden bestimmt. Hierbei wurde darauf geachtet, die Konformität zu ISO/SAE 21434:2021 zu bewahren. Zudem wurden die Schadensklassen und -kriterien für das Impact Rating bestimmt. Diese umfassen neben den laut ISO/SAE 21434:2021 erforderlichen Klassen Safety, Financial, Operational und Privacy (SFOP) auch weitere Klassen, um OEM-Interessen zu berücksichtigen, wie z. B. potentielle Umsatzverluste, Vertragsstrafen oder Gewährleistungskosten. Zur Einschätzung des Attack Feasibility Ratings wurde im Einklang mit ISO/SAE 21434:2021 ein Attack Potential-basierter Ansatz ausgewählt.

Als Basis für Annahmen- (Angreifermodell, Betriebsumgebung, Scope, …), Bedrohungs- (STRIDE, konkretisiert mit Technologiebezug, UN R.155 Annex 5, …), Maßnahmen- (Existierende Maßnahmen, Abbildung ggf. technologiebezogener Lösungen, …) und Technologiekatalog (Bustechnologien, drahtlose Übertragung, Automotive Betriebssysteme, …) wurden die bestehenden Kataloge von MAN als Grundlage verwendet. Das Fraunhofer AISEC hat dabei vielzählige Anpassungsvorschläge beigetragen, die von den Security-Ansprechpartnern von MAN als sinnvoll erachtet wurden und integriert wurden. Die Kataloge wurden nach Abstimmung zwischen den betroffenen Partner im Projekt verwendet, um Risikoanalysen durchzuführen (siehe AP 2.4). Ferner wurden die Kataloge während der Projektlaufzeit um die Domäne Office-/Backend-IT erweitert. Die Kataloge orientieren sich dabei an aktuellen Standards und Empfehlungen wie ISO/IEC 27005:2022, BSI IT-Grundschutz-Kompendium und dem Security Pillar des AWS Well-Architected Framework. Die Kataloge wurden als notwendige Voraussetzung für die Erstellung der Security-Risikoanalyse zum Control Center in AP 2.4 erarbeitet. Im weiteren Projektverlauf wurden die Erkenntnisse, die während der Erstellung und Durchsprache der Security-Risikoanalyse zum Control Center gewonnen wurden, zurück in die Kataloge gebracht, um diese zu finalisieren. Beispielsweise wurde im Annahmen-Katalog vermerkt, welche Verantwortlichkeiten der Betreiber der Cloud-Infrastruktur und der Betreiber des Control Centers hinsichtlich Security übernehmen muss, oder im Maßnahmenkatalog Resilienz/Diversität für kritisch exponierte Control Center Komponenten ergänzt und hinsichtlich Wirksamkeit eingestuft.

Zudem wurden all diese Aspekte vollständig in ein MoRA-konformes Excel-Tool implementiert. Hierbei wurde ebenfalls die Performance, Übersichtlichkeit und Wartbarkeit des Excel-Tools durch die Implementierung von LET und LAMBDA Funktionen deutlich gesteigert. Darüber hinaus wurden kleinere Bugs im MoRA-Excel-Tool gefixt und es wurde um mehrere Sheets, bspw. zur automatisierten Generierung von PlantUML-Sequenzdiagramm-Input-Strings, erweitert. Dies erhöht gemäß Feedback von Projektpartnern die Übersichtlichkeit und Verständlichkeit der System-/Untersuchungsgegenstandsmodellierung. Ferner wurde die Methode den Safety-Experten des Konsortialpartners TU-Braunschweig präsentiert und Feedback aufgenommen.

Ebenfalls wurde der Stand der Wissenschaft und Technik bzgl. Security-Management und Security-Risikoanalysen für hoch- und vollautomatisierte Fahrzeuge ermittelt. Hierfür wurden systematische Literaturrecherchen durchgeführt und die ermittelte Literatur hinsichtlich Systemmodellen aus Security-Sicht, Methoden zur Security-Risikoanalyse sowie Angriffen und Schutzmaßnahmen miteinander verglichen. Die Ergebnisse wurden in einem wissenschaftlichen Paper festgehalten, welches erfolgreich bei der 21st escar Europe Konferenz in Hamburg (15.-16. November 2023) veröffentlicht https://doi.org/10.13154/294-10391) und einem breiten Konferenzpublikum präsentiert wurde. Bei der escar Europe Konferenz handelt es sich um die Top Automotive Security Konferenz, was sich auch an der Teilnehmeranzahl von über 350 Vertretern aus Wissenschaft und Industrie, z. B. von Volkswagen, BMW, CARIAD, MAN und Knorr-Bremse, zeigt. Die Paper-Akzeptanzquote lag bei knapp unter 25%.

### 3.2.2 Security Standards (AP 2.2)

Für die Ermittlung der relevanten, aktuell vorhandenen Security-Standards wurde eine Normensuche mit der Datenbank Nautos durchgeführt. Um möglichst alle relevanten Security-Standards zu ermitteln, wurde folgende Freitextsuche durchgeführt: (vehicle OR vehicles OR car OR cars OR automobile OR automobiles OR automotive OR truck OR trucks OR bus OR busses OR transportation OR logistics OR production OR road) AND (secure* OR *security OR cyber* OR encryption). Für die größten Standards der Bereiche Office-/Backend-IT (ISO/IEC 27000 Familie), Fahrzeugentwicklung (ISO/SAE 21434) und Produktion (IEC 62443 Serie) wurde ein detaillierter Standardvergleich durchgeführt. Hinsichtlich Terminologie wurden Gemeinsamkeiten und Unterschiede analysiert und ein Vorschlag für eine übergreifende Terminologie erarbeitet. Die Konzepte und Anforderungen der jeweiligen Standards wurden in Graphen dargestellt, um diese übersichtlich und verständlich darzustellen sowie bereichsübergreifende Anforderungen hervorzuheben. Die Ergebnisse wurden zusammen mit den Ergebnissen der Experteninterviews aus AP 2.3 in ein wissenschaftliches Paper mit dem Titel „Cross-Divisional Cybersecurity Risk Management in Automotive: Requirements and Current Practices“ überführt, welches bei der IEEE ETFA 2025 Konferenz veröffentlicht und einem breiten Konferenzpublikum präsentiert wurde [4].

Als Reaktion auf den rasanten digitalen Wandel des Automobilsektors und der damit einhergehenden Cybersicherheitsbedrohungen haben verschiedene Regionen regulatorische Rahmenwerke geschaffen, um die Cyber-Resilienz zu verbessern und Sicherheitspraktiken zu standardisieren. Während der Projektlaufzeit wurden drei prominente Ansätze in einer Studie verglichen: die rechtsverbindlichen Vorschriften der Wirtschaftskommission der Vereinten Nationen für Europa (UNECE), die chinesische Norm GB 44495-2024 und die freiwilligen Richtlinien der US-amerikanischen National Highway Traffic Safety Administration (NHTSA). Jedes Regelwerk wurde anhand von sechs Kriterien analysiert, darunter Geltungsbereich,

Zertifizierungsanforderungen, Cybersicherheitsmanagementstrukturen, Software-Update-Mechanismen, Risikominderungsstrategien und Überwachungspflichten. Einerseits zeigt die Studie wesentliche Unterschiede bei den Durchsetzungsmechanismen, der technischen Spezifität und den Zertifizierungsprozessen auf. Andererseits identifiziert sie gemeinsame Kernprinzipien wie risikobasiertes Lebenszyklusmanagement und sichere Update-Praktiken. Darüber hinaus identifiziert die Studie wichtige regulatorische Lücken, wie z. B. methodische Klarheit, inkonsistente Zertifizierungsansätze sowie Herausforderungen bei der Angleichung nationaler Praktiken, und bewertet deren operative Auswirkungen. Sie hebt auch hervor, wie benachbarte Vorschriften, darunter Datenschutzgesetze und horizontale digitale Gesetzgebung, zunehmend die Cybersicherheit von Fahrzeugen beeinflussen. Die Studie schließt mit gezielten Empfehlungen für verbesserte operative Leitlinien zur Stärkung der langfristigen Widerstandsfähigkeit im Automobilsektor. Die Ergebnisse sind detailliert im partnerspezifischen Schlussbericht des Fraunhofer AISEC beschrieben

Weiterhin wurde eine umfassende Analyse der aktuellen maschinellen Lernverfahren und infrastrukturellen Voraussetzungen für das automatisierte Fahren auf Level 4 durchgeführt. Dabei lag der Fokus darauf, wie die neuen Regularien des EU AI Acts den Einsatz dieser Technologien beeinflussen und welche Anpassungen möglicherweise erforderlich sind, um eine rechtskonforme Umsetzung sicherzustellen. Insbesondere wurden die Anforderungen an Risikomanagement, Datenverwaltung, Protokollierung, Transparenz und Sicherheit untersucht, da diese essenzielle Aspekte für den Betrieb von hochautomatisierten Fahrzeugsystemen darstellen. Ein zentraler Bestandteil der Analyse war die Identifikation der spezifischen Artikel des AI Acts, die für das ATLAS-L4-Projekt von Relevanz sind. Dazu gehörte beispielsweise die Einordnung von Level-4-Fahrfunktionen als Hoch-Risiko KI-Anwendung, wodurch besondere Anforderungen an die technische Robustheit und die Nachvollziehbarkeit der Entscheidungsprozesse gestellt werden. Zudem wurde überprüft, inwiefern bestehende Sicherheits- und Datenschutzmaßnahmen des Projekts den regulatorischen Anforderungen entsprechen oder ob zusätzliche Maßnahmen erforderlich sind. Basierend auf den gewonnenen Erkenntnissen wurden abschließend konkrete Handlungsempfehlungen formuliert, um eine AI-Act-konforme Umsetzung zu gewährleisten. Dazu zählen unter anderem mögliche Anpassungen der Trainings- und Evaluationsverfahren der zugrunde liegenden ML-Modelle sowie ergänzende Dokumentations- und Testverfahren, um die geforderte Transparenz und Nachvollziehbarkeit sicherzustellen.

Zudem wurden die Sicherheitsaspekte vernetzter Fahrzeugtechnologien im Nutzfahrzeugsektor untersucht, insbesondere im Hinblick auf Driver-Assistive Truck Platooning (DATP) und die damit verbundene Fahrzeug-zu-Fahrzeug-Kommunikation (V2V). Auch wurde die Anwendung von Post-Quanten-Kryptografie in den Bereichen V2V und In-Vehicle Kommunikation für autonom fahrende Lkw untersucht, um eine Grundlage für die Integration von PQC in Automotive Standards zu schaffen. Die Integration dieser Technologien zielt darauf ab, den Güterverkehr effizienter und sicherer zu gestalten, insbesondere durch die Reduzierung von Kraftstoffverbrauch und CO2-Emissionen sowie die Verringerung von Auffahrunfällen. Ziel ist es, die Sicherheit und Integrität der Kommunikationssysteme in autonomen Fahrzeugen zu gewährleisten, insbesondere im Hinblick auf die zukünftige Bedrohung durch Quantencomputer. V2V, Vehicle-to-Everything (V2X) und In-Vehicle Technologien sind entscheidend für autonom fahrende Lkw, da sie eine nahtlose Kommunikation zwischen Fahrzeugen, Infrastruktur und anderen Verkehrsteilnehmern ermöglichen. Um über V2X-Dienste zu informieren und einen Überblick zu gewähren, welche Anforderungen an eine sichere und

vertrauenswürdige V2X-Kommunikation bestehen, hat die Autobahn GmbH im Rahmen des AP 2 einen Online-Workshop veranstaltet. Die Autobahn GmbH ist Entwickler und Betreiber von V2X-Diensten, wie dem „Baustellenwarner“, der vernetzte Fahrzeuge über den Kommunikationsstandard ETSI IST G5 (basierend auf IEEE 802.11p) vor Tagesbaustellen warnt. Aktuell werden diese Nachrichten vom Fahrzeug empfangen und dem Fahrer im Bordcomputer als Warnmeldung dargestellt. Zukünftig könnten Dienste wie der „Baustellenwarner“ die Sensorik autonomer Fahrzeuge unterstützen: Gefahrenstellen können erkannt werden, noch bevor diese für die Sensorik sichtbar sind. Insgesamt wird durch V2X die Verkehrssicherheit und Effizienz erheblich erhöht und die Interoperabilität verschiedener Systeme und Hersteller hergestellt, was außerdem die Integration und Skalierbarkeit autonomer Technologien erleichtert. Die Einführung von Post-Quanten-Kryptografie ist in diesem Kontext besonders wichtig, da herkömmliche kryptografische Verfahren durch zukünftige Quantencomputer potenziell gebrochen werden könnten. Dies würde die Vertraulichkeit und Integrität der Fahrzeugkommunikation gefährden und somit die Sicherheit autonomer Lkw beeinträchtigen. Aus diesen Überlegungen leiten sich spezifische Anforderungen hinsichtlich der Sicherheit und Robustheit der Kommunikationsprotokolle ab. Diese Anforderungen bieten zusammen mit generischen Sicherheitsanforderungen eine Grundlage für die Auswahl geeigneter Post-Quanten-Kryptografie-Verfahren. Dafür wurde eine systematische Analyse der aktuellen Forschung und bestehender Lösungen durchgeführt, bei der sowohl die Effektivität als auch die Effizienz der verschiedenen Kryptografieansätze bewertet werden. Auch die aktuellen Ergebnisse der NIST-Standardisierung zur Post-Quanten-Kryptografie wurden berücksichtigt. Die Forschungsergebnisse sollen als Hilfestellung dienen, um die richtige Technologie für die zukünftige Implementierung in autonomen Fahrzeugen zu finden.

Im Paper mit dem Arbeitstitel "Confidentiality-protecting intelligent, Privacy-Preserving analysis of sensor data" werden verschiedene Use Cases in den Bereichen Industrial, Smart Home und Automotive vorgestellt. Aus diesen Use Cases leiten sich spezifische Anforderungen hinsichtlich des Schutzes von Privatsphäre und geistigem Eigentum ab. Diese bieten zusammen mit generischen Anforderungen, die unter anderem aus relevanten Standards extrahiert werden, eine Grundlage für die Auswahl von geeigneten Privacy Enhancing Technologies (PETs). Dafür wurde eine systematische Literaturrecherche durchgeführt, bei der bestehende Lösungen und noch offene Forschungsfragen diskutiert werden. Es wurde eine Auswahl der auf Eignung zu prüfenden PETs getroffen: Differential Privacy, Federated Learning, Attribute Based Encryption, Zero Knowledge Proofs, Homomorphic Encryption, Synthetische Daten und anonyme Authentifizierungstechniken. Die Forschungsergebnisse stellen eine Hilfestellung zum Finden der richtigen Technologie für zukünftige Use Cases dar. Jeder Use Case liefert individuelle Anforderungen an die Auswahl der PETs. Zudem wurden mögliche Anforderungen definiert wie bspw. Schutzziele, das funktionale Szenario, Umkehrbarkeit der PETs und Einfluss auf Performance und Architektur. Das Paper soll demnächst eingereicht und veröffentlicht werden.

Die Masterarbeit „Authenticated and fully distributed group key agreement for bus topologies“ befasste sich mit der Analyse der Anforderungen gängiger Busse (z.B. CAN-, Ethernet-Bus) und deren Ökosysteme für Group-Key-Agreement-Protokolle, sowie der prototypischen Entwicklung eines darauf angepassten Group-Key-Agreement Protokolls. Das Thema hat sich als sehr vielschichtig herausgestellt – keines der bisher in der Literatur spezifizierten Protokolle erfüllt die Anforderungen. Es wurde ein Prototyp auf Basis von Messaging Layer Security (MLS) aufgesetzt – dieses in RC9420 definierte Protokoll musste jedoch angepasst

werden. Insbesondere entfällt der Delivery Service, da dieser durch den Bus inhärent gegeben ist. Weiterhin mussten wir Anpassungen vornehmen, die leider die Skalierbarkeit von logarithmisch auf linear zurückwerfen. Außerdem sind Merge- und Split-Operationen noch nicht möglich. Die Masterarbeit wurde Ende 2024 erfolgreich abgeschlossen. Die Ergebnisse werden weiterbearbeitet und die wissenschaftlichen Erkenntnisse nachgeschärft. Eine Veröffentlichung ist angedacht.

Die aktuelle Position ist eine wichtige Eingangsgröße für ein autonomes Fahrzeug, sei es zum Überprüfen der ODD oder als Eingang in die Sensorfusion für Fahrentscheidungen. Meistens wird dabei GNSS/GPS als Grundlage verwendet. Eine Standortbestimmung per GNSS kann jedoch unter Umständen bis zu 17 Minuten dauern. Außerdem verfügt GNSS standardmäßig nicht über Maßnahmen, um die Authentizität der Nachrichten zu überprüfen, und kann folglich einfach gespooft werden. Entsprechend werden meist weitere Informationskanäle verwendet, um diesen Problemen zu begegnen. Eine Möglichkeit ist, per Assisted-GNSS (A-GNSS) über das Mobilfunknetz weitere Informationen wie Ephemeriden zu erhalten. Außerdem können WLAN-SSIDs mit Karten korreliert werden, um einen Standort abzuleiten. Da in der Regel jedoch nicht klar ist, wann ein Gerät welchen Dienst verwendet und welchen Einfluss das auf die Sicherheit hat, haben wir im Rahmen der Masterarbeit „Navigating the Risks: An Investigation into the Security of Location Services“ ein Testbed aufgebaut. Dabei wurden GPS und Mobilfunknetze per Software Defined Radio gespooft und der Netzwerkverkehr auf dem Gerät mitgeschnitten. Insgesamt wurden verschiedene Aspekte der Standortdienste von 10 Geräten untersucht, und es konnte so ein Ablauf für die Standortbestimmung in der Android-Blackbox abgeleitet werden.

Das Paper „Resilience Testing for TSN networks" stellt eine neue Architektur, sowie neue Mechanismen für Testverfahren für Time-sensitive networks (TSN) vor. Die entwickelnden Testverfahren testen Eigenschaften der Resilienz von Datenströmen in diesen Netzwerken und erlauben damit die Überprüfung zwischen erwartetem und tatsächlichem konfiguriertem Verhalten im Netzwerk. Die Systemarchitektur und Testverfahren finden Anwendung im Automobilsektor, sowie dem industriellen Sektor, welches die größten zu erwartenden Anwendungsbereiche für Time-sensitive networks sind. Eine Publikation zur Systemarchitektur, entwickelten Mechanismen sowie Testverfahren soll bald eingereicht werden.

In dem Paper „Efficient and secure embedded communication for smart manufacturing with Industrial Ethernet“ wurden die Sicherheitsherausforderungen von Industrial Ethernet (IE)-Protokollen in modernen, smarten Fertigungsumgebungen untersucht. Es wurden spezifische Schwachstellen in weit verbreiteten IE-Protokollen identifiziert, die insbesondere für kleine und mittelständische Unternehmen Risiken darstellen können. Durch eine Fallstudie zum IE-Protokoll EtherNet/IP wurde aufgezeigt, wie die Informationssicherheit in der Betriebstechnologie (OT) durch den Einsatz von Nachrichten-Authentifizierungscodes (MAC) zur Gewährleistung von Integrität und Authentizität in industriellen Netzwerken verbessert werden kann. Die Studie bewertet die Auswirkungen dieser kryptografischen Kontrollen auf die Kommunikationsleistung und demonstriert, dass kryptografische Operationen ohne signifikante Kompromittierung der Echtzeitanforderungen durchgeführt werden können. Die Ergebnisse bieten wertvolle Einblicke und praktische Lösungen zur Sicherung von eingebetteten industriellen Systemen und kann als Referenz für OT-Ingenieure dienen. Die Ergebnisse sind im partnerspezifischen Schlussbericht des Fraunhofer AISEC detaillierter beschrieben.

### 3.2.3 Prototypisches Werkzeug (AP 2.3)

Während der Projektlaufzeit wurde zwischen den beteiligten Partnern vereinbart, dass vom Fraunhofer-Institut AISEC zuerst ein initialer Prototyp für ein bereichsübergreifendes Security-Management aufgesetzt werden soll. Dies soll noch vor Bestimmung der funktionalen Anforderungen geschehen, um gegenüber MAN Mitarbeitenden bereits einen Mehrwert für ein bereichsübergreifendes Security-Management zu präsentieren. Anschließend soll damit an MAN Security-Verantwortliche aus verschiedenen Unternehmensbereichen herangetreten werden, um weitere funktionale Anforderungen zu erarbeiten. Hierfür wurde Microsoft SharePoint in Verbindung mit Microsoft Power Apps zur Formularanpassung sowie Microsoft Power Automate zur Workflow Erstellung als mögliche Entwicklungsumgebung für den initialen Prototyp evaluiert und als geeignet befunden. Die MoRA-Methode wurde zuerst in der SharePoint Listenfunktionalität abgebildet, um ein Grundgerüst für das Darstellen der Ergebnisse von Risikoanalysen zu bieten. Ein weiteres Feature von SharePoint ist die Active Directory Anbindung, die es ermöglicht, einzelne Risiken und Maßnahmen direkt an (Umsetzungs-)verantwortliche Mitarbeitende zuzuweisen. Neben der Arbeit an den Security-Risikoanalysen soll der Prototyp auch beim bereichsübergreifenden Security-Management, insb. beim Erfüllen von gesetzlichen Anforderungen und Standard-Richtlinien, unterstützen. Hierfür wurden die Anforderungen der drei großen Standards ISO/IEC 27001:2022, IEC 62443 und ISO/SAE 21434:2021 sowie der UN Regulation No. 155 extrahiert und als Elemente in den SharePoint Workspace aufgenommen.

Nachdem initial die MoRA-Methode als SharePoint Listenfunktionalität abgebildet wurde, wurde eine Anbindung entwickelt, mit der Ergebnisse einzelner Security-Risikoanalysen automatisiert in die Kollaborationsplattform überführt werden, um Vergleichbarkeit zwischen den Security-Risikoanalysen herzustellen und die Nachverfolgbarkeit und Weiterbehandlung der Ergebnisse zu verstärken.

Zur weiteren Ermittlung von Anforderungen wurde ein Leitfaden für semi-strukturierte Experteninterviews finalisiert, mit welchem Security-Experten von sechs verschiedenen Automobilherstellern zu Status-Quo, Umsetzbarkeit und Anforderungen sowie Chancen und Risiken von bereichsübergreifendem Security-Risikomanagement befragt wurden. In den Interviews wurde zudem das Basiskonzept für das prototypische Werkzeug validiert und mögliche zusätzliche Lösungsbausteine identifiziert. Die Ergebnisse der Befragungen wurden einerseits direkt im prototypischen Werkzeug berücksichtigt und andererseits in einem wissenschaftlichen Paper mit dem Titel „Cross-Divisional Cybersecurity Risk Management in Automotive: Requirements and Current Practices“ überführt, welches bei der IEEE ETFA 2025 Konferenz veröffentlicht und einem breiten Konferenzpublikum präsentiert wurde [4].

Darüber hinaus wurde das Projekt durch die Umsetzung benutzerfreundlicher Interfaces für das prototypische Werkzeug unterstützt. Dabei wurde die Konzeption unter Berücksichtigung relevanter Standards der Usability und Usable Security unterstützt. Dabei wurde ein Usability-Leitfaden für das Sharepoint-Tool für bereichsübergreifendes Risikomanagement aufgebaut. Dieser Leitfaden ist nach Gestaltungsempfehlungen und einer Dokumentation der Ergebnisse von durchgeführten Usability-Untersuchungen gegliedert. Im Rahmen der Gestaltungsempfehlungen wurden allgemeine Empfehlungen für die Gestaltung nutzendenfreundlicher Systeme in Form der 10 Usability-Heuristiken von Jakob Nielsen sowie der Prinzipien für Interaktionsgestaltung von Don Norman zusammengefasst und erläutert. Außerdem wurde das

Thema Barrierefreiheit aufgegriffen, kurz erläutert sowie einschlägige Empfehlungen hierfür genannt. Weiterhin wurden in den Gestaltungsempfehlungen spezifische Anforderungen für IT Security Management Tools anhand der „7 Heuristics for Evaluating IT Security Management Tools“ von Jaferian et al. (2011) beschrieben. Schließlich wurden die im Rahmen des Projekts durchgeführten Expertennterviews hinsichtlich Usability-Anforderungen untersucht und diese kategorisiert und erläutert. Für den zweiten Abschnitt des Leitfadens wurde ein initiales Experteninterview zum MoRA-Excel-Tool durchgeführt. Aus dem Interview abgeleitete Erkenntnisse und Empfehlungen wurden kategorisiert und im Leitfaden dokumentiert.

Methoden und Tools müssen nicht nur für das Risikomanagement während Design- und Entwicklungsphasen von autonomen Lkws eingesetzt werden, um holistische Security zu erreichen, sondern auch für Testphasen. Das Fraunhofer AISEC entwickelte in vorangegangenen Projekten ein öffentlich verfügbares und quelloffenes Testsystem für Steuergeräte in automobilen Fahrzeugen (https://github.com/fraunhofer-aisec/gallia) basierend auf dem herstellerübergreifenden Unified Diagnostic Services (UDS) Standard gemäß ISO 14229. Auf diesem Protokoll basiert auch das für Nutzfahrzeuge vorgeschriebene WWH-OBD Diagnoseprotokoll gemäß ISO 27145. Im Projekt wurden Beiträge zu diesem Testsystem erstellt, die künftig eine einfachere Automatisierung der Scans und Tests ermöglichen und damit eine einfachere Erweiterung der Testumfänge und einen effizienteren Testablauf ermöglichen. Dafür wurden umfangreiche Teile des Quelltexts erneuert. Darüber hinaus wurde auch der Umfang an unterstützen Transportprotokollen erweitert (FlexRay, DoIP). Weiterhin wurde die Unterstützung auf Windows-Betriebssysteme ausgeweitet. Zudem wurden auch die Tests an der Software überarbeitet und erweitert und Fehler im Quelltext identifiziert und behoben, um nachhaltig eine hohe Qualität sicherzustellen. Im Projekt wurde das System darüber hinaus auch funktional verbessert. Zudem wurden Teile der Ergebnisse in der Dissertation „Towards a More Sustainable and Secure Software Tooling in Free/Libre Open Source Software Environments" (https://doi.org/10.34961/18737) [5] -präsentiert, in welcher auf das ATLAS-L4 Vorhaben hingewiesen wurde.

Daneben hat das Fraunhofer AISEC seine Aktivitäten am Institut im Bereich C-ITS/V2X im Projekt vertieft. Auf Basis der bereits bestehenden Car2Car Communications Consortium Mitgliedschaft, wurde Zugang zu der ECTL Level 0 V2X Pilot PKI, betrieben durch Microsec, erlangt. Dies erlaubt das Ausstellen von validen OnBoard Unit (OBU) und Road Side Unit (RSU) Zertifikaten, die in weiteren Tests verwendet werden können. Dadurch kann Tooling entwickelt und weitergehend getestet werden, bzw. allgemeine Kompetenzen im Bereich V2X vertieft werden.

Mit der steigenden Komplexität von Software auf Steuergeräten in autonomen Lkws steigt auch die Anzahl an Schwachstellen. Dies macht ein frühes Erkennen von Schwachstellen essenziell. Das Integrieren von Analyse Tools in die Entwicklungs-Toolchain und Durchführen von Security Code Reviews bereits in der Implementierungsphase ist ein wichtiger Schritt, um hier rechtzeitig entgegenzuwirken. Das Fraunhofer AISEC hat deshalb den Modul-Baukasten Woodpecker (s.fhg.de/woodpecker) entwickelt, der öffentlich verfügbare „Static Application Security Testing“ (SAST) Tools bündelt und die Nutzbarkeit für eingebettete Systeme optimiert. Der Baukasten soll künftig veröffentlicht werden. Im Rahmen von ATLAS-L4 wurden Optimierungen für Woodpecker speziell für die Automotive Domäne vorgenommen. Eine große Herausforderung bei der Anwendung von SAST-Tools ist die große Anzahl an Falsch-Positiven Ergebnissen, die die Nutzbarkeit für große Code-Basen erschwert. Deshalb filtert und sortiert Woodpecker die Ergebnisse der Tools. Heuristiken hierfür wurden einerseits

anhand von synthetischen Test Suites erstellt und andererseits anhand von realen Software-Projekten. Hierfür wurden beispielsweise Security Software-Bibliotheken wie mbedTLS und SomeIP untersucht, die typischerweise im Fahrzeug verwendet werden. Zudem wurde die Unterstützung auf Windows-Betriebssysteme ausgeweitet, um die Verwendung für die üblichen Entwicklungsumgebungen anzupassen.

### 3.2.4 Durchführung Security-Risikoanalyse (AP 2.4)

Während der Projektlaufzeit wurde eine vollständige, umfassende Security-Risikoanalyse zum Automated Driving System des L4-concept Trucks erstellt. Dabei fanden iterativ mehrere Workshops zwischen Fraunhofer AISEC und MAN statt, in welchen der Scope definiert wurde, die Item Definition auf Grundlage von Interviews mit AP 3 Verantwortlichen erstellt wurde, die Damage Scenarios, Bedrohungen, Risiken und Gegenmaßnahmen präsentiert wurden sowie Feedback der AP 3 Verantwortlichen integriert wurde.

**Beschreibung des Untersuchungsgegenstands**: Das automatisierte Fahrsystem (Automated Driving System, ADS) besteht aus sieben Hauptkomponenten: Wahrnehmung/Perception, Vorhersage/Prediction, Planung/Planning und Steuerung/Control bilden den Regelkreis, der die Umgebungswahrnehmung und das autonome Fahren ermöglicht. Darüber hinaus überwacht das Systemmanagement/System Management den Zustand der ADS-relevanten Komponenten und leitet bei Bedarf Manöver mit minimalem Risiko (Minimum Risk Manoeuvres, MRM) ein. Außerdem stellt die Missionskontrolle/Mission Control die Kommunikation mit dem externen Kontrollzentrum/Control Center her. Schließlich zeigt ein bordeigenes HMI/onboardHMI Informationen für den Testfahrer oder Disponenten an.

Im Allgemeinen verläuft die Kommunikation zur Durchführung der dynamischen Fahraufgabe (Dynamic Driving Task DDT) wie folgt: Sensoren, Basisfahrzeugüberwachung und Kontrollzentrum übertragen Informationen über die Umgebung und das Fahrzeug an den Regelkreis. Der Regelkreis verarbeitet die Informationen und sendet Steuerbefehle an die Aktoren.

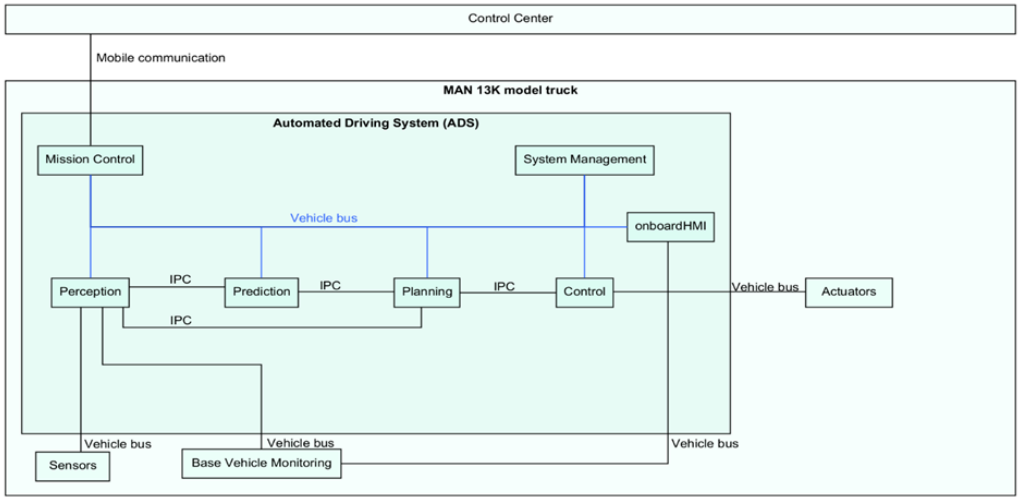



Abbildung 11 Komponentendiagramm des Automated Driving Systems

**Zusammenfassung der Ergebnisse:** Wenn es einem Angreifer gelingt, die Cybersicherheitseigenschaften Vertraulichkeit, Integrität oder Verfügbarkeit von Teilen des Bewertungsobjekts (TOE) zu verletzen, können 18 Schadensszenarien in den Auswirkungskategorien Sicherheit, Finanzen, Datenschutz und Betrieb verursacht werden. Beispiele mit hoher Auswirkungsbewertung sind DS1 Offenlegung von Videodaten, DS6 Verlust der ADS-Funktion während der Fahrt, DS12 Gefährliche Fahrmanöver, DS13 Aktivierung außerhalb von Operational Design Domain (ODD) und DS18 Offenlegung von Bewegungsprofilen einzelner Fahrzeuge.

Die Cybersicherheitseigenschaften des TOE werden durch insgesamt 216 Bedrohungsszenarien gefährdet, die sich aus einer Kombination von 84 Hauptangriffsschritten und 13 Vorbereitungsschritten zusammensetzen. Die Hauptangriffsschritte gefährden die Datenflüsse und Komponenten des TOE, während die Vorbereitungsschritte bestimmen, wie auf sie zugegriffen wird (z. B. physisch oder aus der Ferne) und durch welchen Angreifer (z. B. Fahrzeugbesitzer/Tuner oder externer Angreifer).

Die Bedrohungsszenarien werden einerseits durch 11 Annahmen behandelt, die entweder Schadensszenarien mindern oder transformieren oder sich auf die Bewertung der Angriffsmöglichkeiten auswirken. Die Anforderungen betreffen den Umfang der Analyse, z. B. A1 Angriffe auf das Control Center fallen nicht in den Umfang dieser Risikoanalyse, oder das Angreifer-Modell, z. B. A2 Begrenzter Umfang für Tuning-Angriffe. Darüber hinaus werden wichtige implementierungsrelevante Annahmen, die während der Entwicklung des TOE überprüft werden müssen, in Annahmen spezifiziert, z. B. A5 Domänentrennung, die angibt, an welchen Fahrzeugbus eine ferngesteuerte ECU angeschlossen ist, oder A10 MRM, ausgelöst durchs Control Center, sind nicht sicherheitskritisch.

Andererseits werden die Bedrohungsszenarien durch 20 Schutzmaßnahmen behandelt, die sich ebenfalls auf Schadensszenarien oder die Bewertung der Angriffsmöglichkeiten auswirken. Safety-Maßnahmen wie C1 Erkennung von Systemausfällen oder C4 Redundanz für sicherheitskritische Kommunikation von ADS-Kernkomponenten sowie Security-Maßnahmen wie C6 Authentische Datenübertragung oder C11 Denial-of-Service-Schutz für sicherheitskritische Komponenten sind erforderlich, um die Risikowerte auf ein akzeptables Niveau zu senken. Im Allgemeinen sind die Security-Maßnahmen für die sichere Speicherung und Übertragung von Daten sowie die Härtung von Fahrzeugkomponenten erforderlich.

Unter Berücksichtigung der Annahmen und Schutzmaßnahmen führt die Realisierung dieser Bedrohungsszenarien nur zu einem einzigen signifikanten Risiko. Das verbleibende Risiko mit dem Wert 3 R201 betrifft die Ausnutzung von Software-Schwachstellen auf Mission Control, dem Endpunkt für die externe Kommunikation. Im Rahmen dieser Risikoanalyse kann nicht ausgeschlossen werden, dass diese aus der Ferne zugängliche Komponente durch eine Software-Schwachstelle kompromittiert wird. Um die Wahrscheinlichkeit so weit wie möglich zu reduzieren, wird jedoch C18 Härtung gegen Fernangriffe vorgeschlagen, die eine robuste Implementierung von Software, die Einhaltung sicherer Codierungsrichtlinien, Sicherheits- (Penetrations-)Tests und Codeüberprüfungen umfasst. Selbst wenn es kompromittiert wird, verhindert C21 End-to-End-Signatur virtueller Sensordaten Safety-Schäden. Dies führt zu einem akzeptablem Restrisiko.

Die Ergebnisse der Security-Risikoanalyse zum Automated Driving System des L4-concept Truck wurden ebenfalls in dem in AP 2.1 genannten wissenschaftlichen Paper bei der escar Europe Konferenz 2023 veröffentlicht (https://doi.org/10.13154/294-10391) und präsentiert.

Die vollständige Security-Risikoanalyse wurde bereits auf der ATLAS-L4 Zwischenpräsentation an einem PC-Tisch ausgestellt und interessierten Besuchern demonstriert.

Zusätzlich wurden Cybersecurity Concept und Specification (MAN-spezifische Templates für die interne Weiterverwendung der Ergebnisse) zum Automated Driving System erstellt. Diese enthalten unter anderem ein Mapping der Security-Anforderungen aus der Risikoanalyse zu konkreten Security Controls bzw. Functional Requirement IDs von MAN. Die Security Controls wurden anschließend auf die umzusetzenden Komponenten/Steuergeräten heruntergebrochen und diesen zugeordnet.

Im Projekt konnte außerdem die Security-Risikoanalyse zum Control Center abgeschlossen und die Security-Anforderungen an MAN übergeben werden.

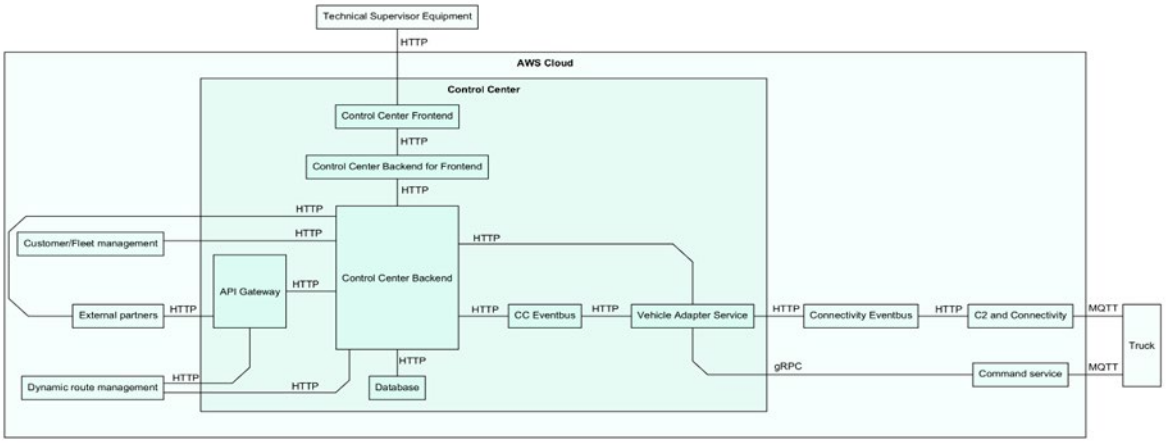



Abbildung 12 Komponentendiagramm des Control Center

**Zusammenfassung der Ergebnisse**: Wenn es einem Angreifer gelingt, die Cybersicherheitseigenschaften Vertraulichkeit, Integrität oder Verfügbarkeit von Teilen des TOE zu verletzen, können 19 Schadensszenarien in den Auswirkungskategorien Sicherheit, Finanzen, Datenschutz und Betrieb verursacht werden. Beispiele mit hoher Auswirkungsbewertung sind DS1 Offenlegung von Videodaten, DS9 Betrieb der Fahrzeugflotte nicht möglich, DS13s/DS13f Aktivierung außerhalb der ODD, DS15 Falsche Routenplanung für die Fahrzeugflotte und DS21 Falsche Auslösung eines MRM für die Fahrzeugflotte.

Die Cybersicherheitseigenschaften des TOE werden durch insgesamt 208 Bedrohungsszenarien bedroht, die sich aus einer Kombination von 89 Hauptangriffsschritten und 39 Vorbereitungsschritten zusammensetzen. Die Hauptangriffsschritte bedrohen die Datenflüsse und Komponenten des TOE, während die Vorbereitungsschritte bestimmen, wie auf diese zugegriffen wird (z. B. physisch oder aus der Ferne).

Die Bedrohungsszenarien werden einerseits durch 9 Annahmen behandelt, die entweder Schadensszenarien mindern oder transformieren oder den maximalen Risikowert begrenzen. Annahmen betreffen den Umfang der Analyse, z. B. A1 Angriffe auf den Lkw fallen nicht in den Umfang dieser Risikoanalyse, oder das Angreifer-Modell, z. B. A4 Begrenzte Störung des Mobilfunks. Darüber hinaus werden wichtige implementierungsrelevante Annahmen, die während der Entwicklung des TOE überprüft werden müssen, festgelegt, z. B. A10 Durch CC ausgelöste MRM sind nicht sicherheitskritisch.

Andererseits werden die Bedrohungsszenarien durch 16 Schutzmaßnahmen behandelt, die sich ebenfalls auf Schadensszenarien oder die Bewertung der Durchführbarkeit von Angriffen auswirken. Lkw-Safety-Maßnahmen wie C5A/C5I Intrinsische Sicherheit des Lkw oder C20 ADS-Sicherheitsvalidierungen nach Entscheidungen des Control Centers sowie Schutzmaßnahmen des Control Centers wie C18 Härtung von internetfähigen Komponenten gegen Software-Schwachstellen oder C23 Schutz vor Distributed-Denial-of-Service-Angriffen (DDoS) für internetfähige Komponenten sind erforderlich, um die Risikowerte auf ein moderates Niveau zu senken. Mit den Maßnahmen dieser Gruppen bleiben 44 Risiken mit einem Wert von 3 bestehen.

Um diese verbleibenden 44 Risiken auf ein akzeptables Niveau zu senken, d. h. ihren Risikowert auf höchstens 2, müssen weitere Schutzmaßnahmen implementiert werden: Ende-zu-Ende-Schutzmaßnahmen, nämlich C27 für die Verschlüsselung und C28 für die Authentifizierung, stellen sicher, dass selbst eine kompromittierte Komponente des Control Centers keine Nachrichten des Lkw lesen oder an diesen schreiben kann. Darüber hinaus erhöht C29 Resilienz/Sicherheit durch Vielfalt die Systemresilienz, sodass die Wahrscheinlichkeit, dass ein einzelner Exploit oder eine einzelne Schwachstelle das gesamte Control Center kompromittiert, verringert wird.

Unter Berücksichtigung aller Annahmen und Schutzmaßnahmen bleiben nur Risiken mit einem maximalen Wert von 2 übrig.

Die vollständigen Security-Risikoanalysen zum Control Center und zum Automated Driving System wurden bei der Abschlusspräsentation auf Bildschirmpräsentationen vorgestellt. Ferner wurden die Security-Risikoanalysen den Safety-Experten des Konsortialpartners TU-Braunschweig präsentiert und Feedback aufgenommen.

Darüber hinaus wurde ein 87-seitiges Cybersecurity Concept und eine Specification (MAN-spezifische Templates für die interne Weiterverwendung der Ergebnisse) zum Control Center er arbeitet und an MAN übergeben. Diese enthalten unter anderem ein Mapping der Security-Anforderungen aus der Risikoanalyse zu konkreten Security Controls bzw. Functional Requirement IDs von MAN. Die Security Controls wurden auf die umzusetzenden Komponenten heruntergebrochen und diesen zugeordnet.

Die Security-Risikoanalysen zum Automated Driving System und Control Center sind detailliert im partnerspezifischen Schlussbericht des Fraunhofer AISEC beschrieben.

### 3.2.5 AP 2 – Vortrag und Poster der Abschlusspräsentation

## AP2: SECURITY

**Security-Anforderungen müssen umfassend und nachvollziehbar ermittelt werden**

Security by Design:

- Ableitung von Anforderungen für sichere Systeme mittels Security-Risikoanalysen und Security-Testing
- Schutzkonzepte zur Erfüllung der Anforderungen für vollautomatisierte Lkw und Control Center

Security-Risikoanalysen:

- Erweiterung der etablierten Modular Risk Assessment (MoRA) Methode auf den Kontext vollautomatisierter Lkw
- Frühe Integration von Security in die neue Fahrzeugarchitektur und das Control Center
- Vermeidung von Sicherheitsvorfällen und negativen Auswirkungen sowie Erfüllung gesetzlicher Anforderungen

Security-Testing:

- Erweiterung des Pentesting-Frameworks Gallia
- Erweiterung des Security Code Review Tooling Woodpecker

ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Patrick Wagner (Fraunhofer AISEC) 18

## AP2: SECURITY

**Security muss holistisch während des gesamten Fahrzeuglebenszyklus berücksichtigt werden**

Security im Fahrzeuglebenszyklus:

- Ausgangslage:
  - Security-Standards und Regularien für einzelne Bereiche ohne Hilfestellung für bereichsübergreifende Aspekte
  - Heterogene Security-Prozesse in den Bereichen trotz vieler Schnittstellen
- Gefahr: Fehlende Identifizierung und Behandlung bereichsübergreifender Risiken
- Ergebnisse im Projekt:
  - Homogenes Security-Konzept mit Ende-zu-Ende Betrachtung von Risiken und Anforderungen
  - Übergreifender Vergleich und Bestimmung der Abhängigkeiten und Schnittstellen zwischen den Security-Standards
  - Anforderungserhebung, Konzepte und prototypisches Werkzeug für bereichsübergreifendes Security Risikomanagement


ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Patrick Wagner (Fraunhofer AISEC) 19

# SECURITY
## Übersicht

### MOTIVATION UND ZIELE

- Methoden für Security-Risikoanalysen ohne Berücksichtigung der spezifischen Gegebenheiten autonomer Lkws
- Security-Standards und Regularien für einzelne Bereiche ohne konkrete Hilfestellung für bereichsübergreifende Aspekte
- Heterogene Security-Prozesse in vielen (Unternehmens-) Bereichen trotz vieler Schnittstellen

→ Ermittlung vollumfänglicher und nachvollziehbarer Security-Anforderungen während des gesamten Fahrzeuglebenszyklus

### ARBEITSSCHWERPUNKTE

- **Methode Security Risikoanalyse:** Anpassung an Standards, Regulierungen und L4 Kontext, Implementierung in Excel-Tool
- **Security Standards:** Ermittlung und übergreifende Analyse, Ableitung von Handlungsempfehlungen
- **Werkzeug für bereichsübergreifendes Security Management:** Status Quo und Anforderungserhebung, Konzeption bereichsübergreifender Schnittstellen, prototypische Implementierung in SharePoint-Tool
- **Durchführung Security-Risikoanalyse:** Modellierung der Untersuchungsgegenstände, Bewertung von Damage Scenarios, Bedrohungen, Risiken und Schutzmaßnahmen


### ERGEBNISSE/HIGHLIGHTS

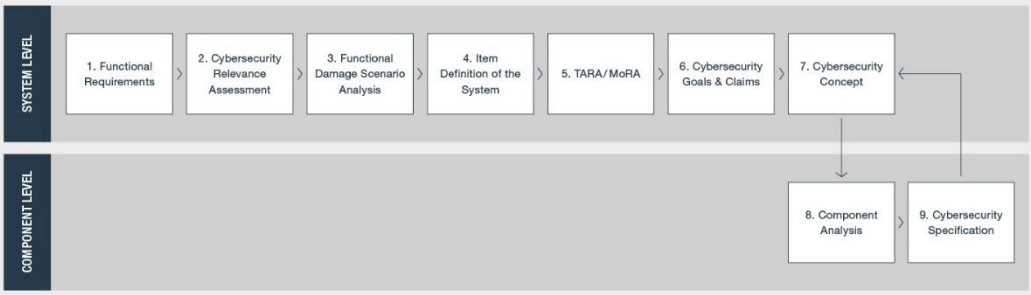
- UN Regulation No. 155 konforme Methode zur Security-Risikoanalyse mit kontextbezogenen Annahmen-, Bedrohungs- und Maßnahmenkatalogen
- Übergreifender Vergleich von ISO/SAE 21434, ISO/IEC 27000 Familie und IEC 62443 Reihe sowie Analyse weiterer Security Standards (PQC, AI/ML, Usability, ...)
- Anforderungsanalyse und -erhebung sowie Konzepte und prototypisches Werkzeug für bereichsübergreifendes Security Risikomanagement
- Security-Risikoanalysen und Schutzkonzepte zum L4 Automated Driving System und Control Center

# PROZESS UND METHODE ZUR SECURITY-RISIKOANALYSE

## Security

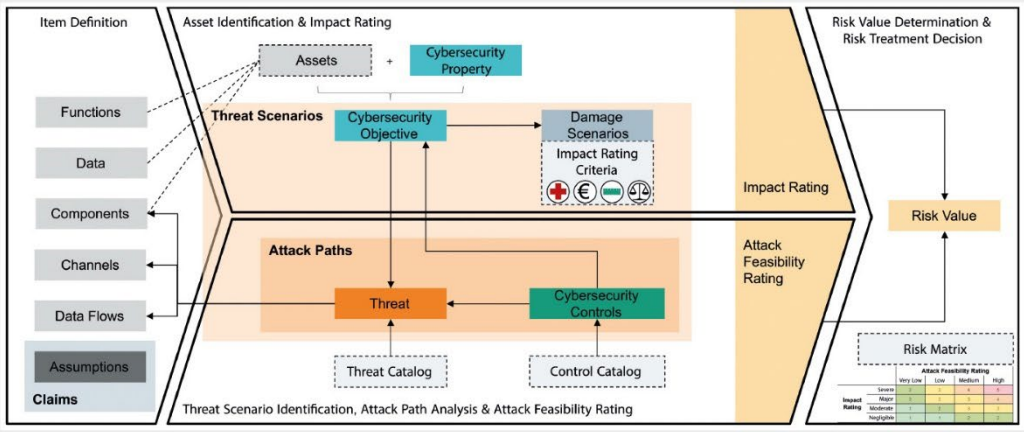
### UN REGULATION NO. 155 KONFORMER PROZESS

Das Prozessschaubild beschreibt die Darstellung von der Systembeschreibung mit funktionalen Anforderungen über die TARA bzw. MoRA bis hin zur Komponentenebene und den entsprechenden Cybersecurity Artefakten.




### MODULAR RISK ASSESSMENT (MORA) METHODE

Die MoRA Methode wurde den Projektanforderungen entsprechend erweitert.



# SECURITY STANDARDANALYSE UND -VERGLEICH

## Security

### MOTIVATION UND ZIELE

Automobilhersteller müssen viele Security Standards in Bereichen wie Engineering, IT und Produktion berücksichtigen, um Fahrzeuge und Insassen optimal zu schützen. Eine isolierte Betrachtung kann bereichsübergreifende Risiken übersehen. Daher wurden die Security Standards ganzheitlich analysiert und verglichen, um holistische Anforderungen, Bedrohungen und Risiken zu ermitteln.

**ISO/SAE 21434 Norm**

- Behandelt die Security bei der Entwicklung von **E/E-Systemen in Straßenfahrzeugen**
- Ermöglicht **Organisationen** die Definition von Security-Richtlinien und -Prozessen, das Management von Risiken und die Förderung einer Security-Kultur
- Dient der Implementierung eines **Cyber Security Management Systems (CSMS) & Risikomanagements**
- Systeme außerhalb des Fahrzeugs (z.B. Backend-Server) sind nicht abgedeckt
- 1 Norm aus 2021, die vom Interpretation Guide der UN Regulation No. 155 als besonders hilfreich für die Umsetzung ihrer Anforderungen bezeichnet wird

**ISO/IEC 27000 ISMS-Normenfamilie**

- Ermöglicht **Organisationen** die Entwicklung und Umsetzung eines Rahmens für die Security ihrer **Informationswerte** mittels **Risikomanagement**
- Bietet detaillierte Anleitungen für den Gesamtprozess zur Einrichtung, Umsetzung, Aufrechterhaltung und Verbesserung eines **Information Security Management Systems (ISMS)**
- Die Anforderungen der ISO/IEC 27001 sollen auf alle Organisationen anwendbar sein, unabhängig von Art, Größe oder Beschaffenheit
- ~100 verschiedene Normen, von Übersicht und Vokabular bis Leitlinien für spezifische Anwendungs-bereiche; die erste Norm wurde 2000 veröffentlicht

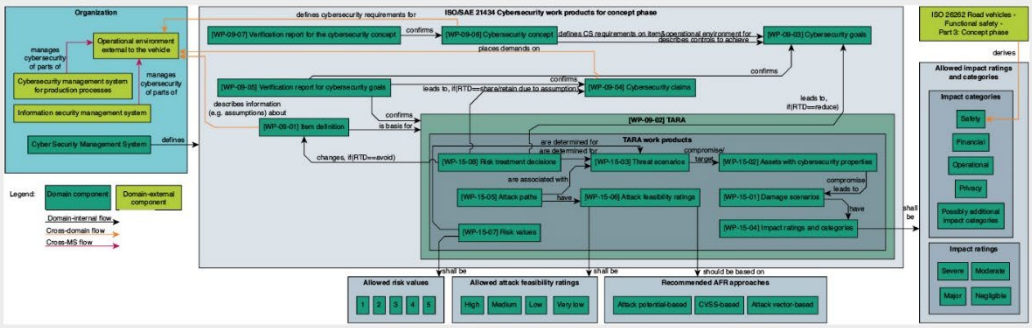
**IEC 62443 Normenreihe**

- Befasst sich mit der Security von **Industrial Automation and Control Systems (IACS)**
- IEC 62443-2-1 stellt Anforderungen an ein IACS **Security Program für Eigentümer** von IACS-Anlagen, das häufig durch **Koordination und Integration mit dem ISMS** der Organisation verbessert wird
- IEC 62443-3-2 leitet **Organisationen** beim **Risikomanagement** von IACS
- Einige Normen richten sich an Anlageneigentümer, Systemintegratoren und Produktanbieter von IACS, während andere bestimmte Gruppe ansprechen
- ~10 verschiedene Normen und technische Berichte; der erste technische Bericht wurde 2007 veröffentlicht

### Identifikation gemeinsamer, inkonsistenter und fehlender Terminologie

| 21434 TERM | 21434 DEFINITION | 27K TERM | 27K DEFINITION | 62443 TERM | 62443 DEFINITION |
|---|---|---|---|---|---|
| Risk | Effect of uncertainty on road vehicle cybersecurity expressed in terms of **attack feasibility** and **impact** | Risk Level of risk | Effect of uncertainty on objectives Significance of a risk, expressed in terms of the combination of **consequences** and their **likelihood** | Risk | Expectation of loss expressed as the **likelihood** that a particular threat will exploit a particular vulnerability with a particular **consequence** |
| **Attack path** | Set of deliberate actions to realize a threat scenario | **Risk scenario** | Sequence or combination of events leading from the initial cause to the unwanted consequence | **Threat vector** | Path or means by which a threat source can gain access to an asset |
| Cybersecu-rity claim | Statement about a risk (can include a justification for sharing the risk) | Risk sharing | Form of risk treatment involving the **agreed** distribution of risk with other parties | / | |
| / | | Residual risk | Risk remaining after risk treatment | Residual risk | Risk that remains after existing countermeasures are implemented |
| / | | Risk appetite | Amount and type of risk that an organization is willing to pursue or retain | Tolerable risk | Level of risk deemed acceptable to an organization |
| / | | / | | Security zone | Grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access or responsible organization |

### Überführung der Konzepte in Graphen und Identifikation bereichsübergreifender Anforderungen



# ANFORDERUNGSERHEBUNG UND -ANALYSE FÜR EIN BEREICHSÜBERGREIFENDES SECURITY-MANAGEMENT

Security

## MOTIVATION UND ZIELE

Um Status Quo, Anforderungen, Chancen und Risiken von bereichsübergreifendem Security-Risikomanagement in der Automobilindustrie zu erheben, wurden leitfadengestützte Interviews mit Security-Experten von sechs OEMs durchgeführt. Die Transkripte wurden mittels induktiven Codes ausgewertet.

| THEMEN | FRAGEN (AUSZUG) | INDUKTIVE CODES [HÄUFIGKEIT] (AUSZUG) |
|---|---|---|
| 1 Status Quo | 1.1 Existenz von Strategien | 1.1.4 Unklarheit oder fehlende Kenntnis über eine bereichsübergreifende Strategie [2]<br>1.1.5 Strategien existieren, sind aber nicht vollständig etabliert oder dokumentiert [2] |
| | 1.2 Einheitlichkeit und Abhängigkeit der Praktiken | 1.2.1 Homogenität innerhalb der Bereiche [5]<br>1.2.2 Heterogenität zwischen Bereichen/Managementsystemen [4] |
| | 1.3 Bereichsübergreifender Austausch und Zusammenarbeit | 1.3.5 Prozesse sind nicht vollständig implementiert oder es gibt Verbesserungsbedarf [2]<br>1.3.6 Claims werden nicht korrekt übertragen oder Backend wird nicht informiert [3] |
| | 1.4 Verwendete Methoden und Werkzeuge | 1.4.1 Unterschiedliche Tools/Methoden in den Bereichen [4]<br>1.4.4 Unterschiedliche Risikobewertungsmethoden (qualitativ vs. quantitativ) [2] |
| | 1.6 Existenz einer einheitlichen Terminologie | 1.6.1 Es gibt keine bereichsübergreifend einheitliche Terminologie [4] |
| 2 Umsetzbarkeit und Anforderungen | 2.1 Zu teilende Informationen und deren Vorteile | 2.1.1 Austausch von Risiken und Schwachstellen zwischen den Bereichen [4] |
| | 2.2 Bedingungen für das Teilen von Risikodaten | 2.2.1 Risikodaten werden geteilt, wenn sie für andere Bereiche relevant sind [4] |
| | 2.3 Methoden zum Vergleich von Risiken zwischen Bereichen | 2.3.1 Wichtigkeit einheitlicher Tools zur Gewährleistung der Vergleichbarkeit [3]<br>2.3.6 Einsatz standardisierter Risikomatrizen und Frameworks über die Bereiche hinweg [2] |
| | 2.6 Maßnahmen zur Verbesserung der Koordination | 2.6.1 Einführung zentraler Rollen/Verantwortlichkeiten, um die Koordination zu verbessern [3]<br>2.6.2 Etablierung von bereichsübergreifenden Teams oder Gremien, die den Austausch fördern [3] |
| | 2.8 Erfüllung von Vorschriften und Standards | 2.8.2 Koordinierte Interpretation und Umsetzung von Regulierungen und Standards [3] |
| 3 Chancen und Risiken | 3.1 Vorteile für das Unternehmen und einzelne Bereiche | 3.1.1 Besseres Risikomanagement / ganzheitlicher Blick auf Risiken [3]<br>3.1.2 Kosteneinsparung durch effizientere Ressourcenzuweisung [5]<br>3.1.5 Vereinfachte Entscheidungsfindung durch einheitliche Strategie [3] |
| | 3.3 Potenzielle Risiken oder Bedenken | 3.3.1 Informationsabfluss an Unbefugte [4]<br>3.3.3 Hohe Komplexität/Bürokratie bei Einführung des bereichsübergreifenden Risikomanagements [2]<br>3.3.5 Widerstand gegen Veränderungen und Silo-Denken [2] |


## KONZEPTION VON LÖSUNGEN UND INTEGRATION IN PROTOTYPISCHES WERKZEUG

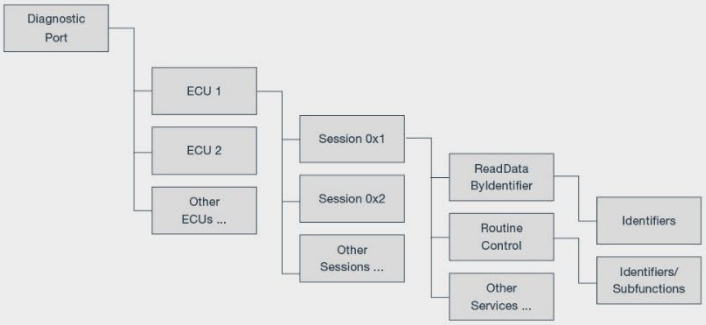
Basierend auf den Ergebnissen wurden Lösungen wie eine bereichsübergreifend-einheitliche Terminologie, Schnittstellen zum automatisierten Austausch von Risikodaten oder ein übergreifendes Risiko- und Maßnahmeninventar konzipiert und in das prototypische Werkzeug zum bereichsübergreifenden Security-Management integriert.

# SECURITY TESTING

## Security

### GALLIA: AUTOMOTIVE TEST TOOLING

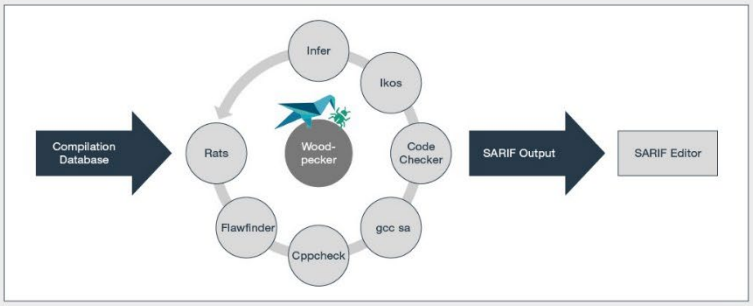
Das erweiterbare Open-Source Framework Gallia bietet Tools zum Testen von Fahrzeugen und Steuergeräten im Bereich der Automobilität, basierend auf herstellerübergreifenden Diagnosestandards (u.a. UDS, WWH-OBD). Gallia unterstützt dabei eine Vielzahl an Netzwerktechnologien und Transportprotokollen (u.a. DoIP) und bietet einen großen Umfang an Tools, vom gezielten Senden einzelner Diagnosebefehle, bis hin zu voll automatisierten Programmen zum Scannen verfügbarer Steuergeräte und deren Diagnosefunktionalität, wodurch potentielle Angriffsoberflächen identifiziert werden können.




| Service | Sess. 0x1 | Sess. 0x2 |
|---|---|---|
| ReadDataByIdentifier | √ | √ |
| ReadDTCInformation | √ | x |
| ClearDiagnosticInformation | √ | x |
| RoutineControl | √ | √ |

### WOODPECKER: SECURITY CODE REVIEW TOOLING

Der Modulbaukasten Woodpecker bündelt Open-Source-Tools zur Codeanalyse. Gepaart mit der Security-Kompetenz des Fraunhofer AISEC identifiziert er sicherheitskritische Schwachstellen. Einzelne Module des Baukastens wurden im Projekt erweitert, um Woodpecker für die Automotive Domäne zu optimieren. Anhand von im Fahrzeug üblichen Security Software-Bibliotheken (mbedTLS, SomeIP) wurden Heuristiken zum Filtern und Sortieren der Toolergebnisse angepasst. Weiterhin wurde die Unterstützung auf übliche Entwicklungsumgebungen ausgeweitet.



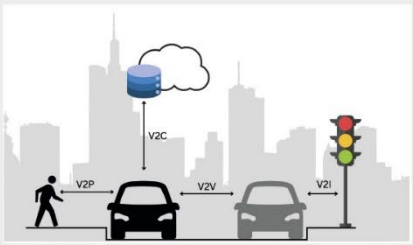
# SICHERHEIT VERNETZTER FAHRZEUGTECHNOLOGIEN IM NUTZFAHRZEUGSEKTOR DURCH POST-QUANTEN-KRYPTOGRAFIE (PQC)

Security

## MOTIVATION UND ZIELE

V2X und In-Vehicle Technologien sind entscheidend für autonom fahrende Lkw, da sie eine nahtlose Kommunikation zwischen Fahrzeugen, Infrastruktur und anderen Verkehrsteilnehmern ermöglichen.

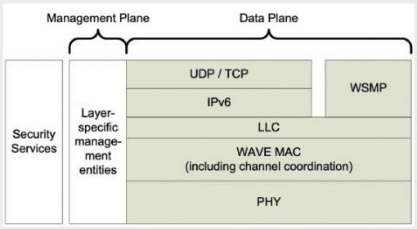
Die Integration von PQC in vernetzte Fahrzeugtechnologien ist entscheidend, um zukünftigen Bedrohungen durch Quantencomputer zu begegnen und die Sicherheit autonomer Nutzfahrzeuge zu gewährleisten.




## TOOLS: IEEE 1609.2 WIRELESS ACCESS IN VEHICULAR ENVIRONMENTS (WAVE)

WAVE ist ein Kommunikationsprotokoll, das für die sichere Datenübertragung in vernetzten Fahrzeugtechnologien entwickelt wurde.

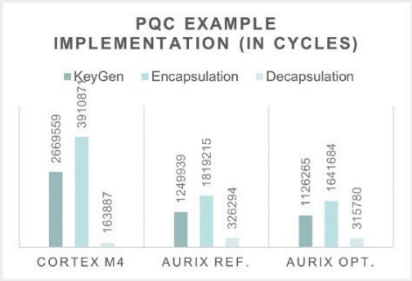
Dabei werden neben dem üblichen Protokollstack für Daten eine Reihe von Sicherheitsdiensten definiert, den sogenannten WAVE Security Services, die Kommunikation im V2X Bereich absichern.




## IMPLEMENTIERUNG: PQC IM V2X BEREICH

Es ist entscheidend, die Integration von NIST PQC-Primitiven in Protokolle und reale Systeme zu analysieren und die Eignung potenzieller zukünftiger Algorithmen zu prüfen.

Dafür wurden PQC-Algorithmen auf Microcontrollern, die im Automotive-Bereich eingesetzt werden, implementiert und gebenchmarkt. Dabei ist es essenziell, dass PQC-Algorithmen sicher und effizient eingesetzt werden können.



# AP 3: Funktionale Anforderungen

Lavinia Stollfuß; Dominik Anderle – MAN Truck & Bus SE

## 3.3 AP 3: Funktionale Anforderungen

*Arbeitspaketleitung: Lavinia Stollfuß; Dominik Anderle – MAN Truck & Bus SE*

### 3.3.1 Anforderungsanalyse der dynamischen Fahraufgabe (AP 3.1)

Im Rahmen von ATLAS-L4 wurde ein methodischer und technischer Beitrag zur modellbasierten, szenarienorientierten Entwicklung automatisierter Fahrsysteme erarbeitet. Der Schwerpunkt lag auf der Entwicklung formalisierter Modelle und Ontologien zur Beschreibung der Betriebsumgebung (Operational Design Domain, ODD) sowie des gewünschten Systemverhaltens. Ziel war es, Konzepte des Model-Based Systems Engineering (MBSE) an die spezifischen Anforderungen des sicherheitskritischen Kontexts des automatisierten Fahrens anzupassen und weiterzuentwickeln. Darüber hinaus wurde eine konkrete ODD und DDT erstellt, welche sowohl für das L4 Zielbild als auch in Abstufungen für den Testbetrieb im Rahmen der AFGBV-Freigabe dient.

#### Systematische Anforderungsanalyse und Grundlagenentwicklung

Zu Projektbeginn erfolgte eine enge arbeitspaketübergreifende Abstimmung zur Etablierung eines gemeinsamen Verständnisses zentraler Begriffe, insbesondere des Szenarienbegriffs. Basierend auf einer umfassenden Literaturrecherche wurden Anforderungen an die Verhaltensspezifikation systematisch erhoben und in ein initiales Konzept überführt. Dieses wurde als Ontologie ausgearbeitet und mit bestehenden Modellierungsansätzen (z. B. SysML) sowie der Beschreibung der ODD integriert, um eine durchgängige modellbasierte Repräsentation sicherheitsrelevanter Anforderungen zu ermöglichen.

Parallel dazu wurden normative und wissenschaftliche Quellen zur ODD ausgewertet. Dabei standen Terminologie, Repräsentationsformen, Klassifikationskriterien sowie potenzielle Anwendungsfälle im Fokus. Die Ergebnisse bildeten die Grundlage für nachfolgende konzeptionelle und technische Arbeiten im Projektverbund.

#### Entwicklung und Integration technischer Modelle

Im weiteren Projektverlauf wurden aufbauend auf der Anforderungsanalyse drei Ontologien entwickelt: zur Beschreibung der ODD, zur Spezifikation des Sollverhaltens sowie zur Modellierung temporaler und kausaler Zusammenhänge innerhalb von Szenarien. Diese Ontologien ermöglichen eine formale und strukturierte Beschreibung von Szenen und deren Verknüpfung zu Szenarien, einschließlich der zugehörigen Anforderungen und Handlungsmöglichkeiten für automatisierte Fahrsysteme.

Ein zentrales Ergebnis war die Implementierung eines Szenario-Graphen, mit dem sich – ausgehend von einer definierten Startszene – mögliche Handlungsverläufe gemäß der spezifizierten Anforderungen analysieren lassen. Die zugrundeliegenden Konzepte wurden in einem wissenschaftlichen Fachartikel (IEEE Access) veröffentlicht [6].

Zur technischen Umsetzung wurde ein Architekturframework zur durchgängigen Systemmodellierung entwickelt [7]. Dieses unterstützt die Modellierung der ODD und des Systemverhaltens in SysML. Erste exemplarische Modelle wurden mit CATIA Magic Cyber-Systems Engineer umgesetzt. Die teilweise automatisierte Generierung von SysML-Diagrammen stellt einen Zwischenschritt hin zu einer vollintegrierten Toolchain dar, die für weiterführende Sicherheitsanalysen genutzt werden kann.

### Szenarien- und fähigkeitsbasierte Datensatzentwicklung

Ergänzend zu den Modellierungsarbeiten wurde ein methodischer Rahmen zur datengestützten Entwicklung sicherheitskritischer Systeme unter Verwendung maschineller Lernverfahren erarbeitet. Im Zentrum stand ein szenarienbasierter Ansatz zur Erstellung, Analyse und kontinuierlichen Verbesserung von Datensätzen, der sich an bestehenden Normen wie ISO 26262, ISO/TR 4804 und ISO/PAS 8800 sowie an V&V-Methoden orientiert.

Ein besonderer Fokus lag auf der Verknüpfung funktionaler, logischer und konkreter Szenarien mit Anforderungen an Datenqualität und Sicherheit. So ermöglichen funktionale Szenarien – als narrativ beschriebene Zielzustände innerhalb der ODD – eine strukturierte Ableitung sicherheitsrelevanter Anforderungen. Diese können etwa aus HARA-Ergebnissen oder regulatorischen Vorgaben abgeleitet werden.

Logische Szenarien dienen der formalen Parametrisierung relevanter Umwelt- und Systemattribute. Mithilfe etablierter Modelle (z. B. 6-Ebenen-Modell) kann die Szenarioraumabdeckung der Datensätze analysiert und durch kombinatorisches Testen quantitativ bewertet werden. Auf dieser Grundlage wurden Methoden zur Identifikation und Reduktion von Verzerrungen (Bias) im Datensatz entwickelt – ein bislang wenig adressiertes Thema im Bereich des automatisierten Fahrens.

Die Operationalisierung konkreter Szenarien erlaubt eine durchgängige Rückverfolgbarkeit einzelner Datenpunkte entlang definierter Sicherheitsanforderungen – sowohl bei realer als auch bei synthetischer Datenerfassung (z. B. durch Simulation oder gezielte Augmentierung). Diese Rückverfolgbarkeit ermöglicht eine automatisierte Analyse von Datensätzen hinsichtlich Szenarioabdeckung und potenzieller Verzerrungen. Zudem kann über Zielverteilungen für relevante Parameter (z. B. Wetter, Tageszeit, Infrastrukturelemente) ein Abgleich mit der tatsächlichen Verteilung erfolgen, um systematisch Korrekturmaßnahmen einzuleiten.

Auch im Trainings- und Validierungsprozess eröffnen szenarienbasierte Methoden neue Möglichkeiten. Seltene, aber sicherheitskritische Szenarien können gezielt gewichtet, Modellschwächen systematisch identifiziert und durch gezielte Datenerweiterung adressiert werden. Damit entsteht ein geschlossener Qualitätsregelkreis zwischen Datensatzentwicklung, Modelltraining, Validierung und Nachbesserung.

Insgesamt wurde ein übertragbarer methodischer Rahmen zur sicherheitsorientierten Datensatzentwicklung etabliert, der eine explizite Rückverfolgbarkeit zu Sicherheitszielen erlaubt. Erste Ergebnisse dieses szenarien- und fähigkeitsbasierten Ansatzes wurden auf einer Fachkonferenz vorgestellt [8], ein weiterführender Artikel ist in Vorbereitung.

### Definition der ODD

Basierend auf dem Pegasus-6-Ebenen-Modell wurde eine ODD-Datenbank mit der zugehörigen ODD-Taxonomie erstellt und im Rahmen der AFGBV-Freigabe konkret für den Testbetrieb verwendet. Dabei wurden auch Aspekte bzgl. möglicher Sicherer Zustände im Zuge eines MRM zwischen den verschiedenen Projektbeteiligten abgestimmt.

### Spezifikation des Sollverhaltens des L4-Fahrzeugs innerhalb der ODD

Um das Sollverhalten des L4 Fahrzeugs innerhalb der ODD festzulegen, wurden in erster Linie die möglichen Fahrmanöver/ Fähigkeiten des Fahrzeugs, als auch die äußeren Einflussgrößen (Infrastruktur …) identifiziert und im Rahmen einer Item Definition spezifiziert.

Dies erfolgte in Form eines Szenarienkatalogs, welcher die Nominal-Szenarien beschreibt und auch in den Safety Prozess integriert ist. Ferner wurde auch das sichere Sollverhalten beschrieben.

**Dissemination und wissenschaftlicher Austausch**

Die erzielten Ergebnisse wurden sowohl durch Veröffentlichungen in IEEE Access als auch durch Diskussionen auf Fachkonferenzen wie der safetronic disseminiert. Der Austausch mit Fachvertreterinnen und -vertretern aus Industrie und Wissenschaft trug zur Validierung und Weiterentwicklung der entwickelten Konzepte bei.

**Zusammenfassung**

Im Arbeitspaket 3.1 wurden zentrale methodische und technische Grundlagen zur modellbasierten, szenariengestützten Entwicklung automatisierter Fahrsysteme gelegt. Die entwickelten Ontologien, Modellierungsansätze und datenbezogenen Methoden bilden eine tragfähige Grundlage für zukünftige Entwicklungs- und Absicherungsprozesse im Bereich des hochautomatisierten Fahrens. Durch die Integration formaler Verhaltensmodelle, normkonformer ODD-Beschreibungen und sicherheitsgerichteter Datensatzentwicklung wird ein systematischer und nachvollziehbarer Entwicklungsansatz ermöglicht.

Darüber hinaus wurden wesentlich der ODD und DDT konkret erstellt und auch im Rahmen der AFGBV-Freigabe in der Praxis erprobt.

### 3.3.2 Systemsicherheit FuSi & Sotif (AP 3.2)

Im Rahmen von Arbeitspaket 3.2 wurden über mehrere Projektphasen hinweg wesentliche Beiträge zur Entwicklung sicherer automatisierter Fahrsysteme geleistet. Im Mittelpunkt standen die Erstellung einer normenkonformen Item Definition, die Entwicklung eines Verhaltenssicherheitskonzepts sowie die Integration dieser Arbeiten in modellbasierte Entwicklungsansätze.

Dabei wurde für die konkrete Umsetzung der verschiedenen Arbeitsprodukt neben dem L4 Zielbild auch der Testbetrieb berücksichtigt und entsprechende Sicherheitskonzepte erstellt. Diese Konzepte wurden in Zusammenarbeit mit anderen APs in die verschiedenen Prototypen-Fahrzeuge implementiert.

**Erstellung einer normenkonformen Item Definition**

Die Arbeiten begannen mit der Analyse relevanter Normen, insbesondere ISO 26262:2018 (Funktionale Sicherheit) und ISO 21448 (Safety of the Intended Functionality, SOTIF). Auf dieser Grundlage wurde ein konzeptioneller Rahmen zur Erstellung einer Item Definition entwickelt. Dieser umfasste zentrale Inhalte wie:

- Beschreibung des Anwendungsfalls
- Definition der Betriebsmodi
- Abgrenzung der funktionalen Systemgrenzen
- Identifikation relevanter Abhängigkeiten zu anderen Systemen und Items
- Strukturierte Domänenbeschreibung
- Spezifikation des Sollverhaltens

Zur Ausarbeitung des Konzepts wurden interne Workshops sowie Erkenntnisse aus früheren Projekten (z. B. aFAS, UNICAR*agil*, VVMethoden) einbezogen. Der resultierende Entwurf wurde im Konsortium vorgestellt, diskutiert und im Folgejahr finalisiert. Dabei wurden erste operationelle und funktionale Anwendungsfälle sowie Betriebsmodi für das Zielsystem („Ghost-Truck“) definiert. Die Domänenbeschreibung wurde mithilfe modellbasierter Methoden systematisch strukturiert.

**Entwicklung eines Konzepts zum Risikomanagement spezifizierten Verhaltens**

Ein zentrales Ziel war die Entwicklung eines Verfahrens zur Risikobewertung, das explizit das spezifizierte Sollverhalten unter gegebenen Betriebsbedingungen berücksichtigt. Aufbauend auf einer umfassenden Literaturstudie, auch aus Domänen wie der Luftfahrt, und den Anforderungen der genannten Normen wurde ein methodisches Konzept erarbeitet, das die Beschreibung und Analyse geschätzter Risiken innerhalb spezifischer Szenarien ermöglicht. In einer ersten Fallstudie kamen zudem Ergebnisse aus dem Projekt VVMethoden zum Einsatz. Die Ergebnisse wurden in einem wissenschaftlichen Artikel veröffentlicht (IEEE Access) [9].

**Risikoanalyse und Definition der Sicherheitsziele und sicheren Zustände**

Bei den Risikoanalysen war ein wesentliches Ziel die verschiedenen Sicherheitsnormen wie die Funktionale Sicherheit (ISO 26262) und SOTIF (ISO 21448) kombiniert durchzuführen, um eine effiziente Erstellung zu gewährleisten und konkurrierende Anforderungen zu vermeiden. Hierfür wurde ein entsprechender Ansatz, welcher auf den vorhergehend Beschriebenen Erkenntnissen aufbaut, entwickelt. Dieser wurde sowohl für den L4 Betrieb als auch für den Testbetrieb durchgeführt.

**Erweiterung der Sicherheitsanalysen um Aspekte der Teleoperation**

Teleoperation wurde als ergänzender Anwendungsfall im Kontext funktionaler Sicherheit untersucht. In einer exemplarischen Anwendung auf ein Logistikzentrum wurden sicherheitsrelevante Aspekte, insbesondere im Hinblick auf Verbindungsabbrüche, analysiert. Eine auf realen Daten basierende Simulation zeigte potenzielle Gefährdungen infolge verzögerter Reaktionen auf Kommunikationsstörungen. Die Resultate wurden in einem wissenschaftlichen Beitrag zusammengefasst, dessen Veröffentlichung für Ende 2025 vorgesehen ist.

**Bewertung von Bestandsfunktionalitäten und deren Sicherheitskonzepte (ASC)**

Auf Grund des Projektziels ein Dual-Mode-Fahrzeug zu entwickeln, wurde es erforderlich neben den „neuen“ L4 Funktionen auch die bestehenden Funktionalitäten des Basis-Fahrzeug, sowie deren Absicherung und Weiterverwendbarkeit für den L4 Betrieb zu betrachten. Hierfür wurde eine spezifische Methodik namens ASC entwickelt und durchgeführt.

**Entwicklung eines modellbasierten Verhaltenssicherheitskonzepts**

Zur strukturierten Dokumentation von Annahmen, Entwurfsentscheidungen und Risiken wurde das in Arbeitspaket 5 entwickelte modellbasierte Architekturframework eingesetzt. Auf dieser Grundlage wurde ein formaler, modellgestützter Ansatz zur Spezifikation eines Verhaltenssicherheitskonzepts entwickelt. Ziel war unter anderem die Harmonisierung der Terminologie aus der ISO 21448 mit bestehenden Konzepten aus der ISO 26262 und IEC 61508.

Zu diesem Zweck wurden erweiterte Begrifflichkeiten eingeführt, darunter Verhaltenssicherheitsanforderungen und Verhaltenssicherheitskonzept. Aktuell befindet sich ein zugehöriger Fachartikel in Vorbereitung [10].

Ein möglicher Anwendungsfall des Verhaltenssicherheitskonzept findet sich im Genehmigungsverfahren für autonome Fahrfunktionen. Bei der Betriebsbereichsgenehmigung findet ein Abgleich zwischen den Fähigkeiten des Fahrzeugs (ODD) mit den Bedingungen im Betriebsbereich (Target OD) statt. Das Verhaltenssicherheitskonzept kann die Zusammenarbeit bei der Risikobewertung verbessern, da statt der technischen Hintergründe die verkehrlichen Auswirkungen im Vordergrund stehen und so eine „gemeinsame Sprache" zwischen Straßenbetreiber und Hersteller geschaffen werden kann.

**Weitere Veröffentlichungen zu FuSi & SOTIF**

In Kooperation mit dem Deutschen Zentrum für Luft- und Raumfahrt (DLR) wurde ein weiterer Beitrag konzipiert, der die Systemheoretische Prozessanalyse (STPA) auf Basis einer Verhaltensspezifikation für SOTIF-Anwendungen operationalisiert [11].

Im Projektkontext ausgearbeitete Empfehlungen zur Spezifikation von Sicherheitsanforderungen werden in einer Dissertation [12] veröffentlicht.

**Ableitung des Sicherheitskonzepts zur Absicherung des L4-Betriebs (inkl. Testbetrieb)**

Ein wesentlicher Bestandteil der Entwicklung des Dual-Mode-Fahrzeugs ist die Ableitung eines geeignetes Sicherheitskonzepts, welches den fahrerlosen Betrieb absichert. Hierbei wurde ein integrativer Ansatz verfolgt, bei dem neben der ISO 26262 auch die Anforderungen bzgl. SOTIF und weiterer relevanter Standards berücksichtigt werden.

Dabei galt es geeignete Sichere Zustände für die diversen Fehler zu definieren und im Rahmen des MRMs einen entsprechenden Sicheren Zustand des Gesamtfahrzeugs in Form des MRC zu erreichen. Hierfür wurde eine Bewertung des Gesamtsystems mittels diverser Sicherheitsanalysen, wie der FTA (ISO 26262) oder der CTA (SOTIF) durchgeführt.

Ferner wurde eine Systemarchitektur erstellt, welche sowohl die Aspekte der Nominalfunktion als auch die sicherheitsspezifischen Aspekte adressiert.

Für die Umsetzung des Sicherheitskonzepts wurde ein mehrstufiger Ansatz zur Erreichung des Sicheren Zustands gewählt. Im 1. Schritt gilt es den Sicheren Zustand des jeweiligen Systems zu erreichen. Dies erfolgt u. a. durch die Implementierung von Redundanz, wie beispielsweise der Umschaltung von Primär- zu Sekundärlenksystem. In diesem Kontext wurden diverse Redundanzkonzepte von der Sensorik bis zur Aktorik erarbeitet und in diversen Prototypen getestet. Im 2. Schritt erfolgt die Überführung in die MRC durch Ausführung eines geeigneten MRMs.

Darüber hinaus wurde ein separates Sicherheitskonzept inkl. der zugehörigen Sicherheitsanalysen für den Testbetrieb mit Sicherheitsfahrer erstellt und im Rahmen der AFGBV-Freigabe in Prototypenfahrzeugen implementiert.

**Zusammenfassung**

Arbeitspaket 3.2 liefert zentrale Beiträge zur Entwicklung sicherer automatisierter Fahrsysteme. Mit der normkonformen Item Definition, dem szenarienbasierten Risikomanagement, der Integration teleoperativer Anwendungsfälle und dem modellbasierten Verhaltenssicherheitskonzept wurden zentrale Bausteine für die Weiterentwicklung des Sicherheitslebenszyklus geschaffen. Die entwickelten Methoden und Modelle bilden eine tragfähige Grundlage für zukünftige Absicherungs- und Freigabestrategien und eine normgerechte Systementwicklung im Kontext hochautomatisierter Fahrfunktionen.

Zahlreiche Konzepte wurden in Abstimmung mit anderen APs in verschiedenen Prototypen implementiert und bildeten einen wesentlichen Anteil für die Straßenfreigabe des Testbetriebs.

### 3.3.3 Selbstüberwachung (AP 3.3)

Im Projekt ATLAS-L4 erwies sich vor allem das Konzept der Self-Awareness von besonderer Bedeutung. Um ein vollständiges Begriffsverständnis dieses Konzepts zu entwickeln, wurde im Projekt eine umfangreiche Literaturanalyse umgesetzt. Auf Basis dieser Analyse konnten relevante Definitionen rund um die Begriffe Selbstwahrnehmung, Self-Awareness und auch Selbstadaptivität entwickelt werden.

Insbesondere die Implikationen der Self-Awareness auf sogenannte Cyber-physischen System (also Systeme, die mit der physikalischen Welt interagieren – so auch Fahrzeuge) hatte dabei eine besondere Bedeutung. Einen wesentlichen Beitrag hatte auch die Analyse benötigter Überwachungsaufgaben im Kontext eines manuell geführten sowie eines automatisierten Fahrzeugs verschiedener SAE-Level. Letztlich wurde im Projekt die Fokussierung auf drei wesentliche Self-Awareness-Aspekte unternommen: die Generierung von Wissen über den eigenen Systemzustand, die Bewertung der aktuellen eigenen Fähigkeiten des Systems und das Treffen von Entscheidungen unter Unsicherheit. Die dabei nötigen Überwachungsmechanismen innerhalb des technischen Systems, die es erlauben, das Wissen über diesen eigenen Systemzustand zu gewinnen, wurden untersucht. Ein Anhaltspunkt war insbesondere die Architektur des Systems selbst. Hierbei entstanden Anforderungen an die Schnittstellen von Funktionen im System, die es erlaubten, relevante Informationen, die einen Einblick in den Systemzustand gewähren, abzurufen. Die Erhebung von Anforderungen an die Architektur automatisierter Fahrzeuge stellte sich im Projekt als eine der zentralen Notwendigkeiten im Kontext dieses Arbeitspaketes dar, die auch mit anderen, am AP beteiligten Partnern diskutiert wurde.

Auch wenn dies nicht mehr im Rahmen der Projektlaufzeit gelungen ist, so wird im Nachgang des Projekts angestrebt, die verschiedenen Erkenntnisse zur Self-Awareness, terminologische Erkenntnisse sowie insbesondere die Anforderungen an die Architektur eines automatisierten Fahrsystems mit Self-Awareness zu veröffentlichen. Ein konkreter Zeitschriftenbeitrag befindet sich derzeit in Arbeit und wird finalisiert. Mit einer zukünftigen Einreichung bei einer Fachzeitschrift wird gerechnet. Wie im Kürzungsantrag ausgeführt, konnten aufgrund von personellen Engpässen abseits dessen einige Aspekte gemäß Vorhabenbeschreibung im Projekt nicht geleistet werden. Die Zuwendungssumme wurde entsprechend gekürzt.

### 3.3.4 Rückfallebene für die Bewegungsplanung (AP 3.4)

Als Rückfallebene für kritische Ereignisse ist beim autonomen Fahren das sogenannte Minimum Risk Manoeuvre (MRM) vorgesehen, bei dem das Fahrzeug an einer möglichst sicheren Stelle anhält. Um die gemeinsame Strategie für ein MRM zu entwickeln, wurden zunächst gemeinsam mit dem AP 1 die gesetzlichen Anforderungen ermittelt. In § 1d Absatz StVG sind folgende Anforderungen beschrieben:

„Risikominimaler Zustand im Sinne dieses Gesetzes ist ein Zustand, in dem sich das Kraftfahrzeug mit autonomer Fahrfunktion auf eigene Veranlassung oder auf Veranlassung der Technischen Aufsicht an einer möglichst sicheren Stelle in den Stillstand versetzt und die Warnblinkanlage aktiviert, um unter angemessener Beachtung der Verkehrssituation die größtmögliche Sicherheit für die Fahrzeuginsassen, andere Verkehrsteilnehmende und Dritte zu gewährleisten."

Die Ausgestaltung dieser Anforderungen ist eine gemeinsame Aufgabe zwischen Hersteller und Straßenbetreiber.

Nach Auffassung der Autobahn GmbH sind die möglichst sicheren Stellen auf Autobahnen in Abstufung von sicher zu unsicher:

- Rastanlage/Parkplatz
- Nothaltebucht/Seitenstreifen
- Seitenstreifen an einer Autobahn, auf der die „Temporäre Seitenstreifenfreigabe (TSF)" grundsätzlich existiert, aber gerade nicht aktiv ist

Eine wichtige Grundlage für das MRM stellt zudem die Norm ISO/FDIS 23793-1 „Intelligente Verkehrssysteme – Not-Halt-Assistent für das automatisierte Fahren" dar. In der Norm werden drei verschiedene Arten von MRM definiert:

1. Halt auf dem Seitenstreifen
2. Halten im Fahrstreifen
3. Direkter Halt

Der Halt auf dem Seitenstreifen ist aus verkehrstechnischer Sicht das sicherste der drei Manöver und ist daher vorzuziehen. Voraussetzung für dieses Manöver ist allerdings, dass sowohl die Lenkung als auch die für einen Fahrstreifenwechsel notwendige Sensorik noch funktionstüchtig bzw. verfügbar ist. Wenn aufgrund ausgefallener Sensorik ein Fahrstreifenwechsel nicht mehr möglich ist, muss gemäß der Norm auf das Halten im Fahrstreifen zurückgegriffen werden. Im Falle eines Ausfalls der Lenkung muss der direkte Halt, also das Verzögern bis in den Stillstand ohne Korrekturmöglichkeiten der Fahrtrichtung durchgeführt werden.

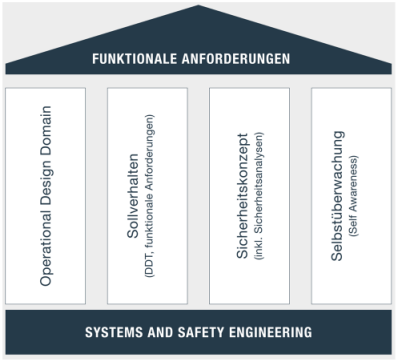
### 3.3.5 AP 3 - Vortrag und Poster der Abschlusspräsentation

## AP3: FUNKTIONALE ANFORDERUNGEN

**Übersicht**

**Wesentliche Inhalte:**

- AP 3.1 Anforderungsanalyse der dynamischen Fahraufgabe
- AP 3.2 Systemsicherheit FuSi & SOTIF
- AP 3.3 Selbstüberwachung
- AP 3.4 Rückfallebene für die Bewegungsplanung




**Beteiligte Projektpartner:**

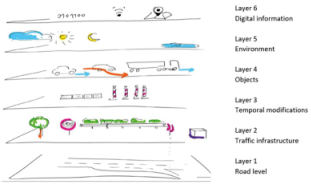
- Autobahn GmbH
- TU Braunschweig [diverse Fachvorträge]
- MAN Truck & Bus mit TU München und CLEAR MOTIVE GmbH im Unterauftrag

ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Dominik Anderle, Clear Motive GmbH 20

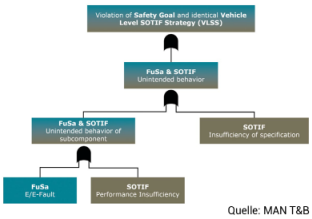
## AP3: FUNKTIONALE ANFORDERUNGEN

**Inhalte und Ergebnisse**

- ODD-Datenbank mit ODD-Taxonomie basierend auf Pegasus 6-Schichten-Modell
- Systematische Beschreibung der Dynamischen Fahraufgabe (DDT) mittels Szenarien
- Szenarienbasierte Gefahrenanalyse und Risikobewertung für SAE L4 autonomen LKW
- Systemübergreifendes Sicherheitskonzept für L4 Betrieb inkl. zugehöriger FuSa & SOTIF Sicherheitsanalysen
- Sicherheitskonzept für den Testbetrieb der L4-Funktion im Rahmen der AFGBV-Freigabe




Quelle: PEGASUS METHOD



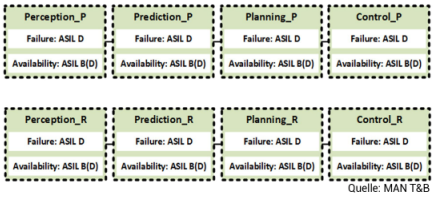

Quelle: MAN T&B

ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Dominik Anderle, Clear Motive GmbH 21

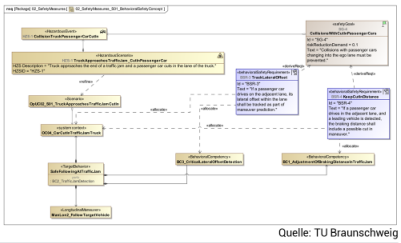
## AP3: FUNKTIONALE ANFORDERUNGEN

**Inhalte und Ergebnisse**

- Erstellung einer dem Sicherheitskonzept entsprechenden Systemarchitektur inkl. notwendiger Redundanzen
- Verifikation der System Architektur mittels Sicherheitsanalysen
- Erstellung eines Self-Awareness Konzepts [TUB]
- Szenarien basierte Sicherheitsanalysen auf Basis einer nachverfolgbaren Verhaltensspezifikation [TUB]
- Modellbasierter Ansatz für Verhaltenssicherheitskonzepte [TUB]



Quelle: MAN T&B

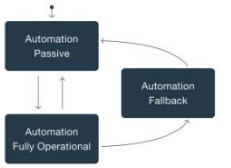

Quelle: TU Braunschweig



## AP3: FUNKTIONALE ANFORDERUNGEN

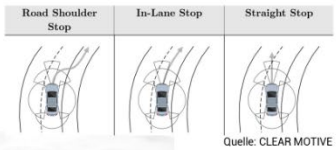
**Inhalte und Ergebnisse**

- Erstellung eines Sicherheitskonzepts für die Rückfallebene der Bewegungsplanung
- Integration der Perspektive des Straßenbetreibers in das Verhaltenssicherheitskonzept & MRM inkl. Fehlerquellen



Quelle: MAN T&B

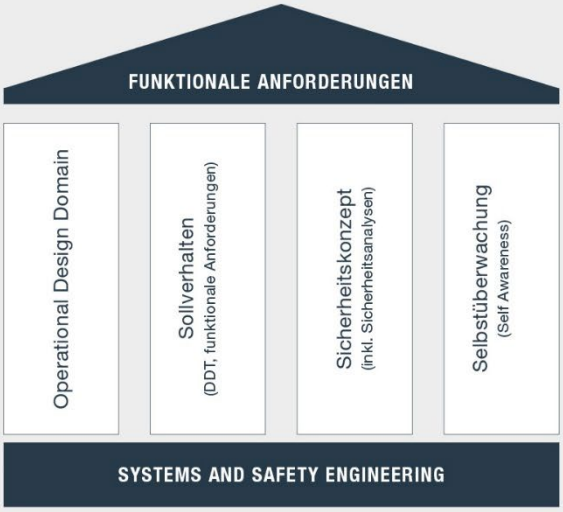
- Einige Ansätze bzw. Lösungen finden sich bereits in den Fahrzeugen auf der Teststrecke oder Autobahn (und können erlebt werden …)
- Sowie den anderen Demonstrator-Fahrzeugen wieder



Quelle: CLEAR MOTIVE

# FUNKTIONALE ANFORDERUNGEN
## Übersicht

### ÜBERSICHT DER THEMENFELDER ZUR FORMULIERUNG FUNKTIONALER ANFORDERUNGEN




### ERGEBNISSE

- Item Definition
- Beschreibung der ODD-Attribute gemäß festgelegter Taxonomie (Pegasus-Level)
- Analyse möglicher Fahrstrecken hinsichtlich deren ODD-Merkmalen
- Definition und Auswahl funktionaler Szenarien, sowie Erstellung der DDT
- HARA
- Detaillierung der Architektur bzgl. Basisfahrzeug, Redundanz-Pfaden und AV-Stack
- Dekompositions- und Redundanz-Konzepte inkl. Beschreibung der Rückwirkungsfreiheit
- Sicherheitskonzept für L4 inkl. Minimum Risk Maneuver (MRM)-Konzept
- Begleitende Sicherheitsanalysen (z.B. FTA / Fehlerbaumanalyse)
- Analyse und Konzept zu Gesetzesvorgaben im Kontext von Überwachungsaufgaben
- Modellbasierter Ansatz für Sicherheitsanalysen
- Konkretisierung der Verhaltensspezifikation nach ISO 21448 (SOTIF)
- Konzipierung und exemplarische Umsetzung eines Verhaltenssicherheitskonzepts
- Untersuchung der Verhaltensspezifikation und des Verhaltenssicherheitskonzepts für die Betriebsbereichsgenehmigung
- Erweiterung der STPA zur systematischen Identifikation auslösender Umstände (SOTIF)

# ODD & FUNCTIONAL SCENARIOS
# Anforderungsanalyse der dynamischen Fahraufgabe
## Funktionale Anforderungen

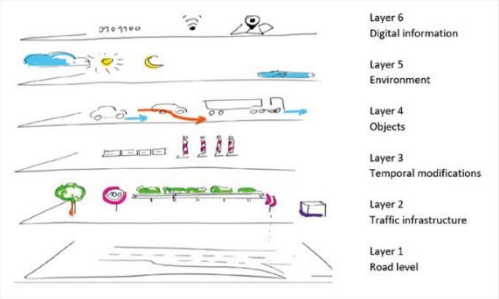
### MOTIVATION UND ZIELE

Die Operational Design Domain (ODD) und funktionale Szenarien sind wesentliche Voraussetzungen für die Entwicklung von autonomen LKW (L4). Die ODD definiert die Betriebsbedingungen, unter denen ein bestimmtes Automatisierungssystem sicher funktionieren soll. Funktionale Szenarien werden aus der ODD abgeleitet und beschreiben die Abfolge von Szenen, in denen sich das autonome Fahrzeug befinden kann. Diese funktionalen Szenarien stellen die Grundlage für die Definition des erwarteten Fahrzeugverhaltens dar.

Quelle: PAS 1883:2020

### ARBEITSSCHWERPUNKTE

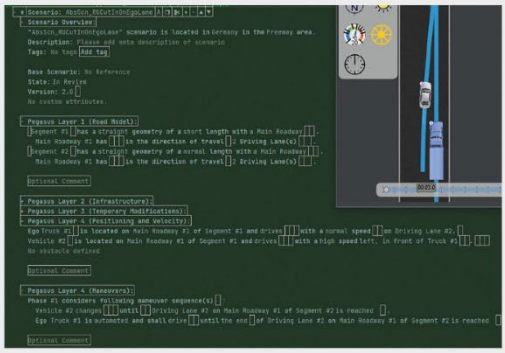
- Konzepte und Modellierung der ODD-Taxonomie
- Definition der ODD-Attribute für die Betriebs-bereiche
- Methodik zur Erstellung funktionaler Szenarien
- Erstellung funktionaler Szenarien gemäß der Methodik
- Modellierung der funktionalen Szenarien in einem maschinenlesbaren Format




Quelle: PEGASUS METHOD

### ERGEBNISSE/HIGHLIGHTS

- ODD-Datenbank mit ODD-Taxonomie basierend auf Pegasus 6-Schichten-Modell
- Modell zur Beschreibung der ODD (OWL, SHACL)
- Funktionaler Szenarienkatalog (Nominal -Szenarien) gemäß der Methodik
- Szenarienkatalog im maschinenlesbaren Format (.json oder .xosc)
- Integration der Ergebnisse in den Safety-Prozess

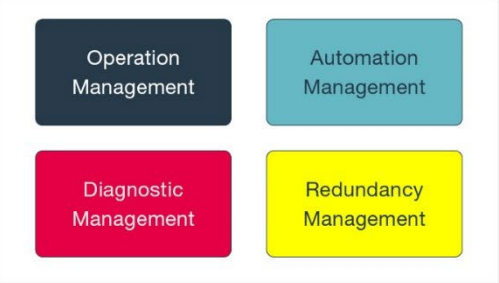


Quelle: MAN

# SYSTEM MANAGEMENT UND MRM
# Systemsicherheit FuSi & SOTIF
## Funktionale Anforderungen

### MOTIVATION UND ZIELE

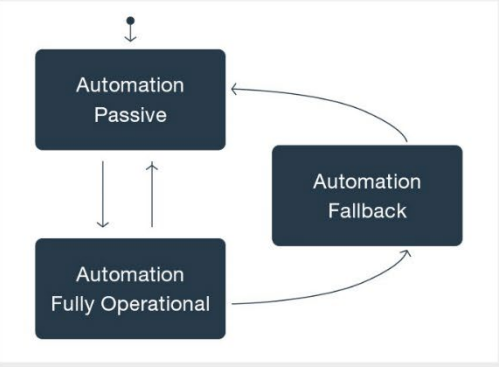
Basierend auf den Risikoanalysen, den abgeleiteten Sicherheitskonzepten und den gültigen Normen ergibt sich die Notwendigkeit das Fahrzeug im Falle eines entsprechenden Fehlers in einen möglichst sicheren Zustand zu versetzen.
Hierbei gilt es eine Menge von geeigneten „Minimum Risk Maneuvers“ (MRMs) zu definieren, welche das Fahrzeug – abhängig von verbleibenden Restfähigkeiten, sowie der aktuellen Umweltbedingungen und Fahrsituation – in einen geeigneten sicheren Zustand bzw. eine „Minimum Risk Condition“ (MRC) überführen.




Quelle: MAN T&B

### ARBEITSSCHWERPUNKTE

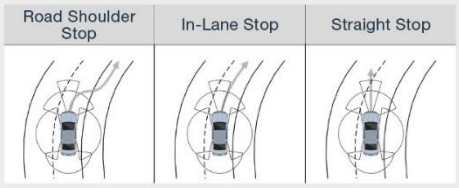
- Methodik zur Ermittlung des relevanten bzw. kritischen Fehlverhaltens
- Methodik zur Ermittlung der Restfähigkeiten des Fahrzeugs
- Analyse geeigneter MRM (auch unter Berücksichtigung baulicher Gegebenheiten)
- Konzept zur Überwachung und Steuerung des Gesamtsystems hinsichtlich
  - Betriebsmodi
  - Redundanzsystemen
  - Notwendiger Strategieanpassungen




Quelle: MAN T&B

### ERGEBNISSE/HIGHLIGHTS

- Konzept zur Erreichung des jeweils optimalen MRM
- Konzept für systemübergreifendes System Management (auch in Fahrdemos erlebbar)
- Abstimmung mit dem Straßenbetreiber




Quelle: CLEAR MOTIVE

# MODELLBASIERTES SICHERHEITSKONZEPT FÜR EINE SICHERE SOLLVERHALTENSSPEZIFIKATION

## Funktionale Anforderungen

- ISO 21448 gibt keinen konkreten Rahmen für die Spezifikation sicheren Sollverhaltens.
- Ein Verhaltenssicherheitskonzept (BSC) bündelt SOTIF-relevante Arbeitsprodukte: Gefährdungen, gefährliche Ereignisse, Sicherheitsziele, Sicherheitsanforderungen.
- Zusätzlich strukturiert es die zu erreichende Risikominderung und entsprechende Maßnahmen im Sollverhalten mithilfe von Verhaltenskompetenzen.
- Die Risikodekomposition (s. Abb. 1) ermöglicht eine explizite Berücksichtigung von Risikoakzeptanzkriterien.

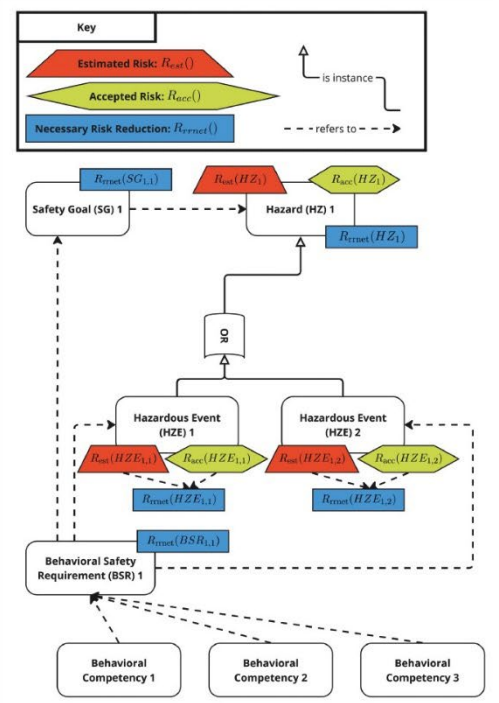



Abb. 1: Risikodekomposition innerhalb eines Verhaltenssicherheitskonzepts

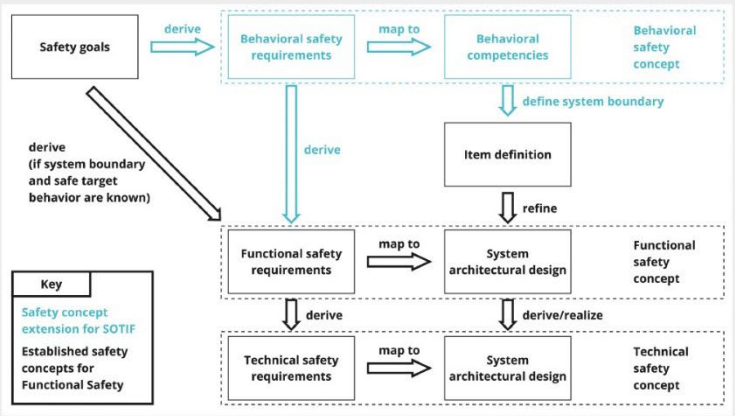



Abb. 2: Erweiterung bestehender Sicherheitskonzepte durch das Verhaltenssicherheitskonzept (Schema nach ISO 26262)

- Das BSC erweitert bestehende Sicherheitskonzepte der ISO 26262 (s. Abb. 2).
- Ein modellbasierter Ansatz unterstützt dabei die Kontrolle über die Komplexität betrachteter Szenarien (s. Demo am Monitor).

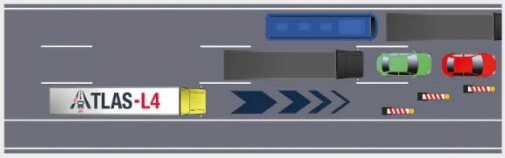
*Quelle: N. F. Salem, M. Nolte, R. Graubohm, O. Franke,T. Schenkel, und M. Maurer, „Towards a Model-based Approach for Behavioral Safety Concepts in Automated Driving," 2025, to be published.*

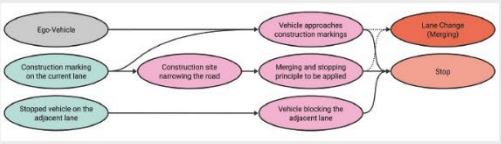
# AUTOMATISIERTE FAHRZEUGE MIT SELF-AWARENESS

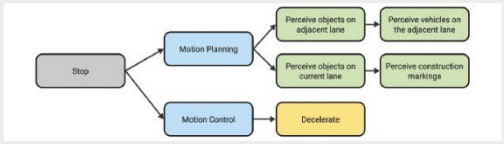
## Funktionale Anforderungen

### MOTIVATION UND EINFÜHRUNG

Automatisierte Straßenfahrzeuge operieren unter einer Reihe von Unsicherheiten sowie internen und externen Störeinflüssen, welche die Fähigkeiten der Systeme beeinflussen. Systeme mit *Self-Awarenesss* sind u. a. in der Lage, ihre eigenen Fähigkeiten zu bestimmen und situationsgerecht zu bewerten. Daraus können zur Laufzeit angemessene Entscheidungen abgeleitet werden.



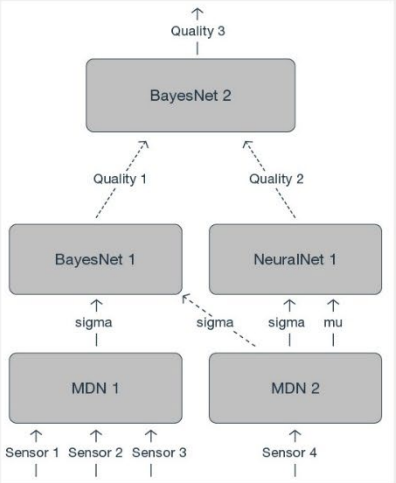

### ZENTRALE PROJEKTERGEBNISSE

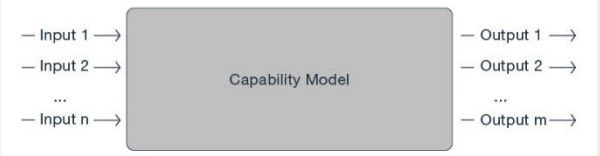
**Erarbeitung eines Konzepts für automatisierte Fahrzeuge mit Self-Awareness**

- Safety Engineering: Basis ist die Sollverhaltensspezifikation, welche zulässige Handlungsentscheidungen in repräsentativen Szenarien analysiert
- Festgelegte Performanzkritierien für die Fähigkeiten des Systems dienen als „Sollwerte" für die Selbstwahrnehmung (engl. Self-Perception) des Systems

**Entwicklung eines Self-Perception-Frameworks**

- Nutzung von ODD-Definition, Systemwissen und zusätzlichen Analysen zur Identifikation relevanter Einflussfaktoren auf die Fähigkeiten
- Entwicklung eines Software-Frameworks zur Modellierung der vielschrittigen Abhängigkeiten zwischen diesen Faktoren und relevanten Performanzgrößen




*Quelle: Cedrik Kaufmann, „Integration von experten- und datenbasierten Ansätzen in ein Framework zur Laufzeitüberwachung automatisierter Fahrzeuge", Masterarbeit, TU Braunschweig, 2023*

# SICHERHEITSBETRACHTUNG VON VERBINDUNGS-ABBRÜCHEN VON FERNGELENKTEN FAHRZEUGEN

## Funktionale Anforderungen

### MOTIVATION UND EINFÜHRUNG

Ferngelenkte Fahrzeuge benötigen zur Steuerung eine Verbindung zu einem Leitstand. Gegenwärtig gibt es keine Garantie, dass diese Verbindung nicht zwischenzeitlich ausfallen kann. Ferngelenkte Fahrzeuge müssen daher für den Fall eines Verbindungsabbruchs mit einem Rückfallmechanismus ausgerüstet sein. Da ferngelenkte Fahrzeuge nicht notwendigerweise über eine automatisierte Fahrfunktion verfügen müssen, ist dieser Rückfallmechanismus häufig eine direkte Bremsung.

### ZENTRALE ERGEBNISSE

Selbst in alltäglichen Szenarien reicht der Rückfallmechanismus der einfachen Bremsung nicht aus, um unzumutbares Risiko zu vermeiden. Wir zeigen dies durch:

**Simulation des Rückfallmechanismus auf Grundlage von natürlichen Fahrdaten**

- Bremsen als Rückfallmechanismus wird mit Hilfe eines realen Datensatzes bei einer Folgefahrt simuliert.
- Das Bremsverhalten des/der Folgefahrers/Folgefahrerin wird anhand von Bremsverhaltensmustern modelliert, um potenzielle Kollisionen zu erfassen.
- Die Simulation zeigt, dass für das simulierte Szenario eine **hohe Wahrscheinlichkeit** für eine Kollision besteht.

**Konzeptuelle Risikobewertung**

- Durch eine konzeptuelle Risikobewertung auf der Grundlage der ISO 21448 wird gezeigt, dass bei einer Folgefahrt selbst bei niedrigen Geschwindigkeiten ein **relevanter Schaden** entstehen kann.


*Inhalte und Grafiken nach „Safety Blind Spot in Remote Driving: Considerations for Risk Assessment of Connection Loss Fallback Strategies" von Leon Johann Brettin, Niklas Braun, Robert Graubohm und Markus Maurer; Preprint: https://arxiv.org/abs/2502.10243*

# AP 4: Test- und Validierungsmethoden

Dr. Tino Teige, BTC Embedded Systems AG

## 3.4 AP 4: Test- und Validierungsmethoden

*Arbeitspaketleitung: Dr. Tino Teige, BTC Embedded Systems AG*

Klassische Testansätze werden zur Freigabe von Level-4-Fahrzeugen aufgrund der enormen Anzahl zu testender Verkehrssituationen, was mehreren Milliarden Testkilometern in der Realität entspricht, nicht mehr ausreichend sein. Daher wird angestrebt, den Großteil dieser Testfahrten in einer Simulationsumgebung zu virtualisieren, da solche Tests in einer virtuellen Simulationsumgebung schneller und mit deutlich weniger Aufwand (und Risiko für Leib und Leben) umsetzbar sind.

Das Arbeitspaket AP4 befasste sich mit solchen simulativen Testansätzen zur Gesamtfahrzeugverifikation und Sicherheitsvaliderung von Level-4-Lkws.

Die Arbeitsschwerpunkte in AP 4 waren

- die Entwicklung von Testkonzepten für die Gesamtfahrzeugverifikation und die Sicherheitsvalidierung von Level 4-Fahrfunktionen,
- die Ableitung von Testfallkatalogen für die Gesamtfahrzeugverifikation und die Sicherheitsvalidierung,
- der Einsatz von szenarienbasierten, simulativen Testmethoden für die Verifikation und Validierung,
- die Validierung der Simulation auf dem Prüfgelände sowie
- die Durchführung relevanter Testfälle zur Freigabe von Demonstrationsfahrzeugen

In den nächsten Unterkapiteln werden die Ergebnisse dieser Arbeitsschwerpunkte dargestellt.

### 3.4.1 Erstellung eines Testkonzepts für die Gesamtfahrzeugverifikation und die Sicherheitsvalidierung (AP 4.1)

In AP 4.1 wurde die Erstellung eines Testkonzept zur Gesamtfahrzeugverifikation und Sicherheitsvalidierung automatisierter Fahrzeuge wissenschaftlich untersucht und basierend darauf ein prototypisches Testkonzept zur Sicherheitsvalidierung der Softwarekomponente zur Trajektorienplanung des Automated Driving Systems von MAN entwickelt[3], welche als exemplarisches Testobjekt im AP 4 diente. Der Fokus lag dabei auf dem Thema Sicherheit (engl. Safety) im Sinne der funktionalen Sicherheit (gemäß ISO 26262) sowie des sicheren Sollverhaltens (gemäß ISO 21448, SOTIF). Andere Aspekte wie Funktionalitäten, Angriffssicherheit (engl. Security) oder Leistungsfähigkeit waren planmäßig nicht Bestandteil der Arbeiten.

[3] Abweichend zur Vorhabenbeschreibung wurde im Konsortium und in Absprache mit dem Projektträger beschlossen, dass nicht das Demonstrationsfahrzeug getestet werden soll (als Basis für die Freigabe des Demonstrationsfahrzeugs für den öffentlichen Straßenverkehr), sondern der Fokus auf die Erforschung von Ansätzen für die Sicherheitsvalidierung der Trajektorienplanung des Automated Driving Systems von MAN, da hier der größte Forschungsbedarf identifiziert wurde und sich die Entwicklung des Demonstrationsfahrzeugs deutlich verzögert hat. Dies führte während der Projektlaufzeit zu einer entsprechenden Anpassung der ursprünglich erarbeiteten Inhalte des Testkonzepts.

Zu Beginn der Arbeiten wurde eine umfassende Literaturrecherche durchgeführt. Als zentrale Referenz diente die Norm ISO/IEC/IEEE 29119 („Software and Systems engineering — Software testing“), anhand derer eine grundlegende Struktur für das Testkonzept entwickelt wurde. Da sich die ISO/IEC/IEEE 29119 primär auf klassische Softwaretests bezieht, wurde kontinuierlich geprüft, inwiefern sie auf die Gesamtfahrzeugverifikation und Sicherheitsvalidierung automatisierter Fahrzeuge übertragbar ist und an welchen Stellen Anpassungen oder Erweiterungen notwendig sind. Im weiteren Projektverlauf wurden die einzelnen Abschnitte des Testkonzepts inhaltlich prototypisch ausgestaltet. Dazu wurden vor allem die Normen ISO 26262 und ISO 21448 sowie die Durchführungsverordnung (EU) 2022/1426 analysiert und berücksichtigt.

Als Testansatz wurde ein szenarienbasierter Ansatz gewählt. Abbildung 13 illustriert das systematische Vorgehen zur Sicherheitsvalidierung automatisierter Fahrfunktionen, basierend auf der Durchführungsverordnung (EU) 2022/1426, welches im Testkonzept beschrieben wurde. Für die Sicherheitsvalidierung werden aus der Operational Design Domain (ODD) des Fahrzeugs funktionale Szenarien abgeleitet, wobei sowohl datenbasierte als auch wissensbasierte Ansätze zur Generierung dieser funktionalen Szenarien Anwendung finden können. Qualitativ können die abgeleiteten Szenarien in „nominale“ und „kritische“ Szenarien unterteilt werden. Diese Einteilung erfolgt im Rahmen des Systems und Safety Engineerings. Die funktionalen Szenarien werden in logische Szenarien überführt, die gegebenenfalls durch zusätzliche Parameter aus der ODD-Definition erweitert werden. Die logischen Szenarien werden anschließend mit Bestehenskriterien versehen, um Testfälle für einen Testfallkatalog zu erstellen. Diese Kriterien beruhen bei nominalen Testfällen auf Sicherheitsanforderungen und Vorschriften (z. B. der Straßenverkehrsordnung; StVO), während kritische Testfälle auf Sicherheitsmodellen basieren. Die daraus abgeleiteten Testfälle können sowohl in realen Fahrversuchen als auch in einer Simulationsumgebung durchgeführt werden. Durch eine gezielte Variation der Szenarien in der Simulationsumgebung kann gezielt nach Sicherheitsverletzungen gesucht werden, die an das System- und Sicherheitsengineering zurückgemeldet werden können. Dabei kann auch eine Aussage über die statistische Restwahrscheinlichkeit von Sicherheitsverletzungen des automatisierten Fahrzeugs getroffen werden. Durch den Vergleich der Ergebnisse aus realen Fahrversuchen und den Ergebnissen aus der Simulation kann zudem eine Validierung der Simulation erreicht werden.

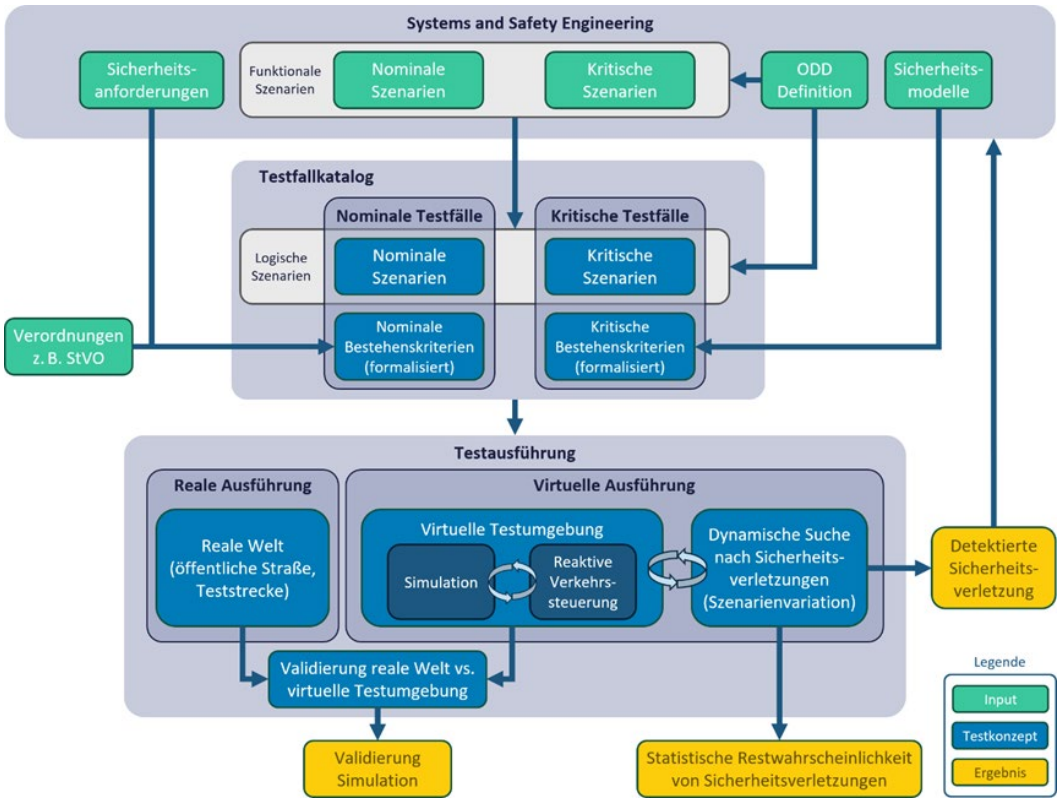



Abbildung 13 Systematisches Vorgehen zur Sicherheitsvalidierung automatisierter Fahrfunktionen, basierend auf DURCHFÜHRUNGSVERORDNUNG (EU) 2022/1426 DER KOMMISSION.

### 3.4.2 Umsetzung des Testkonzepts zur Erstellung des Testfallkatalogs zur Gesamtfahrzeugverifikation des Level-4-Prototyps (AP4.2) und zur Sicherheitsvalidierung (AP 4.3)

Im Rahmen von AP 4.2 und AP 4.3 wurde die Umsetzung des Testkonzepts zur Erstellung eines Testfallkatalogs zur Gesamtfahrzeugverifikation des Demonstrationsfahrzeugs[4] und zur Sicherheitsvalidierung wissenschaftlich untersucht. Zur Veranschaulichung des in AP 4.1 entwickelten Testkonzepts wurde ein grundlegendes Beispiel erarbeitet, das in AP 4 übergreifend Anwendung finden sollte. Das grundlegende Beispiel umfasst drei funktionale Szenarien, die jeweils in logische und anschließend in konkrete Szenarien mit zugehörigen Bewertungskriterien überführt wurden, um konkrete Testfälle zu spezifizieren. Die Initialszenen der drei betrachteten funktionalen Szenarien sind in Abbildung 14, Abbildung 15 und Abbildung 16 dargestellt. Ausgehend von einer textuellen Beschreibung wurden die Szenarien im Projektverlauf kontinuierlich erweitert und verfeinert. Dabei wurden insbesondere die für das Projekt relevanten ODD-Parameter zur Beschreibung der Szenarien identifiziert und die Szenarien mit Hilfe des 6-Ebenen-Modells[5] strukturiert beschrieben – ein Modell zur Beschreibung von

[4] In der ATLAS-L4 Vorhabenbeschreibung wurde der Begriff Level-4-Prototyp verwendet. Dieser entspricht gemäß der abgestimmten Taxonomie dem Demonstrationsfahrzeug.

[5] Eine detaillierte Beschreibung zum 6-Ebenen-Modell ist beispielsweise in nachfolgend zitierten Journalartikel enthalten: [13]
M. Scholtes, L. Westhofen, L. R. Turner, K. Lotto, M. Schuldes, H. Weber, N. Wagener, C. Neurohr, M. H. Bollmann, F. Kortke, J. Hiller, M. Hoss, J. Bock und L. Eckstein, „6-layer model for a structured description and categorization of urban traffic and environment," IEEE Access, Vol. 9, S. 59131–59147, 2021, doi: 10.1109/ACCESS.2021.3072739

Szenarien, das in Projekten wie PEGASUS, SET Level und VVMethoden (weiter)entwickelt wurde. Bei der Beschreibung wurde sich jedoch auf die Ebenen 1 (Straßenebene), 2 (Straßenausstattung) und 4 (Bewegliche Objekte) konzentriert. Die Ebenen 3 (Temporäre Beeinflussung von Ebene 1 und Ebene 2), 5 (Umweltbedingungen) und 6 (Digitale Information) wurden im Projekt ATLAS-L4 für zukünftige Arbeiten konzeptionell vorgesehen, jedoch nicht weiter betrachtet.

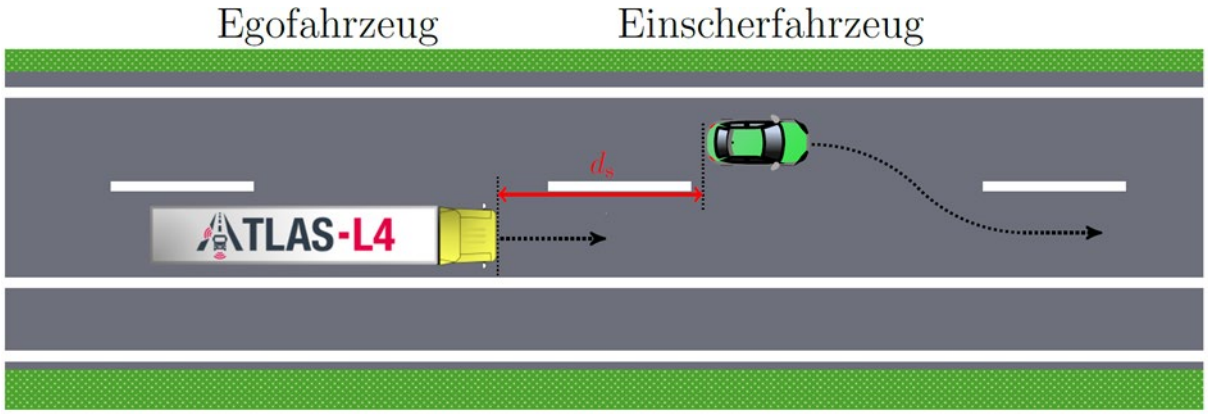



Abbildung 14 Initialszene des Szenarios mit dem Namen „Einscherer von links mit anschließendem Bremsen“
(die gepunkteten Pfeile zeigen das prinzipielle Verhalten der Fahrzeuge während des Szenarios an (nicht maßstabsgetreu gezeichnet); $d_s$: longitudinaler Startabstand der beiden Fahrzeuge)

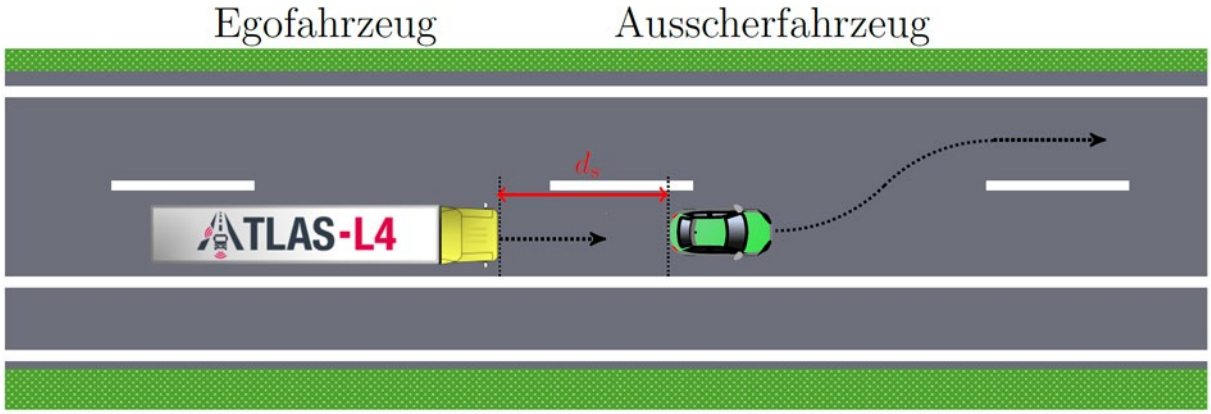



Abbildung 15 Initialszene des Szenarios mit dem Namen „Ausscherer nach links“
(die gepunkteten Pfeile zeigen das prinzipielle Verhalten der Fahrzeuge während des Szenarios an (nicht maßstabsgetreu gezeichnet); $d_s$: longitudinaler Startabstand der beiden Fahrzeuge)

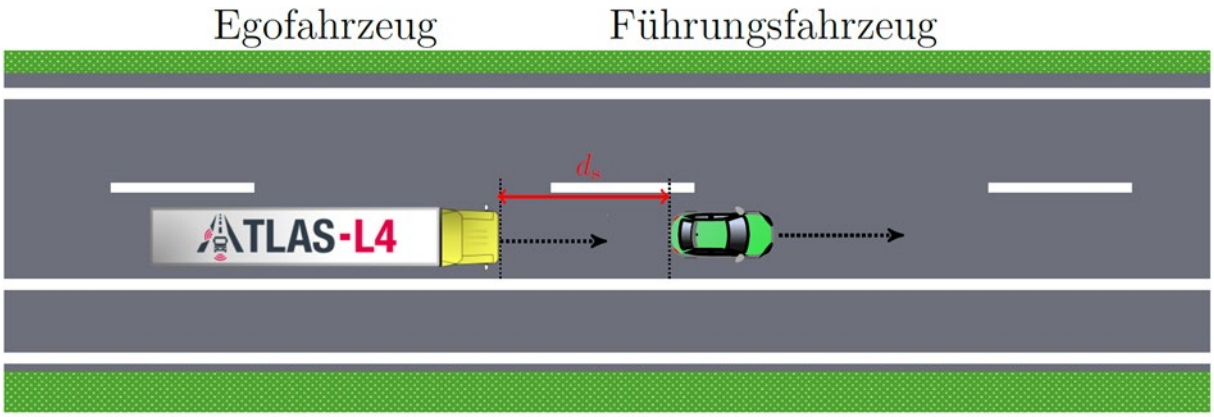



Abbildung 16 Initialszene des Szenarios mit dem Namen „Folgefahrt“
(die gepunkteten Pfeile zeigen das prinzipielle Verhalten der Fahrzeuge während des Szenarios an (nicht maßstabsgetreu gezeichnet); $d_s$: longitudinaler Startabstand der beiden Fahrzeuge)

Die Auswahl der oben genannten Szenarien erfolgte in Abstimmung mit den an AP 4 beteiligten Projektpartnern unter Berücksichtigung technischer Randbedingungen wie den Gegebenheiten des Prüfgeländes in Penzing und der Verfügbarkeit relevanter Eingabedaten, da die Szenarien sowohl in der Realität auf dem Prüfgelände in Penzing als auch in einer Simulation durchgeführt werden sollten. Die Szenarien wurden somit so ausgewählt, dass im Rahmen von AP 4.5 ein Vergleich der Ergebnisse aus den in der Realität durchgeführten Szenarien mit den Ergebnissen aus der Simulation möglich war. Durch den Vergleich der jeweiligen Ergebnisse konnten im Rahmen von AP 4.5 die Ergebnisse aus der Simulation plausibilisiert[6] werden.

Für die Bewertung des sicheren Verhaltens des Egofahrzeugs wurden im Rahmen von AP 4.3 spezifische Sicherheitsmetriken analysiert. Besonders betrachtet wurden

- Time-to-Collision (TTC) – auch im Kontext der EU-Durchführungsverordnung 2022/1426,
- Distance Headway (DHW) und
- Time Headway (THW).

Während diese drei Metriken Aussagen über das sichere Verhalten des Egofahrzeugs ermöglichen, wurden zur Plausibilisierung der Simulation im Rahmen von AP 4.5 weitere Metriken zum Vergleich von Real- und Simulationsdaten herangezogen.

Es ist anzumerken, dass die im Beispiel betrachteten Testfälle einen exemplarischen Ausschnitt der für die Sicherheitsvalidierung des Lkws benötigten Testfälle darstellen. Für eine umfassende Sicherheitsvalidierung des Lkws sind deutlich mehr Testfälle erforderlich.

Zusätzlich wurden Open-Source-Datensätze untersucht. Dabei wurde das Ziel verfolgt, die Daten als Grundlage für die Ableitung und Spezifikation von Szenarien zu nutzen. In einem ersten Schritt wurden verschiedene öffentlich verfügbare Datensätze identifiziert und hinsichtlich ihrer Eignung zur Szenarienableitung analysiert und auf deren Basis ein erster

[6] Es wird hier der Begriff „plausibilisiert“ verwendet, da aufgrund der prototypischen Toolkette und der wenigen ausgewählten Versuche eine echte „Validierung“ budgetbedingt im Projekt nicht möglich war. Eine Validierung für den Serieneinsatz dürfte mehr als das Zehnfache der gesamten Projektsumme kosten.

Ansatz zur algorithmischen Szenarienableitung entwickelt. Als Beispiel wurden dafür die drei oben genannten funktionalen Szenarien herangezogen.

Die daraus gewonnenen Parameterverteilungen und Metriken konnten anschließend genutzt werden, um Testfälle für die Simulation sowie den Realtest genauer spezifizieren zu können.

### 3.4.3 Einsatz simulativer Testmethoden (AP 4.4)

Um den Level-4-Planer aus AP 8 auf den Szenarien des Testfallkatalogs simulativ zu testen, wurde dieser Planer als Testobjekt in die prototypische BTC Werkzeugkette für das szenarienbasierte Testen mit dem Simulationswerkzeug SIMPHERA der Firma dSPACE integriert. Zudem wurden die Szenarien Einscherer, Ausscherer und Folgefahrt des Testfallkatalogs im BTC Testtool mit Hilfe des grafischen Szenarieneditors formal spezifiziert, siehe Abbildung 17. Die Simulationskerntechniken der BTC Werkzeugkette wurden entsprechend den Anforderungen im Kontext des Projektes kontinuierlich angepasst und weiterentwickelt, z. B. die Szenarien-Sprache, der Szenarien-Observer, der Szenarien-Solver, und die Szenarien-Engine (RTC) zum Ausspielen der Szenarien in der Simulation.

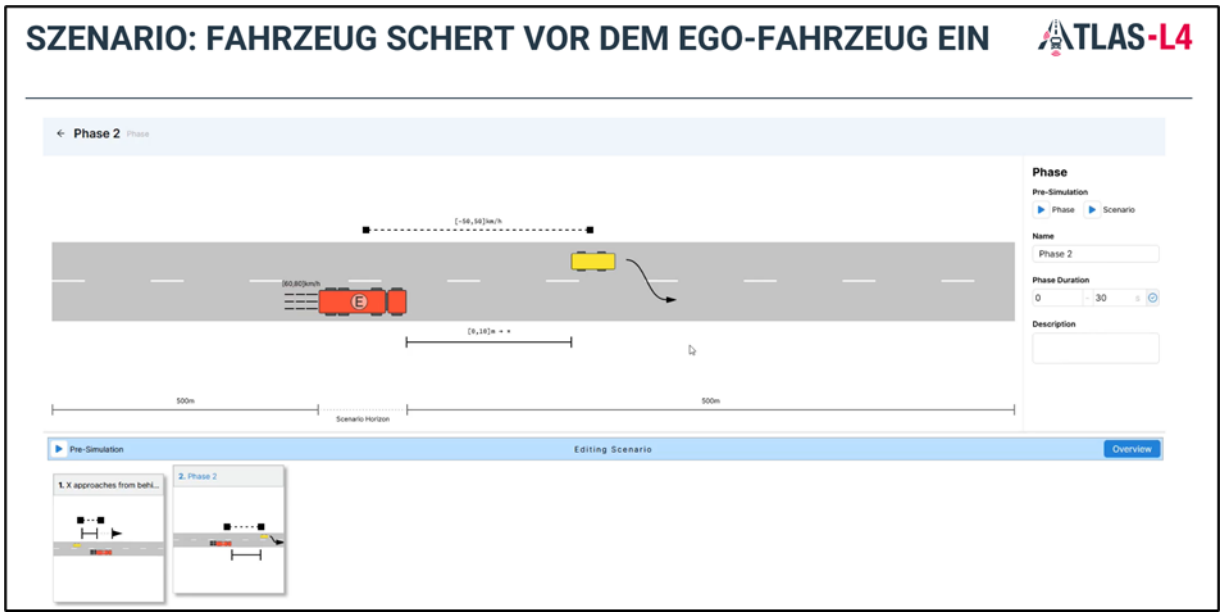



Abbildung 17 Formale Spezifikation mit Hilfe des grafischen Szenarieneditors des Einscherszenarios

Um das Testobjekt nun auf Schwachstellen innerhalb der Szenarien zu untersuchen, wurde die Testmethode Weakness Detection (WD) angewendet. Die WD ist ein globales Optimierungsverfahren, das nach besonders kritischen Szenarienausführungen sucht oder deren Abwesenheit statistisch nachweist. Solche Kritikalitätsmetriken wie Time-To-Collision sind im Testfallkatalog beschrieben. In Abbildung 18 ist ein exemplarischer Verlauf der Weakness Detection für das Einscherszenario und ein Testobjekt mit absichtlich platzierter Schwäche dargestellt.

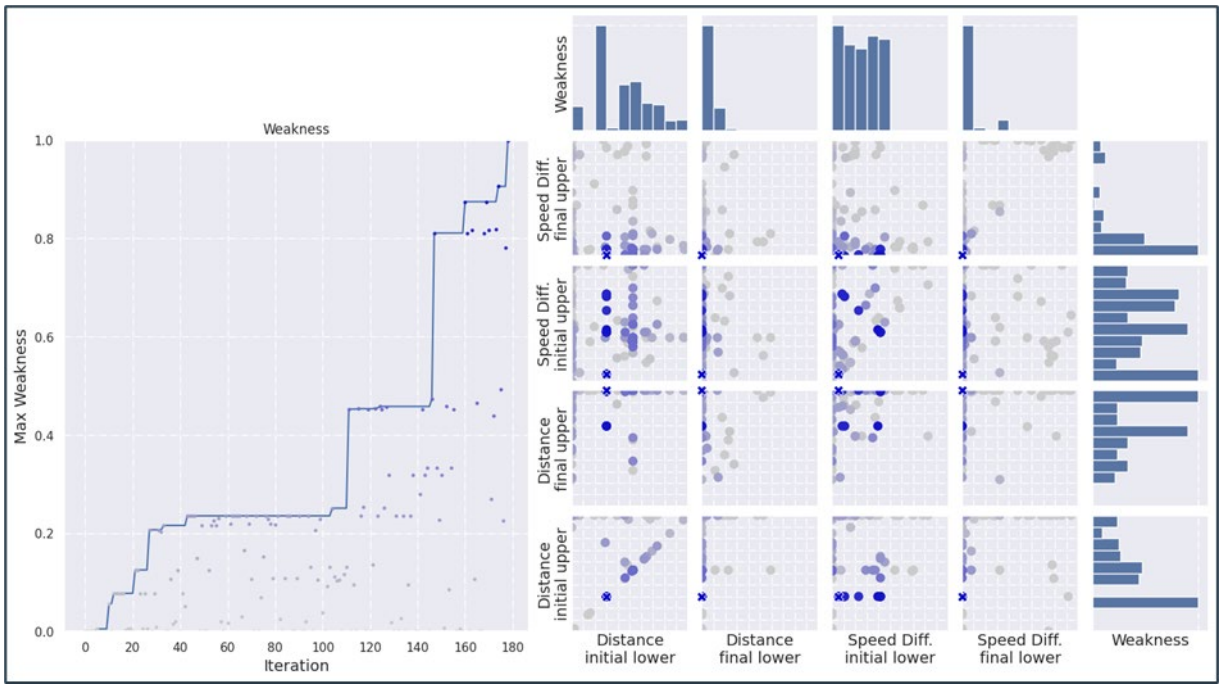



Abbildung 18 Darstellung des Verlaufes der Weakness Detection.
Links: Ermittelter Weakness-Wert, wobei der Wert 1.0 eine gefundene Schwachstelle repräsentiert. Rechts: Teil des Parameterraumes, der abgetastet wurde. Tieferes Blau bedeutet höherer Weakness-Wert. Nach 179 Iterationen wurde eine Weakness (1.0) gefunden.

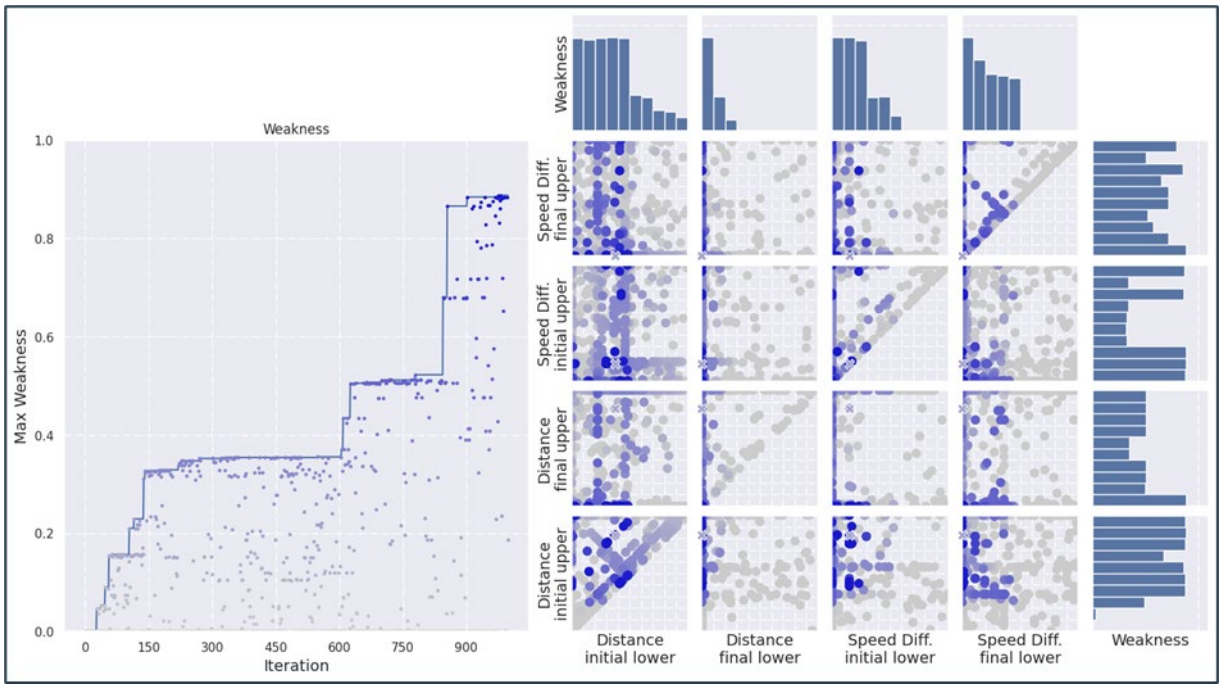



Abbildung 19 Erneuter Lauf der Weakness Detection mit angepasstem Testobjekt
(ohne absichtlich platzierte Schwäche). Im gesamten Lauf wurde keine Weakness gefunden.

Entfernt man die absichtlich platzierte Schwäche aus dem Testobjekt und führt das gleiche Experiment erneut durch, findet die WD keine Schwachstelle innerhalb einer vorgegebenen Anzahl von Iterationen bzw. Simulationen, siehe Abbildung 19. Für die Freigabe von autonomen Fahrzeugen ist es aber essenziell, eine zumindest statistische Aussage über die Abwesenheit von Schwachstellen zu erhalten. Daher wurde im Projekt ein Verfahren zur Abschätzung dieses Restrisikos, falls keine Schwachstelle gefunden wurde, untersucht und experimentell angewendet. Für das Einscherszenario konnte beispielsweise die Wahrscheinlichkeit der Existenz einer Schwachstelle mit einem sehr kleinen Wert von ungefähr $10^{-7}$ abgeschätzt werden, siehe Abbildung 20.

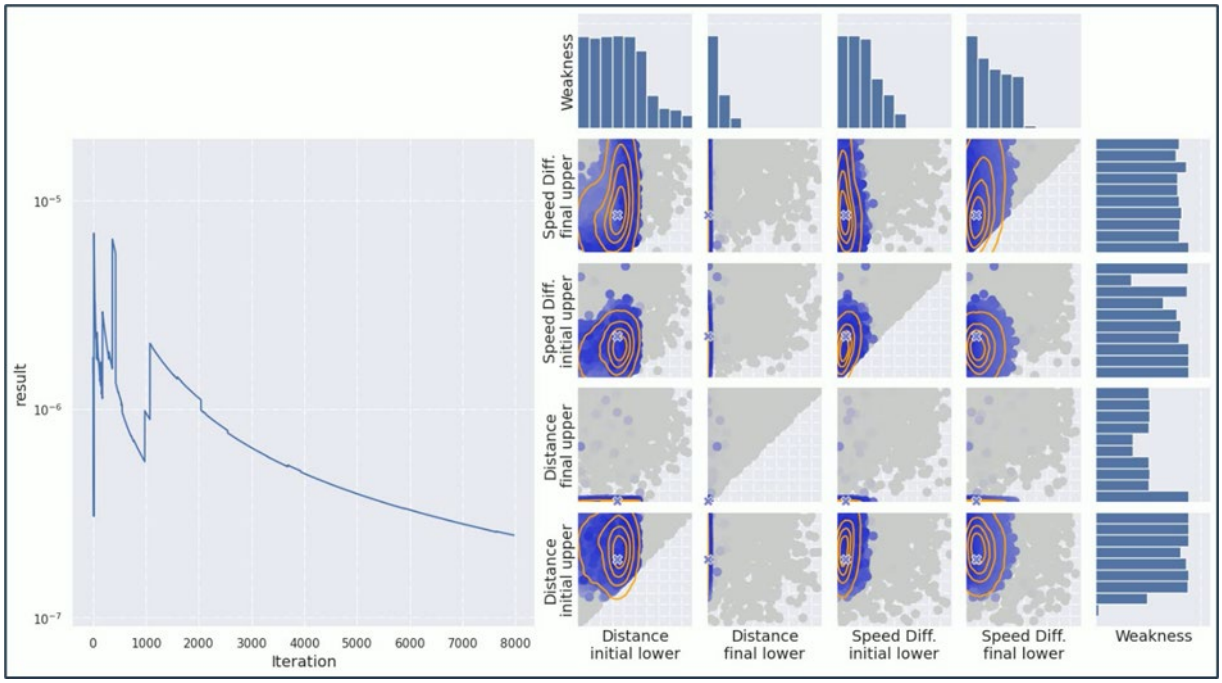



Abbildung 20 Visualisierung der Berechnung der Wahrscheinlichkeit der Existenz einer Weakness. Links: Wahrscheinlichkeit auf Basis der bisher gezogenen Samples der Proposalverteilung. Rechts: Darstellung des bisher abgetasteten Parameterbereiches.

### 3.4.4 Exemplarische Validierung der Simulation auf dem Prüfgelände (AP 4.5)

Um die Testergebnisse aus der Simulation auf die Realität zu übertragen, ist es notwendig, zu überprüfen, ob die virtuelle Simulation die Realität hinreichend genau abbildet. In diesem Arbeitspaket haben wir eine Methodik untersucht, die es ermöglicht, einen Vergleich von simulierten und realen Fahrten durchzuführen.

Zuerst wurden die Szenarien aus dem Testallkatalog auf dem Prüfgelände abgefahren. Diese physikalischen Tests wurden in mehreren Stufen durchgeführt. Im Mai 2023 fand zunächst eine Streckenvermessung in Thurnau statt. Im Juli 2024 folgten umfangreiche Prüfgeländetests in Penzing mit verschiedenen Fahrmanövern wie Einscheren, Ausscheren und Folgefahrt. Im Februar 2025 wurden ausgewählte Ergebnisse erneut validiert.

Zu Beginn wurden die Versuche noch mit einem komplett auf interne Aktuatorik umgebauten Traffic Simulation Vehicle (TSV) durchgeführt. Diese Lösung wurde jedoch im Verlauf des Projekts verworfen, da eine universellere Lösung mit verschiedenen Fahrzeuggrößen und -modellen eine bessere Abdeckung der realen Verkehrssituationen ermöglicht. Daher kam

zunehmend ein Lenkroboter zum Einsatz, der eine flexible und fahrzeugunabhängige Querregelung erlaubt.

Abbildung 21 Einschermanöver – drei Sequenzaufnahmen aus dem Versuch

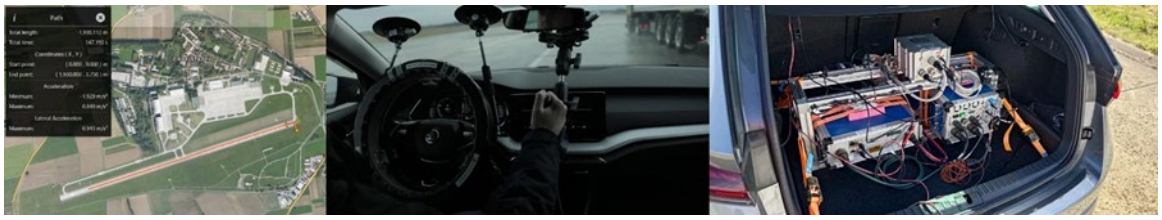


Abbildung 22 Übersicht Prüfgelände, Innenraumaufnahme und verbaute Messtechnik

Die im Rahmen der Tests erhobenen Messdaten wurden an die Projektpartner verteilt und im Post-Processing ausgewertet.

Um den Vergleich zwischen Realfahrt und Simulation durchzuführen, wurde eine Simulationsumgebung basierend auf VEOS und SIMPHERA aufgesetzt. In dieser Umgebung wurde ein Verhaltensmodell des Lkws erstellt und der Level-4-Planer integriert, welcher auch bei den realen Testfahrten zum Einsatz kam. Genau wie in den realen Fahrversuchen, steuerte der Level-4-Planer das Ego Fahrzeug während der Szenarienausführung auch in der Simulation. Für die Ansteuerung des Fellow Fahrzeuges wurde eine Regelungskomponente in die Simulation integriert, welche das Fellow Fahrzeug kontrollierte.

In den durchgeführten Vergleichen wurden die Aufzeichnungen folgender Größen einbezogen:

- **Stoßstangendistanz** zwischen Ego und Fellow: Die Distanz der vorderen Stoßstange des Egos zur hinteren Stoßstange des Fellows in Metern.
- **Geschwindigkeit** des Egos: Die Geschwindigkeit des vom Level-4-Planer gesteuerten Fahrzeuges in km/h.

Da das Verhalten des Fellow Fahrzeugs in der Simulation exakt dem Verhalten des Fellows in dem jeweiligen realen Fahrversuch entsprach (die aufgezeichnete Positionstrajektorie des Fellows wurde in der Simulation exakt abgefahren), beschränkt sich der Vergleich auf Zustandsgrößen des Ego-Fahrzeugs.

Als Vergleichsmetrik wurde die Root-Mean-Square-Error (RMSE) Metrik gewählt, die häufig zum Qualitätsvergleich der Voraussage von Messreihen verwendet wird. Die entsprechenden Ergebnisse für die verschiedenen Szenarien sind in Abbildung 23 und Abbildung 24 dargestellt.

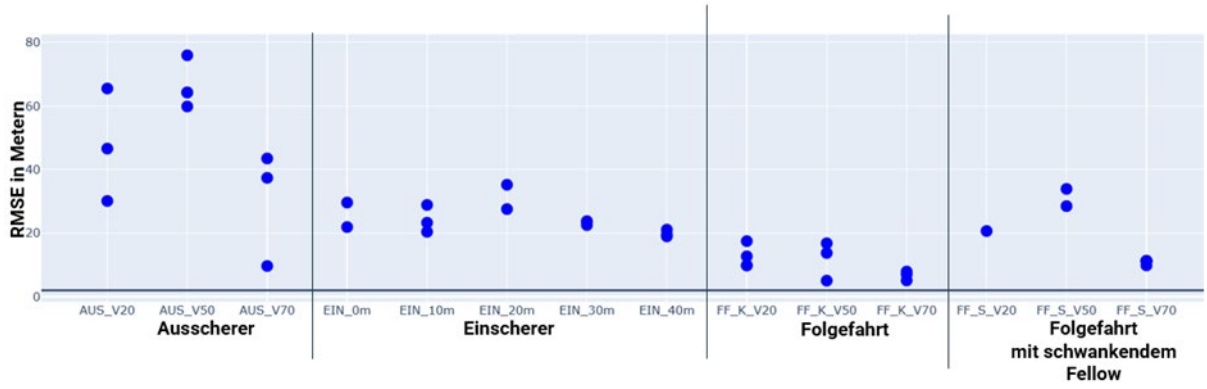



Abbildung 23 Darstellung des RMSE für Distanz zwischen vorderer Stoßstange des Egos und hinterer Stoßstange des Fellows.
Auf der X-Achse sind die verschiedenen Szenarien und ihre Variationen abgebildet.

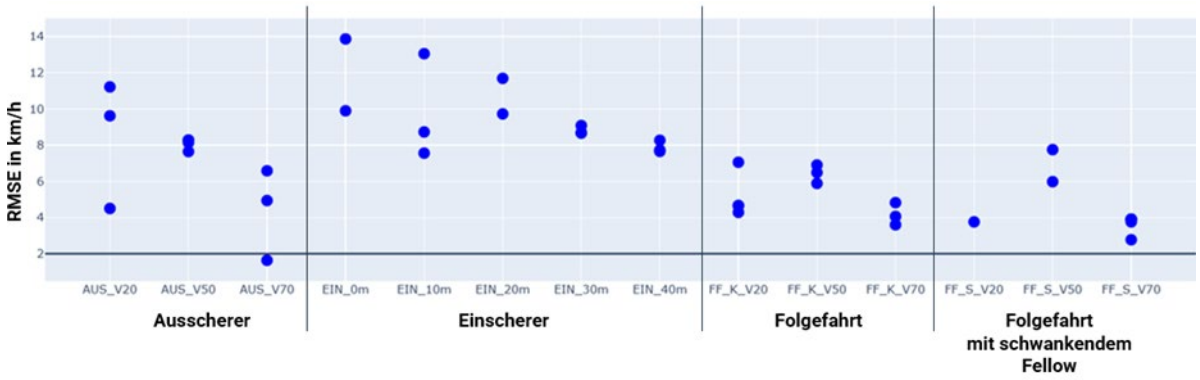



Abbildung 24 Darstellung des RMSE für die Geschwindigkeit des Egos.
Auf der X-Achse sind die verschiedenen Szenarien und ihre Variationen abgebildet

Die untersuchte Methodik erlaubt den automatisierten Vergleich zwischen Realfahrten und Simulationen, um die Validität der Simulation für den virtualisierten Test zu überprüfen. In den konkreten Experimenten konnten wahrscheinlich relevante Abweichungen identifiziert werden. Es deutet darauf hin, dass diese Abweichungen in der Parametrisierung der Simulation und des Level-4-Planers begründet sind. Für den praktischen Einsatz sollten derartige Abweichungen auf ein akzeptables Maß reduziert werden.

### 3.4.5 Durchführung der relevanten Testfälle als Basis für die Freigabe des Level-4-Prototyps für Demonstrationen innerhalb des Projekts (AP 4.6)

Im Rahmen des Projekts wurden in dem AP 4.6 „Durchführung der relevanten Testfälle als Basis für die Freigabe des Level-4-Prototyps für Demonstrationen innerhalb des Projekts“ die für die Freigabe des Level-4-Prototyps (im Level-2-Betrieb mit einem Sicherheitsfahrer im Lkw) erforderlichen Testfälle auf dem Testgelände in Penzing erfolgreich durchgeführt. Somit konnte eine Freigabe gemäß der Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV) durch die zuständigen Behörden sowie den technischen Dienst für ein Sensorfahrzeug erteilt werden.

Um die Umfeldwahrnehmung autonomer Fahrzeuge zu unterstützen, kann Nachrichtenaustausch mit der Infrastruktur oder zwischen Fahrzeugen untereinander ein entscheidendes Instrument sein. Im Rahmen der Testfahrten auf dem Prüfgelände wurden daher zudem zwei C-ITS Anwendungsfälle erprobt: der „Baustellenwarner“ sowie das „Digitale Warndreieck“. C-ITS steht für „kooperative intelligente Verkehrssysteme“ und setzt auf die Vernetzung von Fahrzeugen, Diensteanbietern und Infrastruktur. Das Ziel ist es, die Verkehrssicherheit auf den Autobahnen zu erhöhen. Mit C-ITS erhalten Verkehrsteilnehmende durch Direktkommunikation (IEEE 802.11p/ WLANp) in ihren Fahrzeugen Informationen aus erster Hand und können darauf reagieren.

Der „Baustellenwarner“ funktioniert so: Nähert sich ein (autonomes) Fahrzeug einer Baustelle, erhält es bis zu 800 Meter davor über WLANp die Information „Achtung, Baustelle voraus“. Damit bleibt dem Fahrzeug genügend Zeit, um entsprechend auf die Situation zu reagieren, noch bevor diese von der Sensorik erfasst werden kann. Beim „digitalen Warndreieck“ sendet ein autonomes Fahrzeug, welches ein MRM (siehe auch AP 3.4) durchführt, eine Warnmeldung „Achtung, langsames Fahrzeug voraus“ aus. Verkehrsteilnehmende in der Nähe sind so frühzeitig gewarnt.

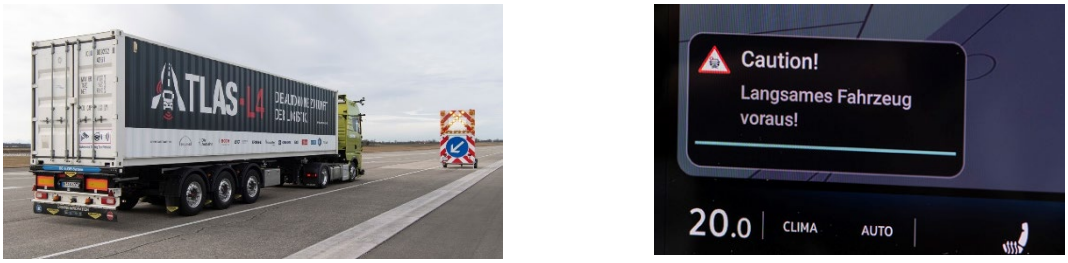



Abbildung 25 links: Testfahrten zum "Baustellenwarner" auf dem Prüfgelände. rechts: Anzeige der Warnmeldung, die beim Anwendungsfall "Baustellenwarner" ausgesendet wurde

Um das Potenzial von C-ITS beim autonomen Fahren zu zeigen, wurden die beiden Anwendungsfälle nicht nur auf dem Prüfgelände erprobt, sondern auch bei der Abschlussveranstaltung erfolgreich demonstriert.

### 3.4.6 AP 4 – Vortrag und Poster der Abschlusspräsentation

## AP4: TEST UND VALIDIERUNG

**Motivation und Ziele**

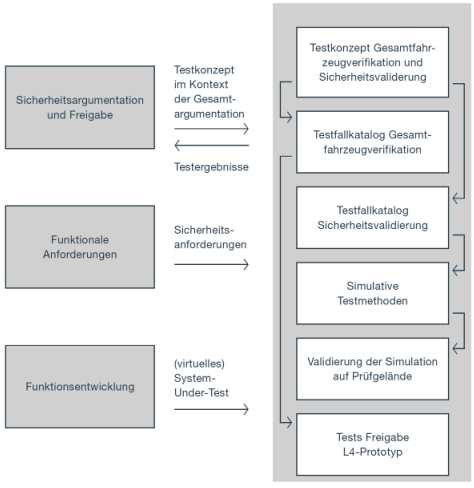
- **Klassische Testansätze** zur Freigabe von Level- 4-Fahrzeugen nicht mehr ausreichend
  - enorme Anzahl zu testender Verkehrssituationen
  - mehrere Milliarden Testkilometer in der Realität
- **Virtualisierung** eines Großteils der Testfahrten
  - Virtuelle Tests schneller und mit weniger Aufwand umsetzbar → Skalierbarkeit
  - Simulation muss Realität ausreichend genau abbilden damit Testergebnisse valide sind
- Anwendung von **szenarienbasierten Testansätzen** zur Gesamtfahrzeugverifikation und Sicherheitsvalidierung eines Level-4-LKWs


ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Dr. Tino Teige, BTC Embedded Systems AG 42

## AP4: TEST UND VALIDIERUNG

**Arbeitsschwerpunkte**

- Entwicklung von **Testkonzepten** für Gesamtfahrzeugverifikation und die Sicherheitsvalidierung von Level 4-Fahrfunktionen
- Ableitung von **Testfallkatalogen** für die Gesamtfahrzeugverifikation und die Sicherheitsvalidierung
- Einsatz **simulativer Testmethoden** für die Verifikation und Validierung
- **Validierung der Simulation** auf dem Prüfgelände
- Durchführung relevanter **Testfälle zur Freigabe** von Demonstrationsfahrzeugen




ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Dr. Tino Teige, BTC Embedded Systems AG 43

## AP4: TEST UND VALIDIERUNG

**Ergebnisse und Highlights**

- Prototypisches **Testkonzept** und beispielhafter **Testfallkatalog** für Gesamtfahrzeugverifikation und die Sicherheitsvalidierung
- Prototypische **Toolkette zum szenarienbasierten Testen** des L4-Planers in virtueller Simulationsumgebung
- Umsetzung eines exemplarischen **Vergleichs zwischen Realfahrten auf dem Prüfgelände** und Simulationen zur Validierung
- **AFGBV-Freigabe für Demonstrationsfahrzeug** nach erfolgreichem Freigabetest in Penzing

ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Dr. Tino Teige, BTC Embedded Systems AG 44

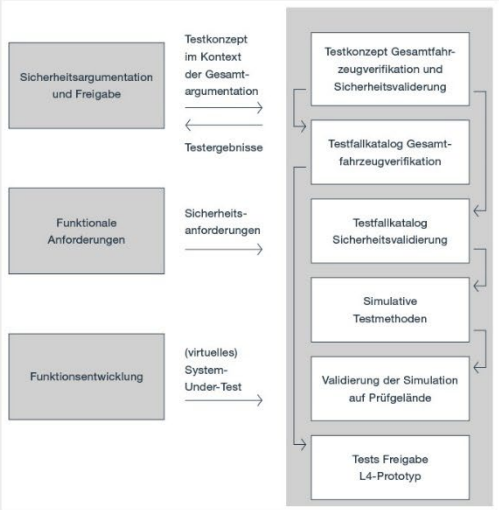
# TEST- UND VALIDIERUNGSMETHODEN
## Übersicht

### MOTIVATION UND ZIELE

- Klassische Testansätze zur Freigabe von SAE Level-4-Fahrzeugen nicht mehr ausreichend aufgrund der enormen Vielzahl der zu testenden Verkehrssituationen (Milliarden Testkilometer)
- Virtualisierung des Großteils der Testfahrten
- Szenarienbasierte Testansätze zur Gesamtfahrzeugverifikation und Sicherheitsvalidierung eines SAE Level-4-LKWs


### ARBEITSSCHWERPUNKTE

- Testkonzepte und Testfallkataloge für die Gesamtfahrzeugverifikation und die Sicherheitsvalidierung
- Einsatz simulativer Testmethoden für die Verifikation und Validierung
- Validierung der Simulation auf dem Prüfgelände
- Durchführung der relevanten Testfälle zur Freigabe von Demonstrationsfahrzeugen




Einordnung der Test- und Validierungsmethoden in den Projektkontext

### ERGEBNISSE/HIGHLIGHTS

- Prototypisches Testkonzept und beispielhafter Testfallkatalog für die Gesamtfahrzeugverifikation und die Sicherheitsvalidierung
- Prototypische Toolkette zum szenarienbasierten Testen des L4-Planers in virtueller Simulationsumgebung
- Umsetzung eines exemplarischen Vergleichs zwischen Realfahrten auf dem Prüfgelände und Simulationen zur Validierung
- AFGBV-Freigabe für Demonstrationsfahrzeug nach erfolgreichem Freigabetest in Penzing

Realfahrt in Penzing

# TESTKONZEPT VERIFIKATION UND SICHERHEITS-VALIDIERUNG AUTOMATISIERTER FAHRZEUGE

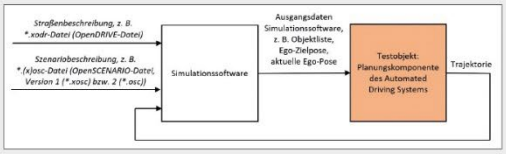
## Test- und Validierungsmethoden

### MOTIVATION

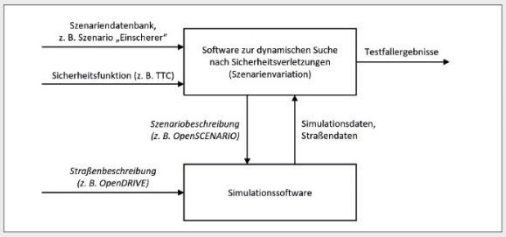
Die Verifikation und Sicherheitsvalidierung eines automatisierten Fahrzeugs nach SAE Level 4 oder (Teile) eines zugehörigen Automated Driving Systems sind zentrale Voraussetzungen für die Freigabe eines automatisierten Fahrzeugs. Um die zugehörigen Testaktivitäten zu koordinieren, ist ein Testkonzept erforderlich. In diesem werden die zu erreichenden Testziele und die Mittel sowie der Zeitplan zum Erreichen dieser detailliert beschrieben.

### ERGEBNISSE

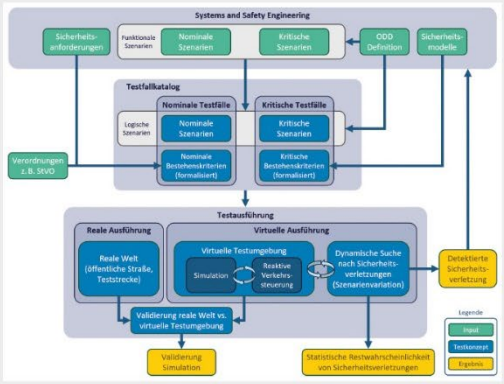
- Literaturrecherche zu Testkonzepten im Kontext Verifikation und Validierung
- Exemplarisches Testobjekt: Planungskomponente des Automated Driving Systems
- Prototypisches Testkonzept für die Sicherheitsvalidierung eines SAE Level 4 LKWs am Beispiel der Planungskomponente basierend auf dem Standard ISO/IEC/IEEE 29119 (Software and Systems Engineering – Software Testing)
- Methoden und Ansätze zur Sicherheitsvalidierung am Beispiel der Planungskomponente
- Funktionale Simulationsarchitektur für Planungskomponente (Software-in-the-Loop; siehe obere Abbildung)
- Funktionale Testarchitektur unter Berücksichtigung einer (automatisierten) Szenarienvariation (siehe mittlere Abbildung)
- Entwicklung eines systematischen Vorgehens zur Sicherheitsvalidierung automatisierter Fahrfunktionen basierend auf Durchführungsverordnung (EU) 2022/1426 (siehe untere Abbildung)




Abstrakte Darstellung funktionale Simulationsarchitektur




Abstrakte Darstellung funktionale Testarchitektur




Systematisches Vorgehen zur Sicherheitsvalidierung automatisierter Fahrfunktionen

# TESTKONZEPT VERIFIKATION UND SICHERHEITS-VALIDIERUNG AUTOMATISIERTER FAHRZEUGE

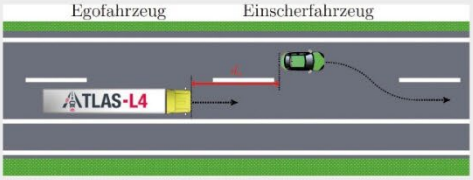
## Test- und Validierungsmethoden

### MOTIVATION

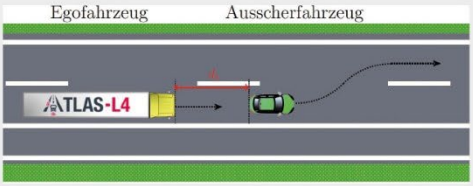
Für die Sicherheitsvalidierung eines automatisierten Fahrzeugs nach SAE Level 4 oder (Teile) eines zugehörigen Automated Driving Systems werden derzeit szenarienbasierte Ansätze erforscht. Dazu müssen relevante Szenarien und geeignete Bewertungskriterien abgeleitet und spezifiziert werden. Datensätze können die Szenarienableitung und die Bestimmung stochastischer Verteilungen der Parameterwerte unterstützen.

### ERGEBNISSE

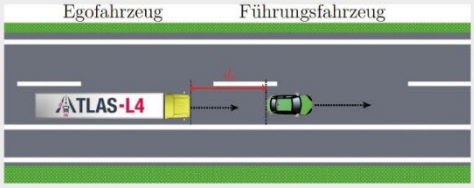
- Drei exemplarischen Szenarien als durchgängiges Beispiel: Einscherer, Ausscherer, Folgefahrt (Initialszene siehe oberen drei Abbildungen):
  - Beschreibung durch 6-Ebenen-Modell
  - Verwendung für Sicherheitsvalidierung und Plausibilisierung der Simulation
- Drei Bewertungsmetriken zur Sicherheitsvalidierung (unter Berücksichtigung der UN-Regelung Nr. 157[1]):
  - Time-to-Collision
  - Distance Headway
  - Time Headway
- Implementierung eines Ansatzes zur Ableitung von Szenarien aus Open Source Datensätzen
- Ableitung stochastischer Verteilungen der Parameterwerte aus Open Source Datensätzen
- Plausibilisierung der Metriken auf Basis der Open Source Datensätze in Hinblick auf deren Anwendbarkeit in den betrachteten Szenarien (Beispiel zur Metrik Distance Headway basierend auf highD Datensatz[2] siehe Abbildung unten)



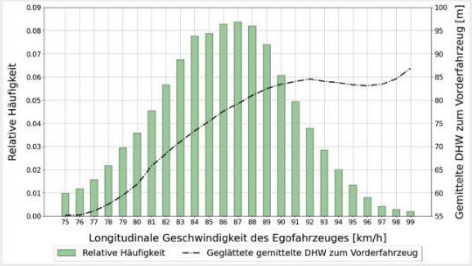

Initialszene Szenarios „Einscherer“ ($d_s$: initialer longitudinaler Abstand; gestrichelte Linie: prinzipielles Verhalten der Fahrzeuge)




Initialszene Szenarios „Ausscherer“ ($d_s$: initialer longitudinaler Abstand; gestrichelte Linie: prinzipielles Verhalten der Fahrzeuge)




Initialszene Szenarios „Folgefahrt“ ($d_s$: initialer longitudinaler Abstand; gestrichelte Linie: prinzipielles Verhalten der Fahrzeuge)




Distance Headway (DHW) Verteilung bei „Folgefahrt“

[1] *UN-Regelung Nr. 157 — Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich des automatischen Spurhalteassistenzsystems (ALKS) [2021/389].*

[2] *Krajewski et al. „The highD Dataset: A Drone Dataset of Naturalistic Vehicle Trajectories on German Highways for Validation of Highly Automated Driving Systems“. 2018.*

# EINSATZ SIMULATIVER TESTMETHODEN: PROTOTYPISCHE TOOLKETTE

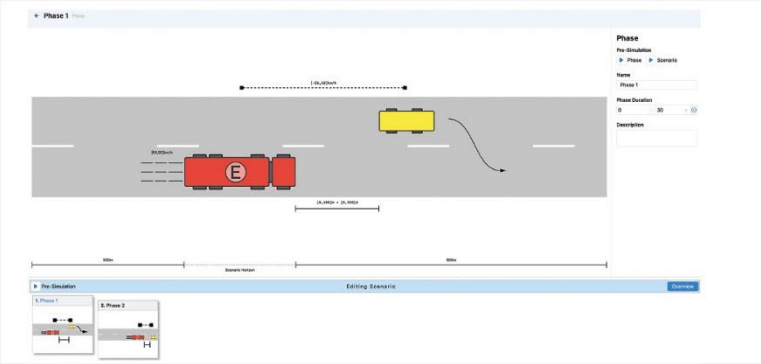
## Test- und Validierungsmethoden

### SZENARIENBASIERTES TESTEN

Abstrakt modellierte Verkehrsszenarien werden automatisch in Simulationen auf Schwachstellen hin untersucht und gegebenenfalls ihre Abwesenheit statistisch nachgewiesen.

### GRAFISCHE SZENARIENMODELLIERUNG

- Testszenarien aus Testfallkatalog: Einscherer, Ausscherer, Folgefahrt
- Grafische Modellierungssprache: Szenarien bestehen aus Phasen und Fahrmanövern
- Szenarioparameter wie z. B. Abstand und Geschwindigkeitsdifferenz beeinflussen Kritikalität




Grafische Modellierung eines Verkehrsszenarios

### SIMULATION & WEAKNESS DETECTION

- Integration der prototypischen Toolkette mit automatisierter Fahrfunktion (L4-Planer) in realitätsnahem Simulator
- Automatisches Finden von Schwachstellen mittels Optimierungsmethoden
- Statistischer Nachweis der Abwesenheit von Schwachstellen

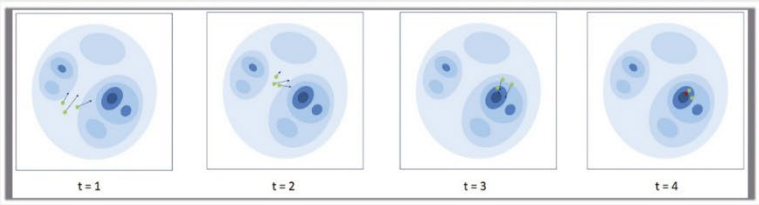



Illustration des Optimierungsverfahrens in der Weakness Detection

# AP 5: Software-Plattform L4

Nebiyat Taye, MAN Truck & Bus SE

## 3.5 AP 5: Software-Plattform L4

*Arbeitspaketleitung: Nebiyat Taye, MAN Truck & Bus SE*

### 3.5.1 Architektur (AP 5.1)

#### Motivation

Ein Ziel der Architektur ist eine übergreifende Systemarchitektur für das Fahrzeug zu entwickeln, die eine vollautomatisierte Fahrt über die Autobahn ermöglicht, unter Berücksichtigung aller Sicherheitsaspekte.

#### Aufbau der Architektur

Die Definition der Architektur beginnt mit der Funktionalen Architektur. Diese beschreibt das System lösungsunabhängig durch Funktionen. Die Funktionen sind an diesem Punkt als Zielverhaltensdefinitionen zu interpretieren und direkt aus den funktionalen Anforderungen abzuleiten (siehe AP3). Die Architekturdarstellung hilft, die Interaktionen und Zusammenhänge unterschiedlicher Anforderungen in einer Gesamtlösung zu verstehen. Ab diesem Punkt wird die entwickelte technische Lösung als logische „Fähigkeitskomponenten“ dargestellt und anschließend auf Hard-ware und Software konkretisiert (siehe Abbildung 26).

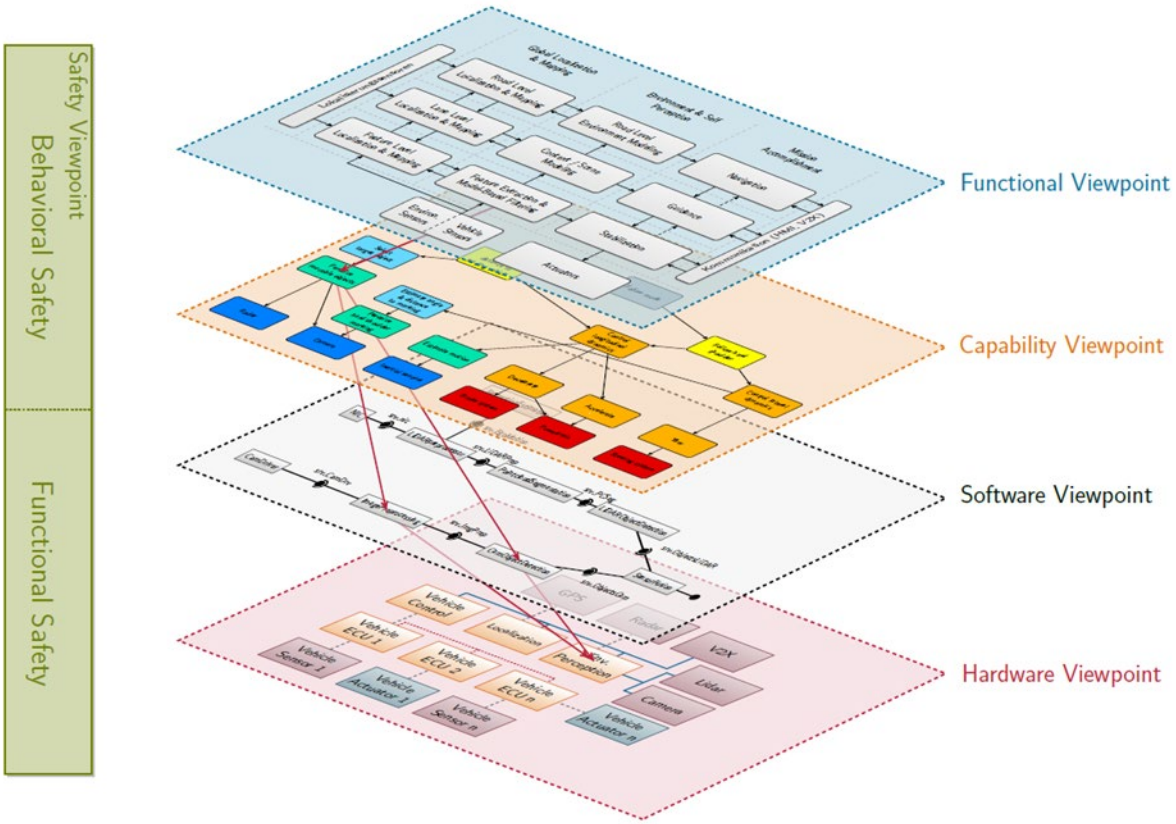



Abbildung 26 Architekturframework [G. Bagschik, M. Nolte, S. Ernst und M. Maurer, „A System's Perspective Towards an Architecture Framework for Safe Automated Vehicles“, 2018 21st International Conference on Intelligent Transportation Systems (ITSC), 2018, S. 2438-2445, doi: 10.1109/ITSC.2018.8569398]

### Anlegung der funktionalen Architektur mittels „model-based systems engineering“

Mit zunehmender Komplexität in mechatronischen Systemen kommen klassische Dokumentationsmethoden schnell an die Grenze. Um eine konsistente, nachvollziehbare Architektur zu erstellen, wurde eine modellbasierte Softwarelösung (Sparx Enterprise Architekt) verwendet, bei der jeder Aspekt der Architektur in einem überprüfbaren Modell angelegt wird:

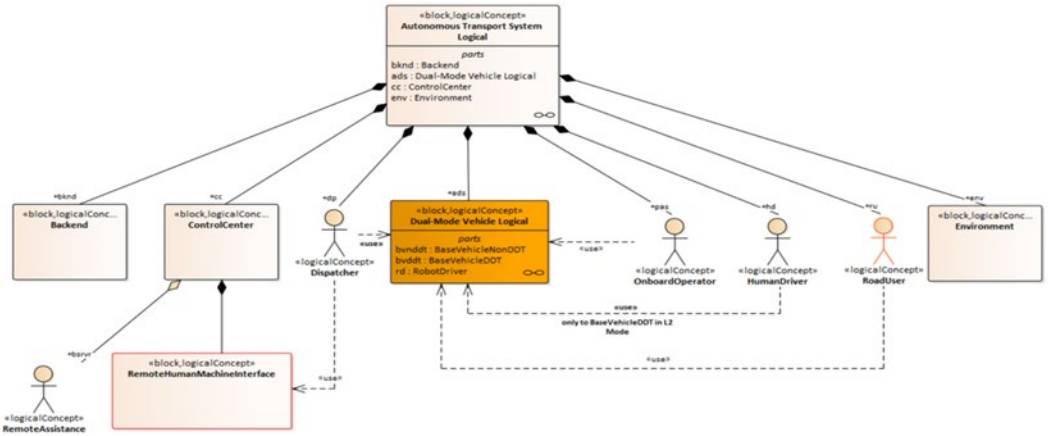



Abbildung 27 Darstellung der Gesamtlösung in Sparx Enterprise Architect

Basierend auf den funktionalen Anforderungen und internen Abstimmungen wurde die Gesamtfahrzeugfunktion „Automated Driving System" angelegt und die Schnittstellen zu bereits existierenden Fahrzeugfunktionen definiert. Diese Schnittstellen wurden festgelegt, da man für die Ausführung der Fahraufgabe auf den Großteil der existierenden Systeme zugreifen muss und existierende Serienfunktionen nicht neu entwickeln sollte.

### Sichere Architektur

Wie bereits erwähnt, ist eines der Hauptziele der Architektur, die Sicherheit des Gesamtsystems zu gewährleisten. Aus der initialen Definition der Funktion „Automated Driving System“ und ihrer Sub-Funktionen wurden die abstrakten Signalflüsse definiert und modelliert. Auf dieser Abstraktionsebene wurde eine Sicherheitsanalyse durchgeführt und die Verfügbarkeitsanforderungen an die Funktion abgeleitet. Daraus folgte, dass einige kritische Sub-Funktionen in zwei parallelen Implementierungen verfügbar sein mussten, um eine kontinuierliche, sichere Funktionalität gewährleisten zu können. Entsprechend wurde die Hauptfunktion neu definiert und mit redundanten Funktionalitäten ausgestattet.

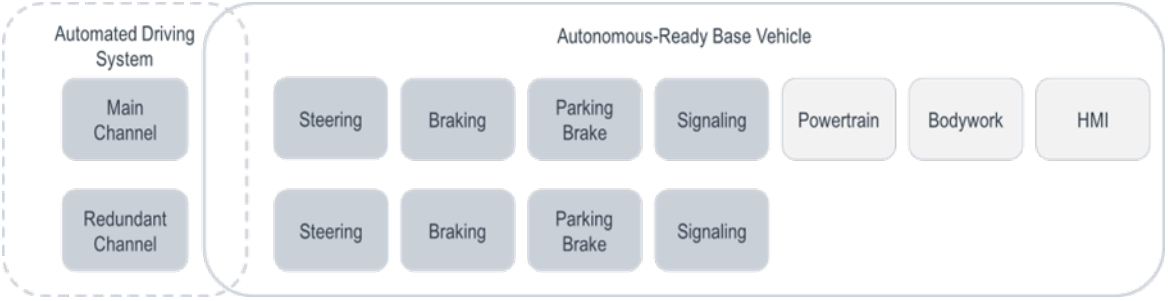



Abbildung 28 Angepasste funktionale Architektur mit parallelen Implementierungen

**Ableitung von Anforderungen**

Aus dieser Aufteilung heraus konnten die funktionalen Aspekte des Fahrzeugs generisch betrachtet werden. Somit ließen sich Anforderungen ableiten, die nicht von bestimmten Komponenten, sondern von deren Funktion abhängig sind. Allerdings mussten Bauteile aufgrund ihrer langen Entwicklungszeiten früh genug definiert werden. Deshalb wurde die Architektur für die redundante Bremse (Konsortialpartner Knorr-Bremse) als erstes bis auf Komponentenebene detailliert. Dazu gehörte nicht nur die funktionale Architektur, sondern auch die gesamte Systemarchitektur, bei der die spezifischen Funktionen den Bremskomponenten zugeordnet sind. So konnten z. B. aus den Funktionsbausteinen „Deceleration“ (Bremsfunktion) und „Steering“ (Lenkfunktion durch „Steer-by-Brake“) funktionale und sichere Anforderungen für die Entwicklung der redundanten Bremse von Knorr-Bremse abgeleitet werden. Dieser Prozess wurde entsprechend für alle Fahrzeugkomponenten systematisch durchgeführt.

**Iterative Detailierung der Architektur**

Nach der Erstellung der sicheren Architektur mit redundanten Funktionalitäten wurde eine detailliertere Sicherheitsanalyse und eine entsprechende Klassifizierung und Zuteilung der nötigen Integritäts- und Verfügbarkeitsattribute für die verschiedenen Funktionen und Signale vorgenommen. Das zweikanalige Design führte nicht nur zu einer parallelen Kommunikation zwischen zwei Funktionsketten, sondern auch eine transversale Kommunikation zwischen den redundanten Modulen, um einen nahtlosen Übergang zwischen primären und redundanten Funktionen zu gewährleisten. Diese Architektur wurde für das Sensorfahrzeug und das Demonstrationsfahrzeug in konkrete Funktionen zerlegt (sog. konkrete funktionale Architektur). Diese wurden als reale Softwaremodule entwickelt und implementiert. Somit konnte ein direkter Zusammenhang zwischen der Sicherheitsanalyse und dem spezifischen System am Fahrzeug hergestellt werden, was eine konsistente Definition von Tests und Validierungsstrategien ermöglicht hat.

#### 3.5.1.1 Architektur C-ITS für V2X-Kommunikation

Im Rahmen des ATLAS-L4 Projekts wurde die Gesamtarchitektur um Komponenten aus dem Bereich C-ITS (Cooperative Intelligent Transport Systems) erweitert. Die Integration basiert auf der V2X (Vehicle-to-Everything) Kommunikationstechnologie (ITS-G5 Standard), der eine direkte Kommunikation zwischen Fahrzeugen, Infrastruktur und Diensteanbietern ermöglicht. Die Direktkommunikation im reservierten Frequenzbereich ermöglicht den schnellen Austausch zwischen Verkehrsteilnehmern – unabhängig vom Mobilfunknetz. So können relevante Ereignisse frühzeitig erkannt und darauf reagiert werden. Die erweiterte C-ITS-Architektur zeigt ihr Potenzial zur Erhöhung der Verkehrssicherheit auf Autobahnen.

**Realisierte Use-Cases**

Im Projekt wurden zwei V2X-Basierte C-ITS Use-Cases erfolgreich umgesetzt und erprobt: Minimum Risk Maneuver (MRM) mit V2X (Versenden von Broadcast-V2X-Nachrichten (DENM) bei MRM/MRC-Zustand) und Baustellenwarner mit V2X (Empfang und Verarbeitung von V2X-Nachrichten (DENM) Absperrtafel-Warnungen). Die gesamte Interaktion zwischen dem Lkw und V2X Komponente ist im Abbildung 29 dargestellt.

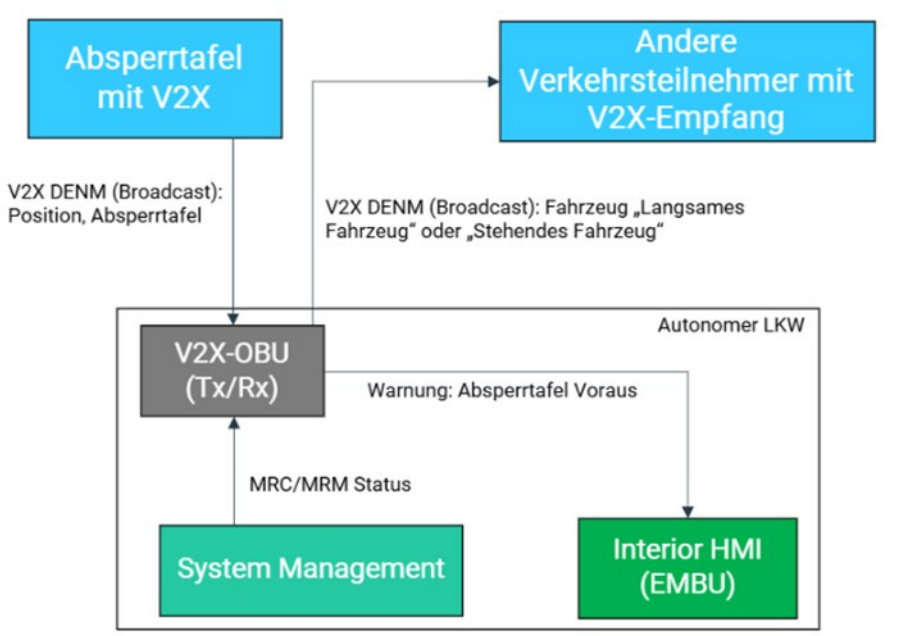



Abbildung 29 Flow-Diagramm vom V2X-Basierten C-ITS Use-Cases

**Minimum Risk Maneuver (MRM) mit V2X (Versenden von Broadcast-V2X-Nachrichten (DENM) bei MRM/MRC-Zustand)**

Diese Funktionalität dient der aktiven Warnung anderer Verkehrsteilnehmer, wenn sich ein autonomer Lkw in einem sicherheitskritischen Zustand befindet. Die Kommunikation erfolgt über DENM (Decentralized Environmental Notification Messages), ein etablierter Nachrichtentyp im C-ITS-Standard. Je nach Zustand des Fahrzeugs und Geschwindigkeit werden unterschiedliche Nachrichten generiert:

- Wechsel von „Autonomes Fahren“ zu „Minimum Risk Condition (MRC)". Diese Nachricht informiert andere Verkehrsteilnehmer über ein langsam fahrendes Fahrzeug, das sich in einem sicherheitskritischen Zustand befindet.
- Zustand MRC, MRM oder „Shadow“ bei Geschwindigkeit < 10 km/h. Diese Nachricht dient als digitales Warndreieck und warnt andere Verkehrsteilnehmer frühzeitig vor einem potenziellen Hindernis oder einem liegengebliebenen Fahrzeug.

**Baustellenwarner mit V2X (Empfang und Verarbeitung von V2X-Nachrichten (DENM) Absperrtafel-Warnungen)**

Diese Funktionalität ermöglicht es dem Fahrzeug, Warnungen aus der Infrastruktur zu empfangen und an den Fahrer oder das autonome System weiterzuleiten. In diesem Szenario erhält der Lkw die DENM-Nachrichten (u. a. Road Works Warning, RWW). Diese Nachricht wird typischerweise von einer Straßeninfrastrukturkomponente (z. B. Absperrtafel mit V2X-Sender) ausgesendet und erreicht das Fahrzeug bis zu 800 Meter vor der Baustelle. Nach dem Empfang der RWW-Nachricht werden relevante Informationen visuell über das EMBU-Display dargestellt („Achtung, Baustelle voraus“) und können vom autonomen System zur Planung der Fahrstrategie genutzt werden. Diese Funktionalität erhöht die Reaktionszeit und Sicherheit im Baustellenbereich erheblich, insbesondere bei eingeschränkter Sicht oder komplexen Verkehrssituationen.

### 3.5.1.2 Architekturframework

Dieser Teil der Architektur widmete sich unter anderem der Konzeption und Entwicklung eines modularen Architekturframeworks zur durchgängigen Modellierung automatisierter Fahrzeugsysteme. Ziel war es, unterschiedliche Systemaspekte – insbesondere Fähigkeiten, Funktionen, technische Komponenten und sicherheitsrelevante Anforderungen – konsistent zu verknüpfen. Das Ergebnis bildet eine tragfähige Grundlage sowohl für die modellbasierte Systementwicklung (MBSE) als auch für die Laufzeitüberwachung sicherheitskritischer Fahrzeugfunktionen.

#### Entwicklung eines modularen Architekturframeworks

Zentrales Ergebnis ist ein in SysML realisiertes Architekturframework, das in fünf strukturierte Gesichtspunkte untergliedert ist. Diese adressieren unterschiedliche Stakeholder-Bedürfnisse und ermöglichen die modellbasierte Beschreibung von:

- Betriebsumgebungen
- Systemfähigkeiten
- Funktionalen Strukturen
- Technischen Realisierungen
- Sicherheitsrelevanten Eigenschaften

Die Grundlage der Kontextmodellierung bildet das aus den Projekten PEGASUS und VVMethoden bekannte 6-Ebenen-Modell, das in ein spezifisches SysML-Profil überführt wurde. Dieses Profil unterstützt u. a. die strukturierte Fähigkeitenspezifikation und erlaubt eine systematische Rückverfolgbarkeit zwischen Fähigkeiten, Funktionen und technischen Komponenten. Damit leistet das Framework auch einen methodischen Beitrag zur Entwicklung von Self-Awareness-Funktionen im Rahmen des Arbeitspakets 8.3.

#### Integration sicherheitsrelevanter Modellierungskonzepte

Ein besonderer Fokus lag auf der Erweiterung bestehender Sicherheitsmodellierungssprachen. Das auf RAAML (Risk Analysis and Assessment Modeling Language) basierende Profil wurde um Elemente ergänzt, die die Abbildung von Sicherheitsanalysen nach dem SOTIF-Standard (ISO 21448) ermöglichen. Darüber hinaus wurden Modellierungskonzepte aus dem in Arbeitspaket 3 entwickelten Verhaltenssicherheitskonzept integriert. Dadurch wird die gleichzeitige formale Berücksichtigung funktionaler Sicherheit (ISO 26262) und Verhaltenssicherheit (SOTIF) innerhalb eines durchgängigen Modells ermöglicht.

#### Grundlagen für systemweites Laufzeitmonitoring

Ein weiteres Ziel war die Ableitung einer Architektursicht zur Unterstützung der Laufzeitüberwachung automatisierter Systeme. Hierfür wurden Korrespondenzen zwischen fähigkeitsbasierten, funktionalen und sicherheitsrelevanten Modellierungsebenen identifiziert und in eine konsistente Struktur überführt. Diese bildet die methodische Grundlage für Monitoring-Architekturen, wie sie in Arbeitspaket 8 gefordert sind – insbesondere im Hinblick auf die Reaktion auf Fehlermodi und die Gestaltung robuster, sicherer Softwarearchitekturen.

**Methodische und wissenschaftliche Einbettung**

Die Konzeption des Frameworks wurde begleitet durch eine umfassende Literaturstudie bestehender Architekturansätze. Dabei wurden insbesondere Stärken und Grenzen etablierter Frameworks im Hinblick auf die Verbindung von Systemfunktionen mit technischen Lösungen analysiert. Die entwickelten Modellierungskonzepte flossen in die wissenschaftliche Bearbeitung von Fragestellungen zur Verhaltenssicherheit ein und bildeten die methodische Basis für einen im Rahmen von Arbeitspaket 3 entstandenen Fachartikeln sowie Dissertationen.

**Zusammenfassung**

Dieser Teil des Arbeitspakets liefert mit dem entwickelten Architekturframework eine robuste Grundlage für die modellbasierte, interdisziplinäre Systementwicklung hochautomatisierter Fahrfunktionen. Die konsistente Verbindung zwischen Fähigkeiten, Funktionen, technischen Komponenten und Sicherheitsanforderungen ermöglicht nicht nur eine nachvollziehbare Systemarchitektur, sondern auch eine fundierte Basis für zukünftige Monitoring- und Absicherungsstrategien. Die Integration sicherheitsrelevanter Modellierungskonzepte stärkt zudem die normgerechte Entwicklung im Spannungsfeld zwischen ISO 26262 und ISO 21448.

### 3.5.2 Tooling (AP 5.2)

Dieser Abschnitt des Arbeitspakets gibt einen kurzen Überblick über die verwendeten Tools und den im Projekt angewandten Softwareentwicklungsprozess.

Ein kohärenter Entwicklungsprozess erfordert eine strukturierte Versionierung und Verknüpfung aller Artefakte. Daher wurden Erweiterungen für das Anforderungsmanagement-System konzipiert, insbesondere zur Darstellung der Operational Design Domain (ODD) und zur Integration wissensbasierter Szenarien.

**Entwicklung einer effizienten Toolchain für C++-Anwendungen**

Die moderne Software-Entwicklungsumgebung für In-Vehicle-Systeme wurde mit dem Ziel konzipiert, den gesamten Lebenszyklus von Softwaremodulen – von der Entwicklung über das Testen bis hin zur Bereitstellung – effizient und skalierbar zu gestalten. Zur Unterstützung einer skalierbaren und effizienten Entwicklungsumgebung kommen moderne Tools, wie Ansible, Docker, GitLab, AWS, Conan und JFrog Artifactory zum Einsatz. Diese Komponenten bilden gemeinsam eine leistungsfähige CI/CD-Infrastruktur, die eine automatisierte, zuverlässige und kontinuierlich optimierbare Softwarebereitstellung ermöglicht.

Im folgenden Schaubild wird der Entwicklungsprozess als eine kontinuierliche, zyklische Schleife dargestellt – ein Symbol für den iterativen Charakter moderner Softwareentwicklung und die fortlaufende Verbesserung von Qualität und Effizienz.

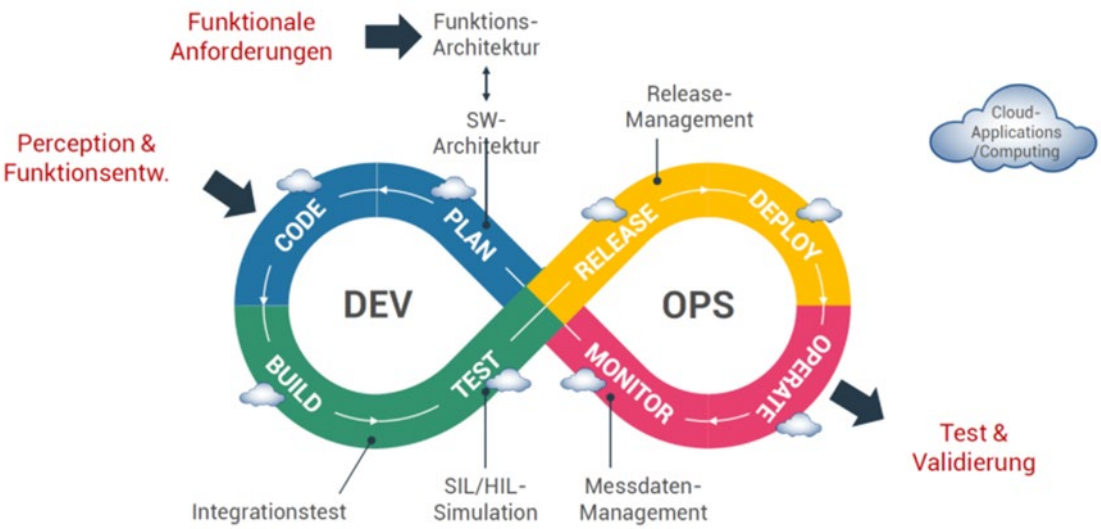



Abbildung 30 Entwicklungsprozess

Die Softwareentwicklungsumgebung unterstützt Entwickler bei der modularen Entwicklung von Softwarekomponenten, die in containerisierten Formaten bereitgestellt werden. Durch die Verwendung von Docker-Containern wird sichergestellt, dass Builds konsistent und plattformunabhängig ausgeführt werden können. GitLab dient als zentrale Plattform für Versionskontrolle, Code-Reviews und die Ausführung automatisierter CI/CD-Pipelines. Diese Pipelines sind so konfiguriert, dass sie bei jeder Codeänderung automatisch Builds auslösen, Tests durchführen und versionierte Artefakte erzeugen.

Ein wesentlicher Bestandteil der Toolchain ist die Integration automatisierter Testframeworks, die Unit-Tests, Integrationstests und Systemtests abdecken. Diese Tests werden kontinuierlich im Rahmen der CI/CD-Prozesse ausgeführt und liefern direktes Feedback zur Codequalität. Fehler können dadurch frühzeitig erkannt und behoben werden, was die Stabilität und Sicherheit der Software erhöhten.

Die erzeugten Artefakte werden eindeutig einer Commit-ID zugeordnet und mit umfangreichen Metadaten versehen. Sie werden in einem zentralen Artefakt-Repository (JFrog Artifactory) abgelegt, das sowohl aktuelle als auch historische Versionen verwaltet. Dies gewährleistet eine vollständige Rückverfolgbarkeit – ein entscheidender Faktor für sicherheitskritische Anwendungen im Fahrzeugbereich.

Ein besonderer Fokus liegt auf der Benutzerfreundlichkeit der Umgebung. Entwickler können über intuitive Kommandozeilen-Interfaces oder grafische Frontend auf alle Funktionen zugreifen. Zusätzlich stehen umfassende Dokumentationen und Tutorials zur Verfügung, die den Einstieg erleichtern und die Einarbeitungszeit verkürzen. Die Umgebung unterstützt sowohl lokale Builds auf Entwicklerrechnern als auch Remote-Builds auf leistungsfähigen Servern, wodurch eine flexible Skalierung je nach Projektanforderung möglich ist.

**Zusammenfassung**

Die Software-Entwicklungsprozess ist ein stark automatisierter Workflow, der auf modernen Technologien wie Infrastructure-as-Code-Technologien (IaC) basiert. Durch den Einsatz von CI/CD-Pipelines wird sichergestellt, dass Softwaremodule gründlich getestet und validiert werden, bevor sie auf die Fahrzeuge ausgerollt werden. Dies verbessert nicht nur die Qualität und Zuverlässigkeit der Software, sondern ermöglicht auch schnelle Iterationen und nahtlose Updates.

### 3.5.3 Messdaten Management (AP 5.3)

Das Messdatenmanagement stellt einen essenziellen Bestandteil der Infrastruktur dar, um autonomes Fahren zu ermöglichen. Es bildet die Grundlage für die effiziente und sichere Übertragung von Fahrzeug-Logs und Sensordaten aus dem Lkw in das Backend-System. Diese Daten sind notwendig, um weiterführende Prozesse wie Analyse, Verarbeitung und die Generierung von statistischen Ableitungen und Berichten zu ermöglichen.

#### 3.5.3.1 Messdaten für verschiedene Nutzergruppen

**Entwickler autonomer Fahrfunktionen**

Für die Entwicklung autonomer Fahrfunktionen sind große Mengen kalibrierter Sensordaten erforderlich, insbesondere in Kombination mit hochgenauen Positionsdaten. Daraus ergeben sich hohe Anforderungen an die Messdatenmanagement-Infrastruktur. Die Daten müssen innerhalb weniger Stunden nach einer Testfahrt für Entwickler verfügbar sein, um eine zeitnahe Analyse und Weiterentwicklung zu ermöglichen.

**Straßenbehörden**

Für den Betrieb autonomer Fahrzeuge auf öffentlichen Straßen hat der Gesetzgeber Anforderungen erlassen, die im Straßenverkehrsgesetz (StVG) und in der Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen (Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung – AFGBV) niedergelegt sind.

Für uns gültig ist derzeit das „Straßenverkehrsgesetz in der Fassung der Bekanntmachung vom 5. März 2003 (BGBl. I S. 310, 919), das zuletzt durch Artikel 16 des Gesetzes vom 2. März 2023 (BGBl. 2023 I Nr. 56) geändert worden ist“.

In der AFGBV werden die Inhalte des StVG ergänzt und mit Details erweitert. Besonders relevant für die Datenaufzeichnung ist die darin enthaltene „Anlage 2“, in der das Format der Daten beschrieben ist.

**Stand:** „Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung vom 24. Juni 2022 (BGBl. I S. 986), die durch Artikel 10 der Verordnung vom 20. Juli 2023 (BGBl. 2023 I Nr. 199) geändert worden ist“

Hierdurch ergibt sich die Notwendigkeit, die Gesetzeslage auch für die Erprobung unserer Prototypen zu beachten.

### 3.5.3.2 Messdatenmanagement im ATLAS-L4 Projekt

Im Rahmen des ATLAS-L4-Projekts wurde ein komplexes Messdatenmanagementsystem aufgebaut, das aus drei Hauptkomponenten besteht (siehe Abbildung 31):

- **Komponente “Data Creation” (Datengenerierung)**
- **Komponente “Data Collection” (Datenerfassung)**
- **Komponente “Data Management” (Datenmanagement)**

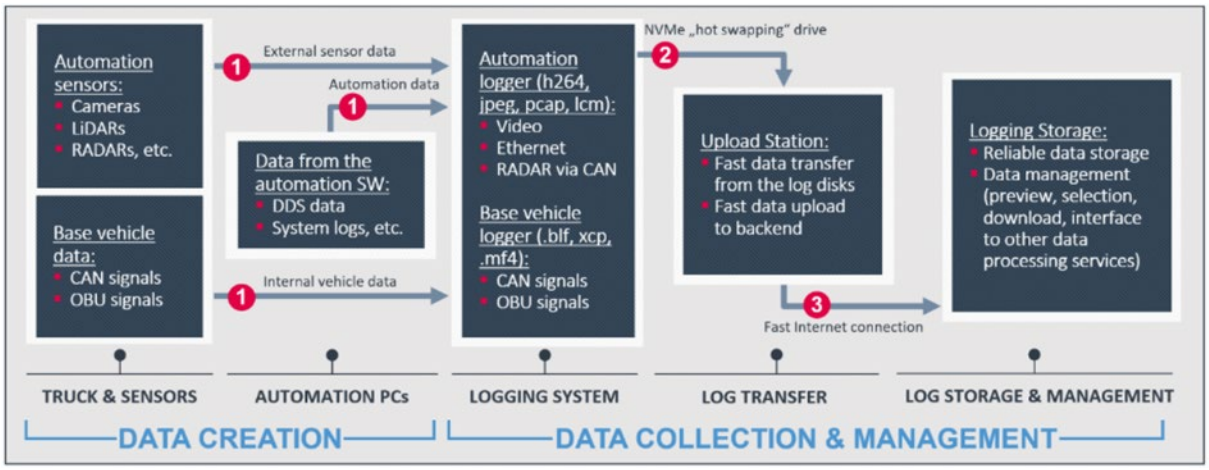



Abbildung 31 Schematische Darstellung von Messdatenmanagement Datenfluss

### 3.5.3.3 Komponente “Data Creation” (Datengenerierung)

Hier werden die Daten von verschiedenen Quellen generiert:

- **Automationssensoren** wie Kameras und LiDARs liefern Daten hauptsächlich über Ethernet-Schnittstellen.
- **Basisfahrzeugsensoren** wie ECUs und OBUs liefern Daten hauptsächlich über CAN-Bus-Systeme.
- Zusätzlich werden die Daten aus Software-Komponenten geloggt, darunter:
  - Ausgewählte Nachrichten zwischen Softwaremodulen
  - System-Logs und Diagnosedaten

### 3.5.3.4 Komponente “Data Collection” (Datenerfassung)

Die Datenerfassung gliedert sich in zwei Bereiche:

- Logger
- Upload-Prozess

#### Logger

Die unterschiedlichen Anforderungen der beiden Use Cases führten zur Entwicklung zweier spezialisierter Logging-Lösungen:

- Automation Logger
- Basisfahrzeug Logger

**Automation Logger:** Eine Software-Komponente, die auf einem Standard-Industrie-PC mit Linux-Betriebssystem läuft. Sie ist für die Erfassung der Daten aus den Automationssensoren zuständig.

Die aufgezeichneten Daten werden – je nach Quelle und Informationstyp – in verschiedenen Formaten gespeichert, unter anderem:

- .**pcap** – für LiDAR-Daten, typischerweise als rohe Netzwerkpakete
- .**dat (DDS)** – für die strukturierte Datenkommunikation zwischen Softwarekomponenten
- .**jpeg und .h264** – für Bild- und Videodaten aus Kamerasystemen

Diese Vielfalt an Formaten ermöglicht eine flexible Weiterverarbeitung und Analyse der Daten in nachgelagerten Systemen.

Mit der zweiten Generation des autonomen Softwareprodukts wurde der Automation Logger direkt in den Automation-PC integriert. Ziel dieser Weiterentwicklung war es, die Anzahl der Hardware-Komponenten zu reduzieren und die Komplexität des Gesamtsystems zu verringern.

**Basisfahrzeug Logger:** Ein speziell entwickelter Linux-PC, der für erhöhte Robustheit ausgelegt ist und die Daten des Basisfahrzeugs erfasst. Die Funktionsfähigkeit dieser Komponente ist Voraussetzung für die Zulassung zum autonomen Fahren im öffentlichen Straßenverkehr. Zur Aufzeichnung findet die Hardware „AUTERA AutoBox“ von dSPACE Verwendung. Dabei handelt es sich um ein „Fahrzeug internes Datenerfassungs-System für Anwendungen im Bereich des autonomen Fahrens". Hier werden interne Zustandsdaten von CVM und der AutoBox erfasst, in einem Zeitraum, der über einen Taster frei vom Benutzer wählbar ist. Damit wird die Funktion des Hochautomatisiertes Fahren / Highly Automated Driving (HAD) Inferfaces protokolliert. Für die Aufzeichnung werden die folgenden Busse herangezogen:

- **CAN:** Die AUTERA AutoBox ist mit allen CAN im Fahrzeug verbunden und zeichnet sämtlichen Datenverkehr auf.
- **Ethernet**: Die Komponenten für das „triggered logging“ sind über Ethernet miteinander verbunden.

**Upload-Prozess**

Analog zum Logging wurden auch beim Upload zwei unterschiedliche Prozesse entwickelt, um den jeweiligen Anforderungen gerecht zu werden:

- **Upload-Prozess – Automation**
- **Upload-Prozess – Basisfahrzeug**

Diese Trennung ermöglicht eine optimierte Verarbeitung der jeweils spezifischen Datenformate und -strukturen.

**Upload-Prozess Automation**
Der Upload-Prozess in der Station umfasst mehrere Schritte

- **Datenübertragung**: Die Daten werden von der NVMe SSD in einen speziell dedizierten On-Premises Speicher kopiert.
- **Archivierung:** Die Daten werden strukturiert archiviert.

- **Weiterleitung ins Backend**: Nach der Archivierung erfolgt die Weiterleitung der Daten in das zentrale Backend-System.
- **Zugänglichmachung für Nutzer:** Im Backend werden die Daten für alle relevanten Nutzergruppen bereitgestellt. Die Daten können nun verwaltet, analysiert und für verschiedene Zwecke weiterverarbeitet werden.

**Upload-Prozess – Basisfahrzeug**

Bei der AUTERA SSD handelt es sich um eine Hot-Swap-fähige, hochleistungsfähige und hochkapazitive Speicherlösung. Sie zeichnet sich aus durch blitzschnelle Datenaufzeichnung und auf umfangreichem, im laufenden Betrieb austauschbarem Speicher.

#### 3.5.3.5 Komponente „Data Management" (Datenmanagement)

Die Speicherung und Verwaltung der Messdaten erfolgt gesetzes- und unternehmenskonform, um sowohl regulatorische Anforderungen als auch interne Richtlinien zu erfüllen. Dabei wird besonderer Wert auf Datensicherheit, Nachvollziehbarkeit und Effizienz gelegt. Die Teilung zwischen Automation und Basisfahrzeug erleichtert die Speicherung und Verarbeitung der Daten.

- **Log Storage und Data Management – Automation**
- **Log Storage und Data Management – Basisfahrzeug**

**Log Storage und Data Management - Automation**

Alle gespeicherten Daten werden mit **Metadaten** angereichert, um ein schnelles und zielgerichtetes Data Management zu ermöglichen. Diese Metadaten umfassen unter anderem:

- Zeitstempel und GPS-Positionen
- Fahrzeug- und Testfahrt-IDs
- Sensortypen und Konfigurationen
- Software-Versionen und Logging-Kontexte

Das Data Management für die Daten vom Automation Logger basiert auf der Databricks-Plattform, die speziell für die Verarbeitung großer Datenmengen und die Zusammenarbeit zwischen Teams ausgelegt ist.

**Log Storage und Data Management - Basisfahrzeug**

Um die besonderen Anforderungen der Straßenzulassung zu erfüllen, wurde das Data Management für die Daten des Basisfahrzeugs Logger separat entwickelt. Hierbei wurde der für die Nachweispflicht notwendige AFGBV Report als pdf-Datei erzeugt und mit den Logfiles abgelegt. Nur dieser Report wird auf Verlangen an das Kraftfahr-Bundesamt (KBA) übermittelt. Er ist mit dem KBA abgestimmt und enthält alle in den Gesetzestexten geforderten Daten.

Das MDM wurde erweitert, um Datasharing und die Bereitstellung dekodierter Daten für alle Nutzer und Stakeholder zu ermöglichen. Es existieren mehrere Stakeholder im ATLAS-L4 Projekt, die eine gemeinsame Postprozessing-Plattform benutzen.

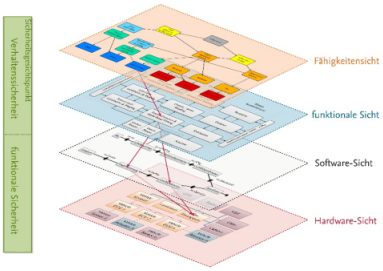
Dafür werden die vorhandenen Daten in einen anderen S3-bucket übertragen, auf den mit dem Tool „Databricks" zugegriffen werden kann. Die Implementierung ist bereits erfolgt. Es werden jedoch keine Reports generiert, da hierfür das MDM ausreichend ist.

### 3.5.4 AP 5 - Vortrag und Poster der Abschlusspräsentation

## AP5: SOFTWARE-PLATTFORM L4

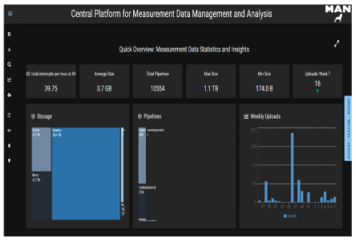
**Architektur, Tooling, MDM**

- Erstellung eines Fähigkeiten-Katalogs (ODD, Szenarien)
- Abbildung der Funktionen in einer funktionalen Schicht
- Schnittstellendefinition und Gewährleistung der Modularität
- Entwurf einer Hardware-Architektur




Systemperspektive für einen Architekturrahmen

- Aufbau einer durchgängigen Software-Toolchain vom Funktions-Build bis zum Fahrzeug-Deployment
  - Containerisierte Entwicklungsumgebung
  - Paketierung & Versionierung der objektorientierten Funktionen
  - Automatischer Build von Binaries und Artefakten
  - HIL/SIL Aufbau für Modul und Fahrzeug-Build-Test
  - Containerisierte Deployment-Methode




MDM – Measurement Data Management

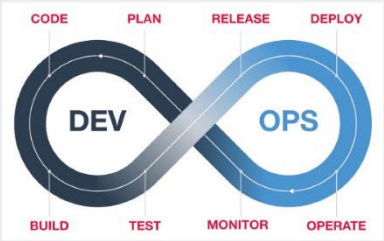
- Messdaten Management System inklusive Anforderungen des Gesetzgebers AFGBV
- CAN/Ethernet Aufzeichnung und Dateninterpretation
- Automatische Report Generierung für AFGBV (PDF) und KPI-Auswertung (GUI)

ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Nebiyat Taye, MAN Truck & Bus SE 41

# SOFTWARE-PLATTFORM L4
## Übersicht

### MOTIVATION UND ZIELE

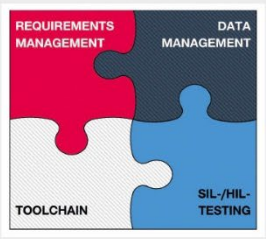
Die Entwicklungsgeschwindigkeit und -effizienz eines größeren Software-Projektes hängt entscheidend von einer klaren Anforderungsdefinition, von der Automatisierung wiederkehrender Aufgaben und dem Einsatz moderner Entwicklungswerkzeuge ab. Das Arbeitspaket „Software-Plattform L4“ zielt darauf ab, eine effiziente Software-Entwicklung zu ermöglichen, indem es CI-Tools und Services für agile Teams bereitstellt und eine benutzerfreundliche Entwicklungsplattform bietet.




DevOps Prozessphasen

### ARBEITSSCHWERPUNKTE

- Darstellung einer Funktionsarchitektur, welche den Aspekten Modularität, Verfügbarkeit, Safety und Testbarkeit Rechnung trägt
- Bereitstellung einer effizienten und durchgängigen Toolkette zur Entwicklung und zum Test von Software
- Weiterentwicklung der Software-Plattform und Anbindung eines Anforderungs-Management-Systems
- Aufbau einer durchgängigen Pipeline zur Messdatenanalyse




Bausteine der Entwicklungsplattform

### ERGEBNISSE

- Konzeption und Realisierung einer skalierbaren Architektur zur Unterstützung komplexer Entwicklungsprojekte
- Einsatz moderner und bewährter Entwicklungsmethoden, kombiniert mit leistungsfähigen Entwicklungsumgebungen zur Steigerung der Effizienz und Qualität
- Aufbau und Inbetriebnahme einer HIL (Hardware-in-the-Loop) und SIL (Software-in-the-Loop) Teststation für die Validierung von Komponenten, sowie kontinuierliche Software-Build-Tests
- Entwicklung und Integration eines leistungsstarken Messdaten-Management-Systems zur effizienten Erfassung, Speicherung und Analyse von Fahrzeugaufzeichnungen
- Erstellung detaillierter Berichte gemäß AFGBV-Richtlinien (z. B. zur Sicherstellung gesetzlicher Konformität und Dokumentation von Testergebnissen)

# TOOLS

## Software-Plattform L4

### HIL-SIMULATION UND INTEGRATIONSTESTS

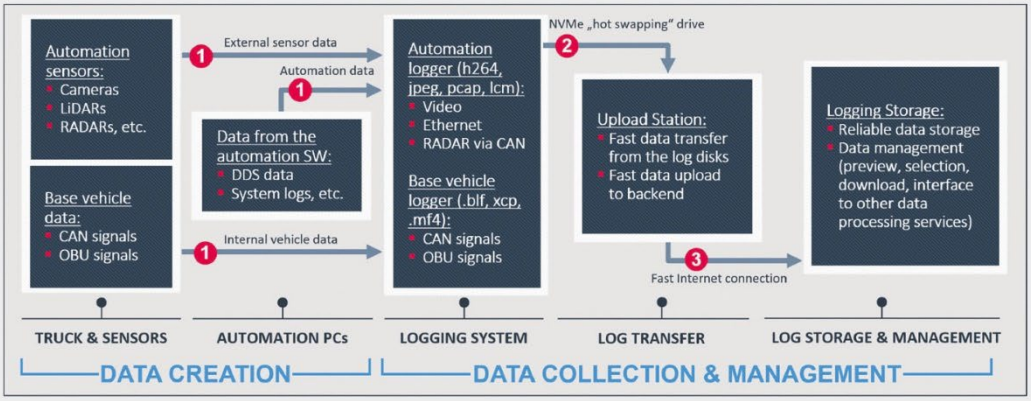
Um die Vorteile eines HiL-Prüfstandes durchgängig im Projekt nutzen zu können, wurde die neueste HW-Generation der autonomen Plattform integriert. Neben dem mechanischen Aufbau und der Installation der grundlegenden HW-Komponenten wurde die SW-Umgebung installiert und in Betrieb genommen. Die Anpassung der CI/CD-Test-Pipelines umfasste die Konfiguration und Integration neuer Tests, um sicherzustellen, dass die Softwarepakete auf der neuen Plattform reibungslos bereitgestellt werden können.


Rechnereinheit der neuen autonomen Plattform

### LOGGING UND PIPELINE FÜR MESSDATENANALYSE

Data Collection

- Logging für das Sensor-Setup des Basisfahrzeugs und des AV-Stacks
- Transfer der Log-Daten vom Fahrzeug zur Upload Station, Data Management im Backend
- Schneller und robuster multi-source Upload
- Frontend mit Preview von Signalverläufen, GPS-Tracks und statistischen Auswertungen




Bestandteile des Konzepts für die Datenaufzeichnung und Messdatenmanagement

# AP 6: Hardware-Architektur L4

Lars Lippert, MAN Truck & Bus SE

## 3.6 AP 6: Hardware-Architektur L4

*Arbeitspaketleitung: Lars Lippert, MAN Truck & Bus SE*

Im Rahmen des Projektss ATLAS-L4 wurden mehrere Fahrzeuge als Versuchsträger aufgebaut. Ein Sensorfahrzeug zur Erprobung der Sensorik und zur Funktionsentwicklung, ein Demonstrationsfahrzeug zur Veranschaulichung des ADS-Konzeptes, ein Bordnetzfahrzeug zur redundanten Bordnetzentwicklung (Kooperation mit dem Projektpartner LEONI), ein ARB-Fahrzeug zur Erprobung redundanter Komponenten (Kooperation mit den Projektpartnern Bosch –Lenksystem – und Knorr Bremse – Bremssystem), als auch ein Teleoperationsfahrzeug (Kooperation mit dem Projektpartner FERNRIDE). Eine Übersicht der Fahrzeuge ist im Kapitel 3.6.6 (Poster Hardware-Architektur L4) tabellarisch dargestellt.

### 3.6.1 ECU / Rechner-Topologie (AP 6.1)

Das AP 6.1 beschreibt die Entwicklung von Automation-Hardware-Architekturen und die Integration dieser in das Sensorfahrzeug und das Demonstrationsfahrzeug sowie deren HIL-Prüfstands-Testumgebungen. Ein Schwerpunkt liegt auf dem Aufbau und der Kühlung der Rechnersysteme sowie dem Aufbau der Sensorsysteme, als auch der Inbetriebnahme der HIL-Prüfstände zur frühzeitigen Funktionserprobung.

- **Architektur- und Konzeptionsarbeiten**: Für das Sensorfahrzeug wurden die Hardwarekomponenten definiert und verbaut. Die Arbeiten an der Rechner- und Kühlungsarchitektur wurden abgeschlossen. Die Konzeptarbeiten für das Demonstrationsfahrzeug wurden durchgeführt und ein Rechnersystem ausgewählt und verbaut. Hierbei handelt es sich um eine Evolutionsstufe der Rechnersysteme des Sensorfahrzeugs.
- **HIL-Prüfstand Entwicklung**: Der HIL-Prüfstand wurde hardwareseitig fertiggestellt und softwareseitig in Betrieb genommen. Zur Unterstützung der Softwareentwicklung wurden sowohl Komponenten des Sensorfahrzeugs als auch des Demonstrationsfahrzeugs in den HIL integriert, um frühzeitige Tests zu ermöglichen. Abbildung 32 zeigt den Aufbau des HIL-Prüfstands.

Abbildung 32 Aufbau des HIL-Prüfstands im Labor

- **Sensor- und Kühlkonzepte:** Für das Sensorfahrzeug wurde eine Sensorarchitektur definiert und eine Luftkühlung für die Rechner umgesetzt und getestet. Das Demonstrationsfahrzeug wurde mit einer leistungsstärkeren wassergekühlten Lösung ausgestattet. Zudem wurde ein mechanisches Konzept zur Verstärkung der Sensorhalter entwickelt, um Vibrationseinflüsse zu minimieren. Abbildung 33 veranschaulicht die Verstärkung der Sensorhalter sowie die installierte Wasserkühlung.

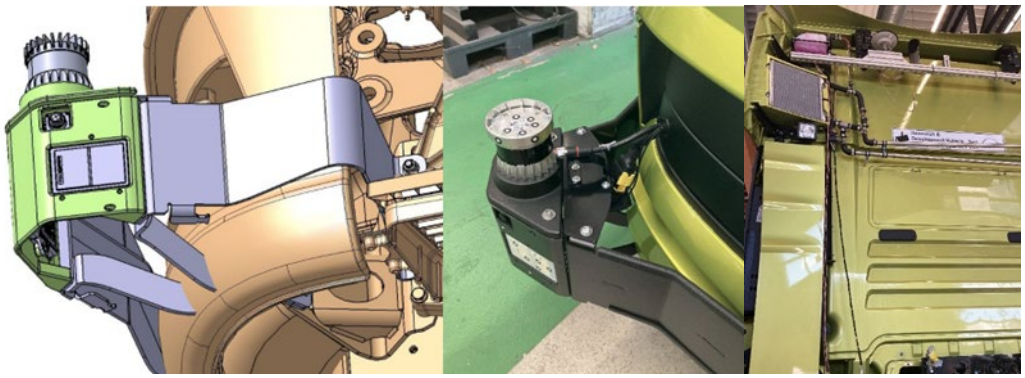


Abbildung 33 Verstärkung der Sensorhalter (links) und Verbau der Wasserkühlung (rechts)

- **Integration und Optimierung im Demonstrationsfahrzeug:** Im Demonstrationsfahrzeug wurde ein leistungsstärkeres Rechnersystem eingebaut, eine redundante Bremse und eine EAS2-Lenkung integriert. Probleme mit dem GPS-Empfang wurden analysiert und behoben. Abbildung 34 (linke Seite) zeigt die wassergekühlten Rechner im Demonstrationsfahrzeug. Abbildung 34 (rechte Seite) zeigt das verbaute Rechnersystem im Sensorfahrzeug.

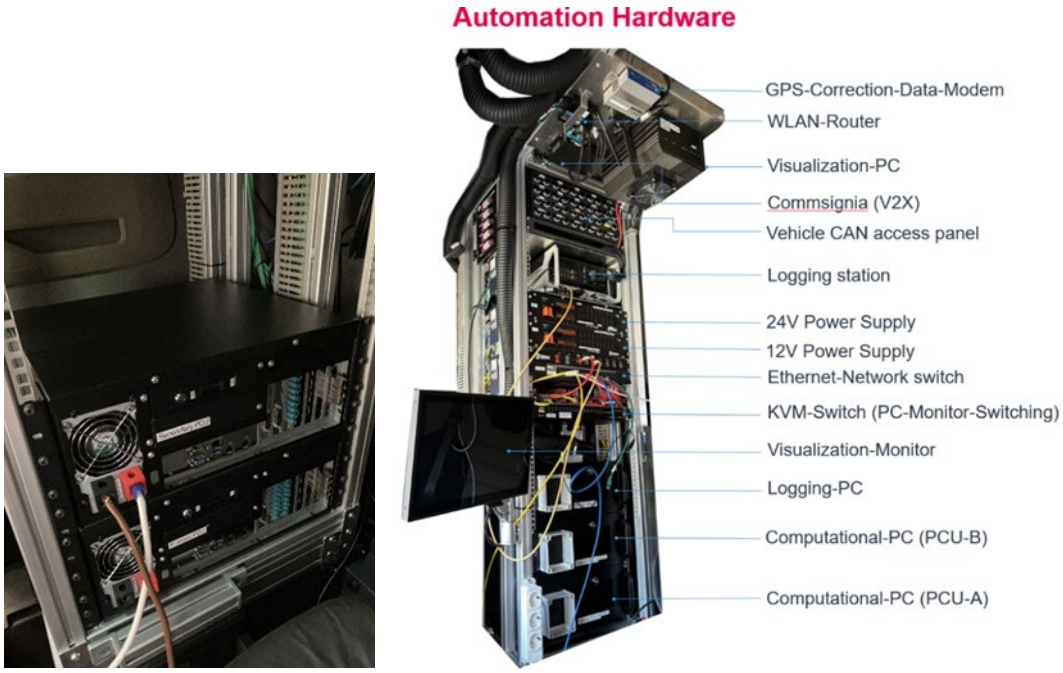



Abbildung 34 Rechner im Fahrzeug

### 3.6.2 Fahrzeugaufbau / Schnittstellen (AP 6.2)

Das AP 6.2 beschreibt den Fortschritt beim Aufbau und der Ausstattung des Sensorfahrzeugs, des Demonstrationsfahrzeugs und der Partnerfahrzeuge (ARB-Fahrzeug, Teleoperationsfahrzeug – FERNRIDE) im Rahmen des ATLAS-L4 Projekts, einschließlich der Bewältigung von Lieferverzögerungen und der Integration von Sensorik und redundanten Systemen.

- **Lieferverzögerungen und Fahrzeugbereitstellung:** Zu Projektbeginn wurden die ersten Fahrzeuge konfiguriert und bestellt, jedoch führten geopolitische Umstände zu etwa sechsmonatigen Lieferverzögerungen, was insbesondere die Bordnetzentwicklung beim Partner Leoni beeinträchtigte. Zwischenzeitlich wurde ein älteres Fahrzeug als Übergangslösung genutzt. Die Lieferung der endgültigen Fahrzeuge erfolgte dann im Oktober 2022.
- **Fahrzeugumbau und Grundaufbau:** Im Sensorfahrzeug, dem Demonstrationsfahrzeug, dem ARB-Fahrzeug, als auch dem Teleoperationsfahrzeug (FERNRIDE), wurden Umbauten wie eine zweite Sitzreihe, Spannungsversorgung, CAN-Abgriffe, Grundaufbauten und Halterungen für Steuergeräte und Verkabelungen vorgenommen. Sicherheitskonzepte mit Notaus-Schaltern für Fahrzeugkomponenten wurden für alle Fahrzeuge umgesetzt. Abbildung 35 zeigt das Sensorfahrzeug von außen, sowie das Rechnerrack im Inneren.


Abbildung 35 Sensorfahrzeug und Rechnerrack

- Sensorik und Kalibrierung: Die Inbetriebnahme und Kalibrierung der Sensorik am Sensorfahrzeug sowie dem Demonstrationsfahrzeug wurde abgeschlossen. Danach konnte mit fortlaufenden Softwaretests und regelmäßigen Testfahrten auf Prüfgeländen sowie öffentlichen Autobahnen (im Rahmen der erhaltenen AFGBV-Erprobungsgenehmigung) zur Optimierung der Automationsalgorithmen begonnen werden. Eine neue Kalibrierhalle wurde aufgebaut, um vor allem die Kalibrierung der Longrange-Sensorik zu optimieren.

Abbildung 36 zeigt anhand eines 3D-Modells die Sensorik des Demonstrationsfahrzeugs. Abbildung 37 zeigt den Fahrzeugaufbau von außen.

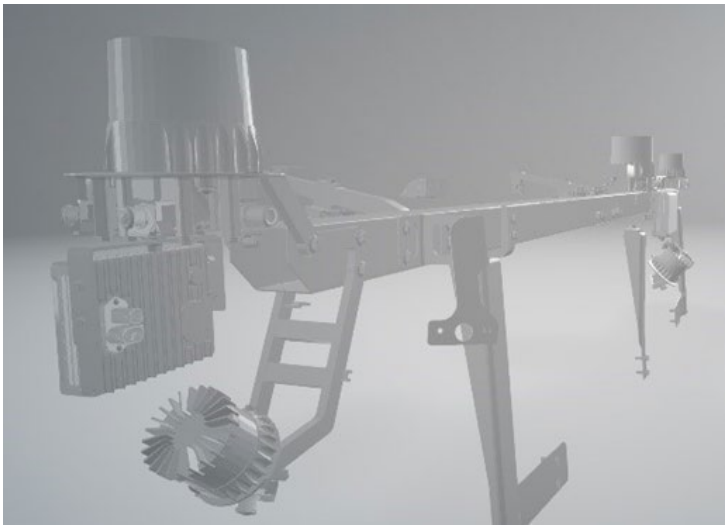


Abbildung 36 Sensorik des Demonstrationsfahrzeugs

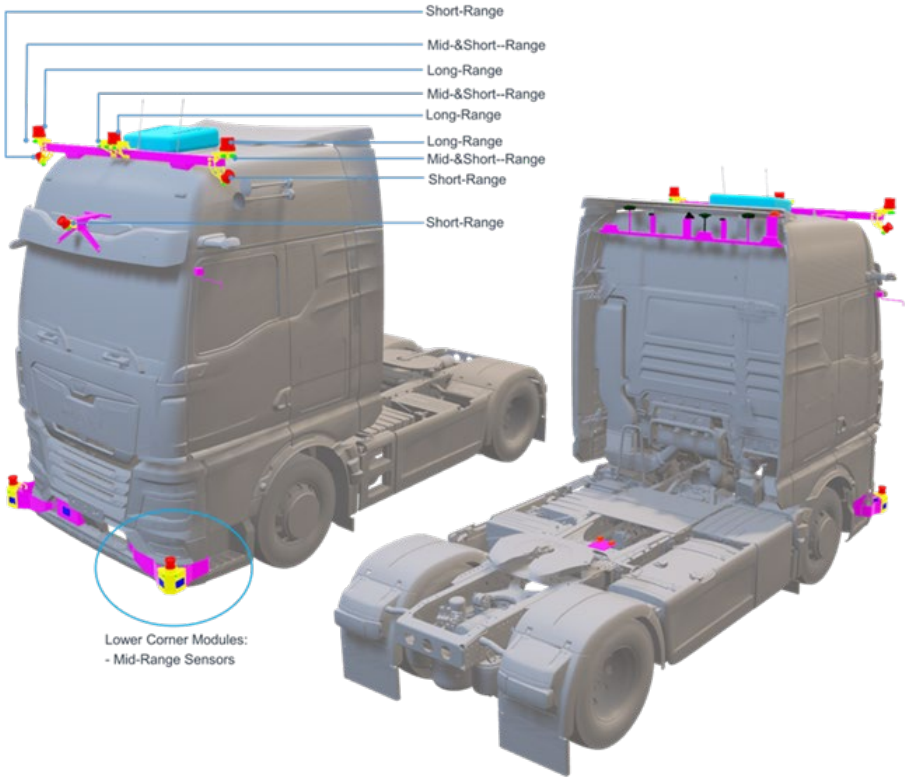



Abbildung 37 3D-Modell des Fahrzeugaufbaus

- Sicherheits- und Testsysteme: Die redundante Bremse und die redundante Lenkung wurden im ARB-Fahrzeug in Betrieb genommen, eine Interfacebox zur Testung der redundanten Systeme installiert und ein Display für Live-Datenvisualisierung verbaut. Das Notauskonzept wurde in allen Fahrzeugen umgesetzt, um die Sicherheit in den Fahrzeugen zu gewährleisten. Zudem wurde ein Lkw für teleoperiertes Fahren mit dem Partner FERNRIDE aufgebaut (Teleoperationsfahrzeug). Abbildung 38 zeigt das Display zur Live-Datenvisualisierung, als auch die Interfacebox zum Testen der redundanten Systeme

Abbildung 38 Datenvisualisierung und Interfacebox für redundante Systeme

### 3.6.3 Bordnetz (AP 6.3)

Im Rahmen des Forschungsprojekts ATLAS-L4, wurde von LEONI ein innovatives Konzept für ein fehlertolerantes Energiebordnetz entwickelt und validiert. Ziel war es, die Energieversorgung sicherheitskritischer Funktionen auch bei Fehlern zuverlässig sicherzustellen. Die Elektronik spielt dabei eine zentrale Rolle, insbesondere durch den Einsatz von intelligenten Leistungsverteilern (ePDB).

Die Motivation für das Projekt lag im Aufbau von Know-how im Bereich automatisiertes Fahren sowie in der Entwicklung eines hochverfügbaren Energieversorgungssystems. Gemeinsam mit Partnern im Konsortium wurden zunächst die Anforderungen an die elektrische Energieversorgung erarbeitet und deren Auswirkungen auf die E/E-Architektur analysiert. Daraus resultierte unter Berücksichtigung der funktionalen Sicherheitsanalyse die Entwicklung eines Konzepts, das sowohl einen intelligenten Leistungsverteiler als auch zwei redundante Kabelsätze als zentrale Entwicklungskomponenten umfasst. Die Validierung erfolgte durch gezielte Fehlerinjektionen, etwa durch Kurzschlüsse in statischen Tests.

Ein weiteres sehr relevantes Thema war die funktionale Sicherheit. Neue Anforderungen an sicherheitsrelevante Verbraucher und die Notwendigkeit, systematische Fehler zu vermeiden, führten zu einer Architektur mit zwei voneinander unabhängigen Energiekanälen. Diese beiden Kanäle erfüllen Anforderungen gemäß ISO 26262 sowie der VDA 450 nach ASIL B(D) und ASIL D und gewährleisten die Durchführung sicherheitsrelevanter Manöver sowie dem Minimum-Risk-Manövern.

Das redundante Bordnetz basiert auf der Architektur des Serienfahrzeugs und wird ohne Modifikation dessen implementiert. Das redundante Bordnetz besteht aus zwei Redundanzpfaden (Grün/Blau, siehe Abbildung 39), einer zusätzlichen Energiequelle (HAD-Batterie) und einem intelligenten Leistungsverteiler pro Redundanzpfad. Diese Erweiterung ermöglicht es, hochautomatisierte Fahrfunktionen unabhängig vom konventionellen Bordnetz zu betreiben und erhöht somit die Ausfallsicherheit und Systemverfügbarkeit. Im Laufe der Untersuchungen, aber auch durch Simulationen und Fahrzeugmessungen gestützt, hat sich gezeigt, dass Schmelzsicherungen ab einem Sicherungswert von 25 A beim Auslösen zu Unterspannungen im Bordnetz führen, die die Sicherheitsziele verletzen. Alle Sicherungswerte ab 25 A wurden daher als Halbleiterschalter ausgeführt und in elektronischen Leistungsverteilern integriert.

Die Verteilung der Verbraucher für das HAD hat ergeben, dass es günstig ist, zwei HAD-Leistungsverteiler am Chassis und zwei in der Kabine zu platzieren. Die Leistungsverteiler am Chassis wurden als Elektronik ausgeführt und beinhalten die Ausgänge für die einzelnen Verbraucher, die Trennschalter zum QM Bordnetz und die Anschlüsse für die HAD-Batterien. Die Leistungsverteiler in der Kabine wurden als reine Schmelzsicherungsboxen (FB) realisiert.

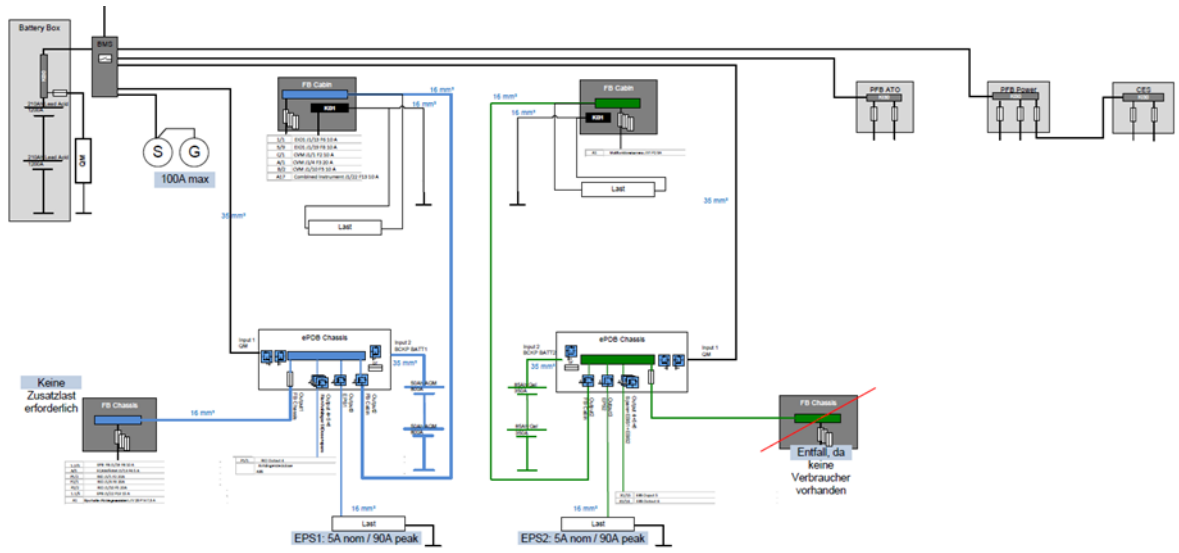



Abbildung 39 Architektur des Energiebordnetz

Der ePDB verfügt über sechs Ausgänge, die kommandiert geschaltet werden können. Er bietet Schutzfunktionen wie Überstrom-, Leitungs- und Übertemperaturschutz, erkennt Über- und Unterspannungen und kommuniziert über den CAN-Bus. Die Diagnosefunktionen umfassen Strom-, Spannungs- und Temperaturmessungen. Die Hardware ist passiv gekühlt, nutzt Hochstromverbindungstechnik und basiert auf einem AUTOSAR-Betriebssystem.

Die Schutzmechanismen des ePDB kombinieren Hardware- und Software-Schwellen, um sowohl schnelle als auch langsame Überströme sicher zu erkennen und zu isolieren. Die Vorteile dieser Lösung liegen in der Gewichtseinsparung, zentralen Steuerbarkeit, frühzeitigen Fehlererkennung und erhöhten Systemsicherheit. Herausforderungen bestehen in der Komplexität, den Kosten, der funktionalen Sicherheit (ASIL) sowie in Cybersecurity- und EMV-Anforderungen.

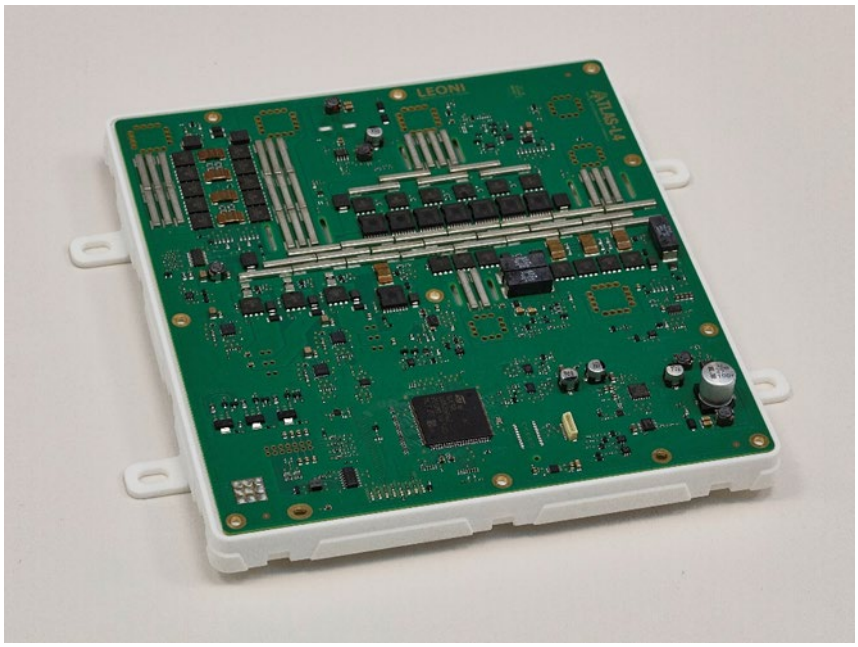



Abbildung 40 Intelligenter Leistungsverteiler (ePDB)

Zur Validierung wurde ein umfangreiches Testsetup aufgebaut. Es umfasste statische Messungen, Fehlerinjektionen und die Integration der LEONI entwickelten Komponenten in einem Prototyp -Fahrzeug. Die Tests zeigten, dass die elektronischen Sicherungen Kurzschlüsse innerhalb der für die unterbrechungsfreien Funktion aller Steuergeräte erforderlichen 100 Mikrosekunden isolieren können. Zudem wurde die Rückwirkungsfreiheit zwischen den Energiekanälen nachgewiesen (siehe Abbildung 41). Brach die Spannung auf Verbraucherebene bei Kurzschlüssen in der Basisarchitektur auf bis zu 16 V ein, konnten die ergriffenen Maßnahmen diese Spannung um bis zu 12 V auf 28 V stabilisieren und dadurch eine erhöhte Spannungsstabilität gewährsleisten.

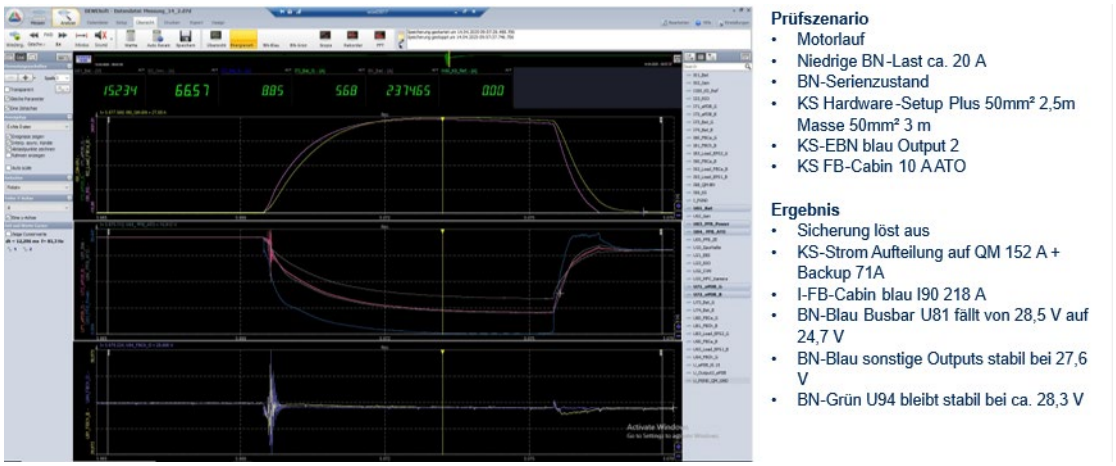



Abbildung 41 Systemergebnis der Rückwirkungsfreiheit

Zusammenfassend lässt sich sagen, dass das entwickelte Energiebordnetzkonzept die Anforderungen für automatisiertes Fahren erfüllt. Es kombiniert klassische und elektronische Absicherungstechnologien, stellt die Unabhängigkeit der Systeme sicher und erhöht die Verfügbarkeit sicherheitskritischer Verbraucher. Damit wurde ein wichtiger Schritt in Richtung sicherer und zuverlässiger autonomer Mobilität gemacht.

### 3.6.4 Lenksystem (AP 6.4)

Aus Sicht der Lenkungsentwicklung war die Anforderung des Projekts ein Lenksystem zur Verfügung zu stellen, welches es ermöglicht das Fahrzeug autonom zu steuern und gleichzeitig den Sicherheitsstandards zu genügen. Zusätzlich sollte noch herausgefunden werden, welche Anforderungen ein zukünftiges Lenksystem ebenfalls erfüllen muss.

**Projektziel aus Lenkungssicht**

Zunächst wurden nach den Architekturtreibern für die Lenkung der nächsten Generation gesucht. Als die beiden relevantesten Technologietreiber wurden der Fahrermangel und somit der Bedarf an SAE L4 Anwendungen als auch das steigende Umweltbewusstsein und somit die Elektrifizierung des Antriebstrangs identifiziert.

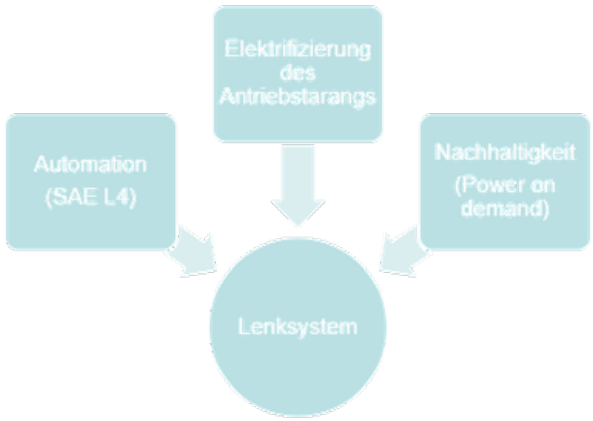



Abbildung 42 Neue Architekturtreiber für Nutzfahrzeuglenkungen der neuen Generation

Gleichzeitig muss das Lenksystem für zukünftige Lkw-Generationen ebenfalls den bisherigen Anforderungen und dem Einbauraum genügen. Ziel war es ein Lenksystem zu definieren, einen Prototyp aufzubauen und diesen dann auch im Zielsystem (Fahrzeug) zu testen.

**Auswahl des geeigneten Lenksystems**

Während mit einem rein hydraulisches Lenksystem ein automatisierter Fahrmodus nicht möglich ist, kommt nur eine elektrohydraulische oder voll elektrische Lenkung in Betracht. Eine elektrohydraulische Lenkung kann mit einer elektrischen Pumpe betrieben werden. Die hydraulische Grundlast und hydraulische Peripherie werden weiterhin benötigt, weshalb eine voll elektrische Lenkung als energetisch besser bewertet wurde.

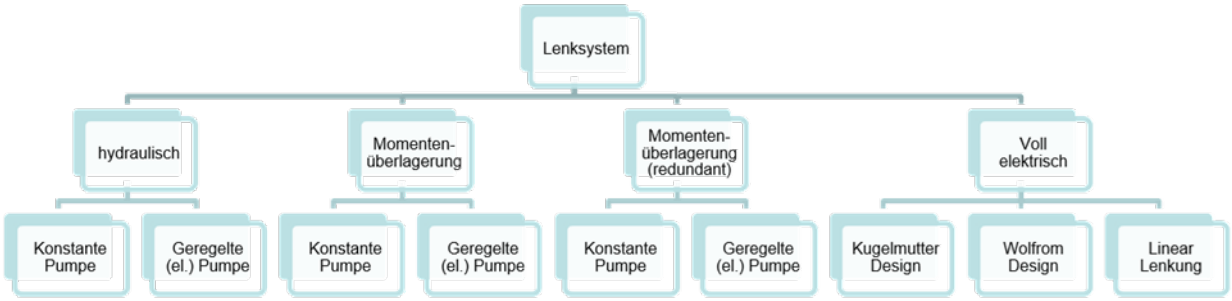



Abbildung 43 Wirkprinzipien und Konzepte für NKW Lenkungen

Das gewählte Design (Vollelektrisch mit Kugelmutter Design) erfüllt am besten alle Anforderungen. Sowohl im Automatisierungsgrad als auch im Energiebedarf über das Kollektiv. Die Wahl für das KM Design ist auf das Packaging zurückzuführen, da nahezu alle aktuellen Anwendungen KM Lenkungen sind und somit der Bauraum für diese Technologie grundsätzlich berücksichtigt ist.

**Entwicklung des Ziellenksystems**

Da das mechanische Zieldesign besteht aus einem Basegear, welches von außen wie eine KMH Lenkung aussieht, jedoch ist der Kraftfluss im Basegear durch die Spindel angetrieben und nicht wie bei einer KMH durch die Kolbenbewegung. Die Schnecke im Basegear wird mittels zwei ServoEinheiten (oben und unten) durch einen Elektromotor angetrieben. Das Signal des Elektromotors kommt entweder über den Sensor (Fahrerwunsch) oder kann auch über eine Schnittstelle mittels eines CAN Signals aktiviert werden

Abbildung 44 Ziellenksystem auf dem Prüfstand

Vorteile dieses Designs sind:

- Kompakte Bauweise
- Redundante EE Architektur (2 getrennte Motoren), somit HAD fähig
- Power on demand System, somit Energieeinsparpotential

**Erprobung des Lenksystems**

Das Lenksystem wurde zunächst auf dem Prüfstand getestet (siehe Abbildung 44) bevor es in ein Fahrzeug eingebaut wurde. Diese Erprobung beinhaltete die Verifizierung, also die Konformität mit den Anforderungen als auch die Validierung, also das Überprüfen des Lenksystems in der Zielumgebung (Fahrzeug) in echten Lebenszyklen wie Straßen Erprobung und Tieftemperatur Erprobung.

Abbildung 45 Wintererprobung des Lenksystems im Fahrzeug

Hierfür wurden Freigabetests durchgeführt, so dass eigene geschulte Fahrer das Fahrzeug auf öffentlichen Straßen bewegen können. Zusätzlich wurde auch eine Wintererprobung durchgeführt, in welcher die Applikation und das Lenkverhalten bei niedrigen Umgebungstemperaturen überprüft wurde. Außerdem konnte ein Vergleich erstellt werden, welcher darstellt wie groß das Energieeinsparpotential für die Systemfunktion Lenken ist.

Tabelle 3: Vergleich der Leistungsaufnahme von elektrischen Lenksystemen zu hydraulischen Lenksystemen

| | **Durchschnittlicher Leistungsbedarf elektrisches LS r** | **Durchschnittlicher Leistungsbedarf hydraulisches LS** | **Einsparpotential** |
|---|---|---|---|
| Europa Nahverkehr (0.8 mio. km) | 105 W | 845 W | 88% |
| Langstrecke (1.5 mio. km) | 45 W | 719 W | 94% |

**Fazit**

Im Rahmen des Projekts wurde ein Lenksystem entwickelt, welches die Anforderungen an hochautomatisiertes Fahren erfüllt. Zusätzlich weist es deutliche Vorteile im Energiebedarf hat, wodurch das System attraktiv für alle Fahrzeugtypen (ICE, BEV und FCEV) ist. Der Funktionsnachweis wurde zunächst auf dem Prüfstand und dann später im Zielsystem (Fahrzeug) auch in Tieftemperaturumgebung erprobt. Die redundante Ausführung des EE Pfades ermöglicht auch die sichere Ansteuerung der Lenkfunktionen mittels der HAD Schnittstelle, die ebenfalls im Projekt prototypisch dargestellt wurde. Der Nachweis über eine signifikante Energieeinsparung konnte ebenfalls erbracht werden.

### 3.6.5 Bremssystem (AP 6.5)

Neben Bordnetz (AP 6.3) und Lenkung (AP 6.4) ist die Bremse das dritte hardwarebasierte System, das aus Sicherheitsgründen redundant ausgelegt werden muss, um den Wegfall des menschlichen Fahrers als Sicherheitsinstanz zu kompensieren. Ziel muss es sein, dass unter allen Umständen noch gebremst werden kann. Besondere Verantwortung wird darüber hinaus mit der Funktion „Steer-by-Brake“ übernommen, die bei einem Ausfall des primären Lenksystems greift.

### Zusammenfassende Ergebnisdarstellung

Das Vorhaben wurde in vier Arbeitspakete unterteilt, die aufeinander aufbauen, allerdings gleichzeitig nicht als strenge sequenzielle Folge zu verstehen sind. Vielmehr wurden neu gewonnene Erkenntnisse immer wieder dazu genutzt, auch konzeptionelle Aspekte zu überdenken und gegebenenfalls weiter zu optimieren. Im Folgenden werden die Arbeitspakete und ihre Ergebnisse vorgestellt.

### Planung und Konzeptionierung

Grundsätzliche konzeptionelle Überlegungen zum Aufbau des redundanten Bremssystems wurden bereits im Vorfeld des Vorhabens angestellt und in der Vorhabensbeschreibung dargelegt. Eine Detailierung dessen erfolgte gemeinsam mit MAN auf Basis eines Lastenheftes. Zu den grundlegenden Eigenschaften des Systems gehört die Skalierbarkeit. Im ersten Schritt und Gegenstand des ATLAS-L4 Projekts ist eine Lösung, die bei Ausfall eines primären Systems (Lenkung, Bordnetz oder Bremse) ein Weiterfahren bis zur nächsten Möglichkeit eines Minimum Risk Maneuvers erlaubt. Gleichzeitig soll das System so skalierbar sein, dass künftig auch ein „Mission Complete“ in Aussicht stellt, was durch Vorhalten eines tertiären Bremssystems in Form einer erweiterten Parkbremse ermöglicht wird. Die Konzeption des redundanten Bremssystems war darüber hinaus von der Idee geleitet, dass eine reine Dopplung des heutigen, elektronischen Bremssystems weder aus technischer noch später aus kommerzieller Sicht Sinn macht (siehe Verwertungsplan). Daher hat sich Knorr-Bremse für die Kombination zweier Bremssysteme entschieden, die für sich betrachtet aus Serienlösungen abgeleitet sind und sich ein Teil der Hardware in Form von druckregelnden Ventilen und Sensorik teilen. Eine Stärke des Ansatzes ist es, dass das primäre und das sekundäre System vergleichbare Bremsperformance aufweisen und beide die gesetzlich geforderten Standards bezüglich Mindestverzögerung übertreffen. Ein bewusst eingegangener Kompromiss und Teil der initial beschriebenen Iterations- und Untersuchungsschleifen war die Entscheidung eines dreikanaligen ABS im Backup. Bei der finalen Zielarchitektur hat man sich hier nach ausführlichen Vergleichen gegen einen vierkanaligen Ansatz entschieden, der weitere Funktionen wie Traktionskontrolle und ESP ermöglichen würde. Im Sinne der Skalierbarkeit sind die technischen Voraussetzungen dafür aber nach wie vor auch in der redundanten ECU vorgehalten.

### Erstmusterrunde

Im ersten Projektjahr 2022 entstanden für alle Produkte Funktionsmuster, die auf Basis des mit dem Konsortialpartner MAN abgestimmten Lastenhefts entwickelt wurden. Diese wurden dem Prozess folgend zunächst für sich betrachtet validiert. Grundlage dessen sind die Testpläne, die Knorr-Bremse für seine pneumatischen und mechatronischen Standardkomponenten vorhält und die für den neuen Einsatzzweck angepasst wurden. Es ist festzuhalten, dass der Übergang zwischen der Produktvalidierung und der des Systems fließend ist. Ein Teil der Produktanforderungen kann abschließen nur im System überprüft werden. Dazu gehört die Validierung der Elektromagnetische Verträglichkeit (EMV) nach ISO-Standard oder die für die spätere Homologation relevanten Schwell- und Lösezeiten des pneumatischen Bremssystems. Der erfolgreiche Abschluss des „Design und Validation Plans“ (DVP) ist die Basis von Produktreleases. Diese lagen Ende 2022 in Form von Straßenfreigaben für sämtliche Komponenten vor. Die identifizierten Abweichungen der Erstmuster von den Zielanforderungen wurden in der nächsten B-Musterrunde adressiert, die dann ebenfalls im ATLAS-L4 Vorhaben ausgerollt wurde.

**Darstellung der ersten Version der Zielarchitektur**

Die Zielarchitektur des redundanten Bremssystems umfasst Aspekte des pneumatischen und elektrischen Layouts sowie des CAN-Netzwerks. Letzteres stellt die redundante Kommunikation zwischen den beiden ECUs des Bremssystems sowie zu dem übergeordneten HAD-System sicher. Die Umsetzung des Konzepts erfolgte zunächst in einer Hardware-in-the-Loop (HiL) Prüfstand. Hier kann das Bremssystem mittels Umgebungssimulation unter kontrollierten Bedingungen stimuliert und untersucht werden. Neben grundlegenden Untersuchungen zu Projektbeginn ist der HiL-Prüfstand fester Bestandteil bei der weiteren Optimierung und Freigabe des Systems. Im zweiten Halbjahr 2022 wurde das Bremssystem erstmalig in einem Versuchsträger installiert, der dann Anfang 2023 nach Arjeplog/Schweden zwecks ausführlicher Wintertests überführt wurde. Exemplarisch als wichtige Erkenntnisse aus dieser Projektphase soll der Umgang mit den zwischen primärem und sekundärem Bremssystem geteilten Komponenten hervorgehoben werden. Hierzu gehören die aktiven Raddrehzahlsensoren. Nach anfänglichen Auffälligkeiten konnten diese durch ein angepasstes Massekonzept im Fahrzeug behoben werden.

Nach Knorr-Bremse internen Versuchen wurde die initiale Version der Zielarchitektur im ersten Quartal 2023 auch für den Konsortialpartner MAN freigegeben und in einem Schwesterfahrzeug (Bordnetzfahrzeug) installiert.

**Darstellung Zielarchitektur sowie Erreichung der Zielreife des Systems**

Nach der beschriebenen Erstmusterrunde und der ersten Version der Zielarchitektur verfolgten MAN und Knorr-Bremse eine iterative, gemeinsame Entwicklung, bei der neue Versionen des Bremssystems im Rahmen von Systempaketen geteilt wurden. In Abhängigkeit von der erzielten Testabdeckung und nachgewiesenen Reife gab Knorr-Bremse diese zunächst für Prüfstandsuntersuchungen und darauf aufbauend für Fahrzeugversuche auf Teststrecke und final öffentlichem Straßenverkehr frei. Das ATLAS-L4 Vorhaben umfasste in Summe fünf Systempakete, wobei ab der Straßenfreigabe des vierten Pakets die im Vorhaben beschriebene Operational Design Domain (ODD) abgedeckt ist. Das finale, fünfte Paket dient der Erhöhung des Reifegrades bezüglich Soft- und Hardware. Im Bereich der Hardware wurden in dem Zuge eine neue Generation der ECUs eingeführt, die unter anderem Verbesserungen bei der EMV beinhalten. Die finale Software beinhaltet Performanceverbesserungen, u. a. im Bereich der Übergabe von primärerem auf sekundäres System sowie Steer-by-Brake, was als Backup bei Ausfall des primären Lenkungssystems zum Einsatz kommt.

Während der Abschlusspräsentation in Penzing im Mai 2025 wurde der finale Stand des redundanten Bremssystems im Rahmen von Fahrversuchen demonstriert. Das erhaltene Feedback bewertet Knorr-Bremse als durchweg positiv und bestätigt unser Anliegen an diesem Zukunftsthema mit seinen Partnern weiterzuarbeiten.

## 3.6.6 AP 6 - Vortrag und Poster der Abschlusspräsentation

### AP6: FAHRZEUGAUFBAU

**Fahrzeugüberblick**

Im Rahmen des ATLAS-L4 Projektes werden vier Fahrzeuge aufgebaut:

- **Sensorfahrzeug**
  - Erstes Automation Fahrzeug
  - angepasste Fahrzeugarchitektur
  - überarbeitetes Sensorkonzept
  - Hochleistungs-Automation-Computer

- **Demonstrationsfahrzeug**
  - zweites Automation Fahrzeug
  - gleiches Sensorkonzept wie Sensorfahrzeug
  - Hochleistungs-Automation-Computer

- **ARB-Fahrzeug**
  - redundante Fahrzeugkomponenten
    - redundante Lenkung BOSCH Invented for life
      - Prüfstandsversuche
      - Erprobung unter Realbedingungen
    - redundante Bremse KNORR-BREMSE
      - Konzeptionierung, Implementierung und Erprobung eines redundanten Bremssystems mit anschließender Straßenfreigabe für das Gesamtfahrzeug
      - Inkl. Sicherheitskonzept, Health Monitoring, Handover auf red. System sowie Steer-by-Brake als Lenkredundanz.

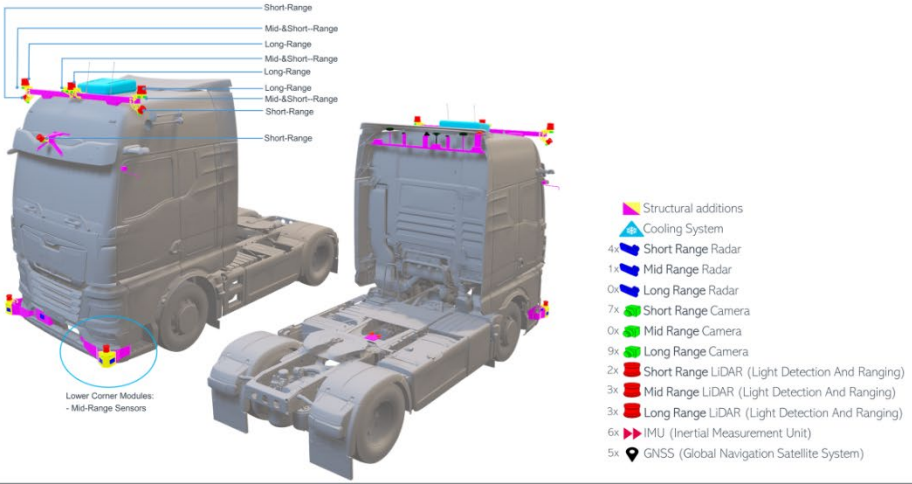
- **Bordnetzfahrzeug** LEONI
  - redundante Bordnetzentwicklung
    - Aufbau der redundanten Leitungsätze und Integration in den Prototypen
    - Elektronische Schutzfunktionen für Kurzschluss, Überstromschutz, Unterspannungsdetektion und thermischer Leitungsschutz

ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Lars Jörn Lippert, MAN Truck & Bus SE 26

### AP6: FAHRZEUGAUFBAU

**Sensorik**

Unsere Automation-Fahrzeuge sind mit nachfolgender Sensorik ausgerüstet (hier am Beispiel des Sensorfahrzeugs):




ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Lars Jörn Lippert, MAN Truck & Bus SE 27

# HARDWARE-ARCHITEKTUR L4
## Übersicht

### MOTIVATION UND ZIELE

Die Hardware Architektur umfasst den Verbund aus Steuergeräten, dem redundanten Bordnetz sowie dem Lenk- und Bremssystem. Sie bildet die Basis um die L4 Automatisierungsfunktion in den Fahrzeugen und am HIL-Prüfstand ausführen zu können.

Rechnerhardware

### ARBEITSSCHWERPUNKTE

- **ECU / Rechner-Topologie:** Entwicklung und Evaluation der hoch performanten und skalierbaren L4 Rechnerarchitektur
- **Fahrzeug- und Schnittstellenaufbau:** Definition der notwendigen Schnittstellen für L4 Architektur und Aufbau der Versuchsfahrzeuge
- **Bordnetz:** Entwicklung eines redundanten Bordnetzes und intelligenten Leistungsverteilers
- **Lenksystem:** Entwicklung eines prototypischen, redundanten Lenksystems
- **Bremssystem:** Entwicklung eines prototypischen, redundanten Bremssystems

Sensorfahrzeug

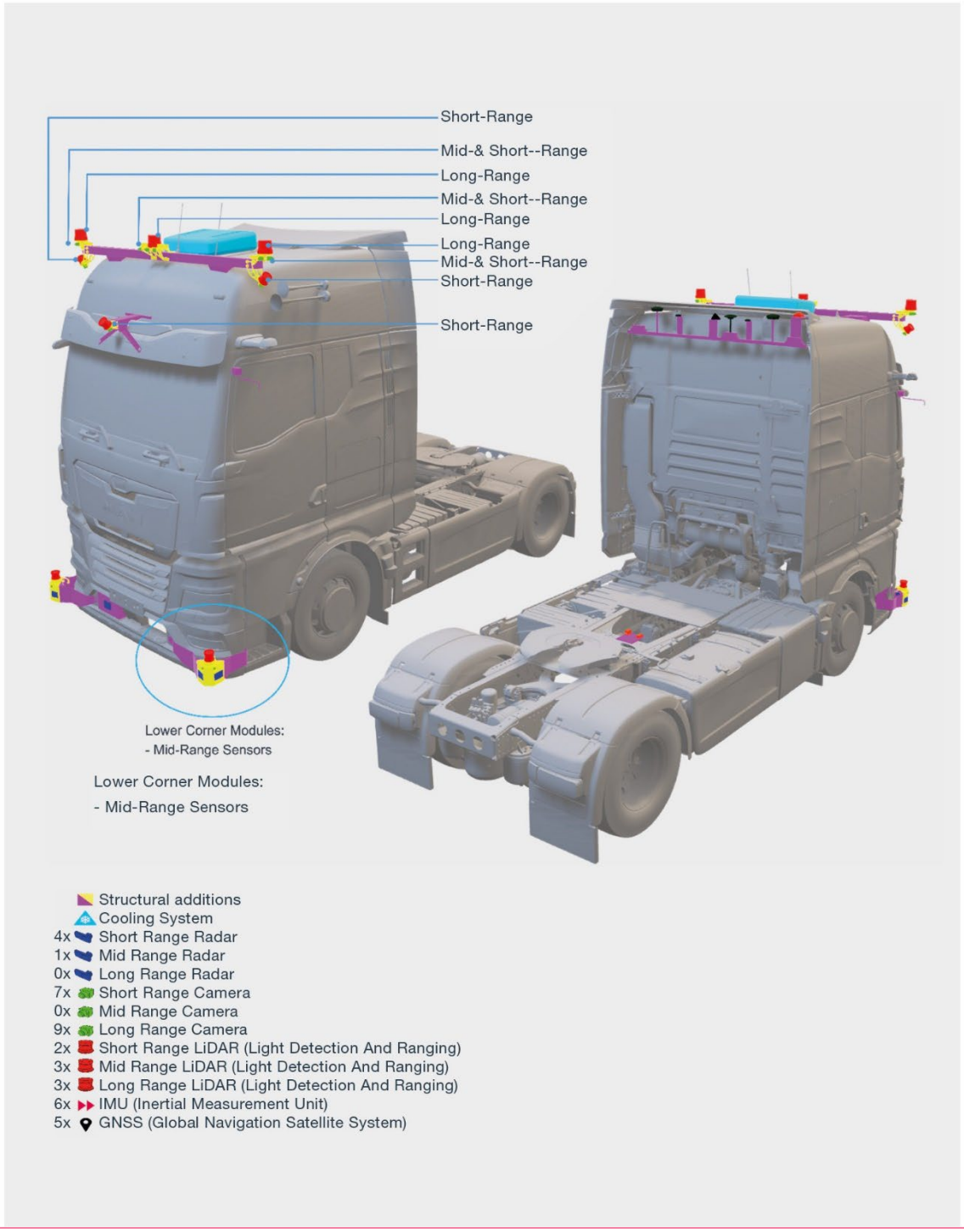
### ERGEBNISSE UND MEILENSTEINE

- Aufbau Sensorfahrzeug für L2 Automatisierung und Funktionsdarstellung auf der Autobahn
- Aufbau und gesetzeskonforme Ausprägung eines Demonstrationsfahrzeugs für L4 Automatisierung

| | BORDNETZ-FAHRZEUG | SENSORFAHRZEUG | DEMONSTRATIONSFAHRZEUG | ARB-FAHRZEUG | TELEOPERATIONS-FAHRZEUG |
|---|---|---|---|---|---|
| Zweck | Bordnetz-Entwicklung | Erprobung Sensorik und Funktionsentwicklung im L2 | Demonstration ADS Konzept | Erprobung der red. Komponenten inkl. Teile der Self-Awareness | Erprobung der Komponenten der ATLAS-Partner |
| Fahrzeug | 4x2 SZM 13K | 4x2 SZM 06K | 4x2 SZM 13K | 4x2 SZM 13K | |
| AD | Bordnetz | ADS Level 2 ohne redundante Komponente Bordnetz, Lenkung,Bremse | ADS Konzept ohne redundante Komponenten Bordnetz, Lenkung, Bremse | redundante Komponenten Bremse und Lenkung | |
| Partnerinhalte | Red. Bordnetz | HW EAS1 & SW EAS2 (Bosch) | Teile des Betriebsmodus-management | Self-Awareness (TUBS), Betriebsmodus-management | Teleoperation Teile des Betriebs-modusmanagement |
| Freigabe | - | §19.6 Shadow-Mode Erprobungsgenemigung AFGBV Ziellevel 4 für autonome Fahrt | Erprobungsgenehmigung AFGBV Ziellevel 4 für autonome Fahrt | Nur Teststrecke | Nur Teststrecke |
| Verknüpfte Meilensteine | 10/24 redundante Plattform im Level-4 Fahrzeug verfügbar 04/25 konforme Ausprägung des Gesamtsystems verfügbar | 04/23 Sensorfahrzeug aufgebaut 08/23 Teststart Level-2 Fahrzeug 07/24 Funktionsdarstellung auf Autobahn L2 01/25 Control Center Technische Aufsicht bedient Use Case | 01/25 Control Center Technische Aufsicht bedient Use Case 04/25 gesetzeskonforme Ausprägung des Gesamtsystems verfügbar | 03/25 redundante Plattform im Level-4 Fahrzeug verfügbar 04/25 gesetzeskonforme Ausprägung des Gesamtsystems verfügbar | 04/25 gesetzes konforme Ausprägung des Gesamtsystems verfügbar |

# FAHRZEUGAUFBAU – SENSORPLATTFORM

## Hardware-Architektur L4



# DAS FEHLERTOLERANTE ENERGIEBORDNETZ

## Hardware-Architektur L4

### MOTIVATION UND ZIELE

Um die stetige Funktion sämtlicher sicherheitsrelevanten Komponenten im Fahrzeug zu gewährleisten, muss sichergestellt werden, dass diese ausreichend mit elektrischer Leistung versorgt sind. In diesem Arbeitspaket wurden die grundlegenden Anforderungen an die elektrische Energieversorgung zusammengetragen und ein System zur hochverfügbaren Bereitstellung von Energie erarbeitet und validiert. Besonderer Fokus wurde auf die Vermeidung von Einfachfehlern gelegt, die zum Funktionsausfall führen können.


Versuchsträger Bordnetz

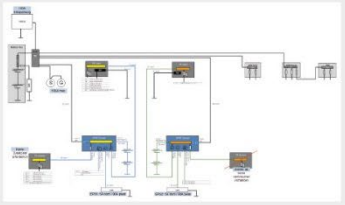
### KOMPONENTEN

**Redundantes Bordnetz**

- Funktionale Sicherheitsanalyse zur Definition von Anforderungen und einer inhärent hochverfügbaren Architektur
- Entwurf des Schaltplans und Definition der Verlegewege im 3D-Modell
- Aufbau der redundanten Leitungsätze und Integration in den Prototypen

**Intelligenter Leistungsverteiler**

- Schutzfunktionen für Kurzschluss, Überstromschutz, Unterspannungs-detektion und thermischer Leitungsschutz
- Elektronische Leistungsschalter zum kommandierten Schalten der Ein- und Ausgänge
- Diagnose mittels Strom- und Spannungsmessung
- Verbrauchervorladung, zyklische Wiedereinschaltstrategie, Überspannungsschutz

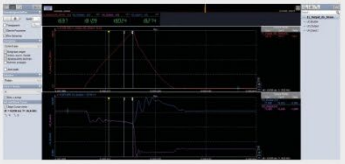


Bordnetzarchitektur

Intelligenter Leistungsverteiler

### ERGEBNISSE

- Bestätigtes Energiebordnetzkonzept für automatisiertes Fahren
- Einhaltung der Rückwirkungsfreiheit zwischen Kanälen & Bordnetz
- Unabhängigkeit zwischen Backup-Systemen kann durch Leistungs-verteiler hergestellt werden
- Erhöhte Verfügbarkeit der Einzelsysteme und ASIL-Verbraucher



Fehlerinjektion mittels Kurzschlüssen

# BREMSSYSTEM

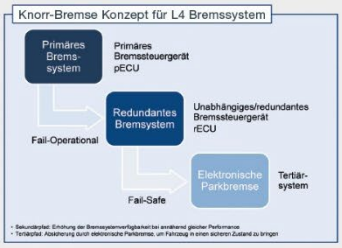
## Hardware-Architektur L4

### MOTIVATION UND ZIELE

Redundante Sicherheitssysteme sind die Voraussetzung für autonome Fahrzeuge, bei denen der menschliche Fahrer als Überwachungsinstanz und Rückfallebene entfällt.
Knorr-Bremse nimmt sich dieser Aufgabe mit dem Ziel an, die für diesen Anwendungsfall notwendigen Sicherheitskonzepte unter gleichzeitiger Einhaltung der fahrdynamischen Anforderungen zu erfüllen.

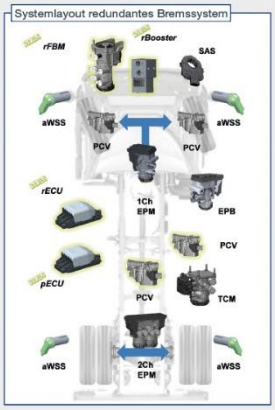
### ARBEITSSCHWERPUNKTE

- Lasten- und Pflichtenheft für primäres und redundantes Bremssystem sowie redundantes Lenksystems (Steer-by-Brake)
- Entwicklung von System- und Softwarearchitektur
- Erstellung und Implementierung des Sicherheitskonzeptes
- Entwicklung und Erprobung der für das redundante Bremssystem notwendigen Komponenten
- Aufbau und Erprobung eines Demonstrationsfahrzeugs bis zur Zielreife




### ERGEBNISSE

- Umsetzung der definierten Zielarchitektur zunächst in einer HiL Umgebung und darauf aufbauend in zwei Versuchsträgern.
- Die dafür notwendigen Komponenten (ECUs, rBooster & rFBM) sind bis zur B-Musterreife entwickelt und für die Verwendung auf öffentlichen Straßen freigegeben.
- Integration der für das redundante Bremssystem und die Lenkredundanz spezifischen Funktionen, u. a.:
  - Health Monitoring
  - Handover auf das red. System, auch während ABS-Einsatz
  - Steer-by-Brake
- Technische Systemfreigabe, welche den in der Vorhabensbeschreibung beschriebenen Inhalt deckt und die Konsortialpartner zu unabhängigen Entwicklungen und Tests auch nach Projektabschluss befähigt.
- Versuche auch im Rahmen von Wintererprobungen in Schweden wurden erfolgreich absolviert.

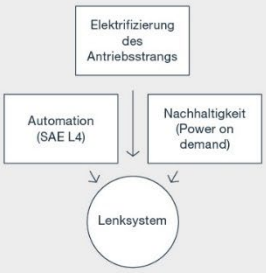


# NEXT GENERATION STEERING SYSTEM

## Hardware-Architektur L4

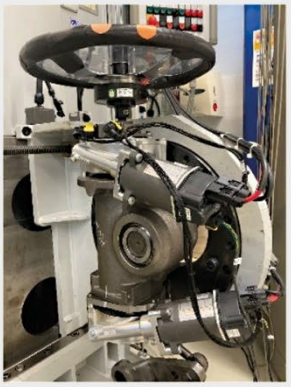
### MOTIVATION UND ZIELE

Im Zwischenbericht wurde aufgezeigt welche Architekturtreiber (Gesellschaft und Technologie) berücksichtigt wurden und wie das Design des zukünftigen Lenksystems aussehen könnte, um in das Package und die Architektur der neuen Fahrzeuggenerationen zu passen. Ziel dieser Phase war es ein mögliches Konzept des Lenksystems zu verifizieren und zu validieren.




### ERPROBUNG DES LENKSYSTEMS

Das bis zur Zwischenpräsentation entwickelte Konzept des Lenksystems wurde in der zweiten Projekthälfte des ögPs erprobt. Diese Erprobung beinhaltete die Verifizierung, also die Konformität mit den Anforderungen, als auch die Validierung, also das Überprüfen des Lenksystems in der Zielumgebung im Fahrzeug bei realen Einsatzbedingungen. Dazu gehören unter anderem das Fahren in verschiedenen Streckenszenarien im öffentlichen Verkehr, sowie unter verschiedenen Rahmenbedingungen. In diesem Kontext wurde eine Wintererprobung durchgeführt, in welcher die Applikation und das Lenkverhalten bei niedrigen Umgebungstemperaturen überprüft wurde.



Funktionsprüfungen am Prüfstand

Wintererprobung (Validierung)

### AUSBLICK

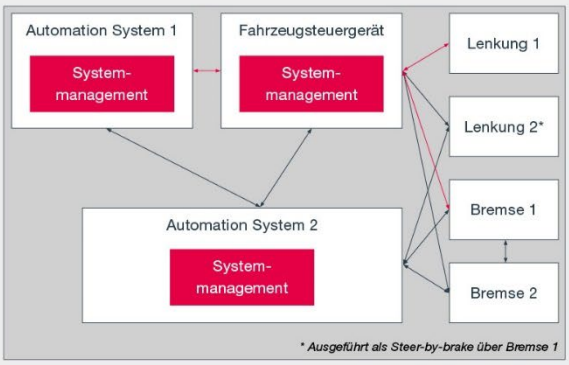
Mittels umfänglicher Prüfstandsversuche ist die generelle Funktion des Lenksystems bereits großteils verifiziert, weitere Versuche sind noch in Durchführung. Die Systemintegration in einen Versuchsträger des Projektpartners MAN ist erfolgt, der Prototyp kann durch eingewiesene Fahrer auf der öffentlichen Straße getestet und Lenkfunktionen weiterentwickelt werden.

# REDUNDANZ & SYSTEM MANAGEMENT

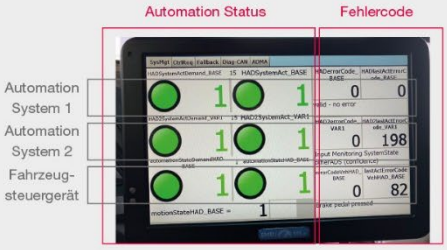
## Ausführung eines Minimum Risk Manövers nach Komponentenverlust

### DEMONSTRATIONSINHALTE

- Simulation des Ausfalls einer oder mehrerer Redundanz-Komponenten während der autonomen Fahrt mithilfe von Trennschaltern
- Selbständige Überführung des Fahrzeugs in einen sicheren Zustand:
  - Einschalten des Warnblinkers
  - Durchführen eines Minimum Risk Manövers: Spurwechsel und Bremsen in den Stillstand
  - Einlegen der Parkbremse
- Darstellung eines verteiltem System Managements zur Überwachung der Fahrzeugsysteme und Bestimmung eines konsistenten Systemzustandes




Fahrzeugarchitektur des Versuchsträgers




Visualisierung der Zustände und Diagnosen des System Managements


Trennschalter für Redundanz-Komponenten

### BESCHREIBUNG DES VERSUCHSTRÄGERS

- TGX 18.510 4x2 LL, 375 kW / 510 PS
- Integration L4-fähiger Aktuatoren
  - Redundante Bremse mit Steer-by-Brake Fähigkeit (Knorr-Bremse)
  - Lenksystem mit neuem autonomem Modus (Bosch)
- Einbau einer Echtzeitkinematik für hochgenaue GPS-Positionierung
- Keine Verwendung von weiterer Sensorik für autonomes Fahren


Autonomous-Ready Base Vehicle (ARB-Fahrzeug)

# AP 7:
# Perception für den UseCase Hub-to-Hub

Dr. Ulrich Voll, MAN Truck & Bus SE

## 3.7 AP 7: Perception für den UseCase Hub-to-Hub

*Arbeitspaketleitung: Dr. Ulrich Voll, MAN Truck & Bus SE*

Im klassischen Architekturschema „Sense-Plan-Act" entspricht die Perzeption, also die Umfeldwahrnehmung, dem „Sense". Sie ist für das automatisierte Fahren Grundvoraussetzung. Hierzu sind im ATLAS-L4-Projekt AP 7 vier wesentliche Beiträge entstanden, auf die unten jeweils detailliert eingegangen wird:

Die ersten beiden beschäftigen sich mit der Kalibration. Ähnlich wie der Mensch ggf. Brillengläser und ein Brillengestell braucht, um mit seinen Augen das Umfeld bestmöglich wahrzunehmen, müssen im Fahrzeug für jeden Sensor die Parameter der Pose (Extrinsik) und innere Parameter wie Linsenparameter (Intrinsik) genau bekannt sein. Dazu gibt es Verfahren, die offline, also einmalig bei der Inbetriebnahme und vor dem Start des Systems, eine Vermessung und damit Bestimmung/Schätzung aller relevanten Parameter vornehmen. Ggf. unter Verwendung von zusätzlichen Hilfsmitteln wie Markern, oder in unserem Fall sogar einer kompletten Kalibrierhalle. Ergänzend, und vielleicht in Zukunft einmal sogar ersatzweise, gibt es Verfahren, die diese Parameterschätzung im laufenden Betrieb, also online (so der mathematisch/algorithmische Terminus) korrigieren oder sogar ganz eigenständig durchführen können.

Durch die Fortschritte im maschinellen Lernen, heute oft als künstliche Intelligenz bezeichnet, entwickeln sich die Verfahren zur Perzeption, also der Sensorfusion, rapide weiter. Unser Beitrag ist hierzu die Industrialisierung, die auf den Use-Case angepasste konkrete Umsetzung neuer Verfahren. Ein wichtiger Fortschritt besteht in der Verwendung von multimodalen Ansätzen, welche die Gesamtheit aller Sensorsignale insgesamt betrachtet und neuronalen Netzwerken zuführt, im Gegensatz zu älteren Verfahren, die lediglich jeden einzelnen Sensorkanal betrachten und nur die Einzelergebnisse mit klassischen Methoden in einer „späten Fusion" zusammenzuführen. Wir haben aktuelle Verfahren angepasst auf die Situation im Truck, und diese mit unserem eigens erstellten, Lkw spezifischen Datensatz „MAN TruckScenes", trainiert.

Mit der Finanzierung durch das ATLAS-L4 Projekt konnten wir als weltweit Erste einen Truckspezifischen Datensatz erstellen und veröffentlichen, mit dem Perzeptionsverfahren trainiert, validiert, verbessert oder gar neu entwickelt werden können. Im Bereich Passenger Cars bilden sich um öffentlich zugängliche Datensätze wie beispielsweise NuScenes eine rege Community und intensive Forschungsaktivitäten, aus denen eine Menge an Verbesserungen und neuen Verfahren hervorgeht. Wir konnten unseren Datensatz MAN TruckScenes zum Training eigener, verbesserter Verfahren nutzen. Aber noch bedeutender ist die Rolle, die er für die Community leistet: er wirkt wie ein Katalysator oder Beschleuniger auf die Fortentwicklung der Perzeption für das automatisierte Fahren, speziell mit Trucks.

Wir haben international positives Feedback für den Datensatz erhalten, insbesondere auch als wir den Datensatz MAN TruckScenes auf der renommierten ML/AI Konferenz NeurIPs 2024 vorstellen durften. Der Datensatz sei ein großer Gewinn für Unternehmen und Community. Besondere Wertschätzung wurde geäußert für den europäischen/deutschen Beitrag; abgesehen davon, dass er der erste überhaupt im Bereich Truck ist, trägt er auch zu einer begrüßenswerten Diversifizierung von öffentlich verfügbaren Datensätzen bei.

### 3.7.1 Offline-Kalibrierung:

Kern der Arbeiten zur Offline-Kalibrierung innerhalb der Projektlaufzeit war der Aufbau und die Inbetriebnahme einer Kalibrierhalle, welche in Kombination mit einer umfangreichen Software Suite (die ebenfalls im Rahmen dieses Projekts stark erweitert worden war) und eines Photogrammetrie Verfahrens eine hochgenaue Kalibrierung ermöglicht.

Unter einer „Kalibrierung“ verstehen wir dabei die Bestimmung von rund 350 Parametern, welche die Extrinsiken und Intrinsiken folgender Sensortypen umfasst: Kameras, Lidare, Radare, Intertialsysteme, GNS Systeme und Antennen.

Zu Beginn sind die Anforderungen an eine solche Lösung erarbeitet worden. Angenommen wurde dabei die ODD Highway mit einem dementsprechend designten Sensorsetups. Dieses hat maßgeblichen Einfluss auf die Gestaltung der Kalibrierhalle – diese Einflüsse sind simulativ erfasst worden. Aus diesem Prozess ließ sich ein Zieldesign der Halle bestimmen, welches anschließend real umgesetzt worden ist. Die abschließenden Tests bestätigten die Wirksamkeit der getroffenen Baumaßnahmen.

Die eigentliche und im Rahmen dieses Projekts erarbeitete Offline-Kalibrierung besteht dabei aus zwei Teilen: einem Photogrammetrie Schritt als „initial guess“ und einem datengetriebenen Optimierungsschritt auf Basis von Sensordaten aus der Kalibrierhalle.

Das Ergebnis der initialen Photogrammetrie sieht für einen Trailer wie in Abbildung 46 dargestellt aus:


Abbildung 46 Photogrammetrie Messung:
links der Trailer mit optischen Markern; rechts die resultierende Punktwolke

Dadurch lassen sich sämtliche relevanten Geometrien (Fahrzeugkontur, Achsen, Sattelkupplung etc.) sowie die Extrinsik der Sensorgehäuse erfassen.

Anschließend sind die mit Umfeldsensoren ausgestatteten Projektfahrzeuge durch die Kalibrierhalle gefahren, wobei sie dabei die Sensordaten kontinuierlich aufgezeichnet haben. Diese Aufnahmen sind danach mit den Ergebnissen der Photogrammetrie in der Software Suite verarbeitet worden.

Mit diesem zweiteiligen Verfahren ist die Aufgabe der Offline-Kalibrierung im Rahmen dieses Projekts hinreichend erfüllt worden. Die Kalibrierung wird von den nachfolgenden Modulen der Perzeption und Lokalisierung genutzt, um die Sensordaten sinnig verarbeiten zu können.

### 3.7.2 Online-Kalibrierung

Die multimodale Online-Sensor-Kalibrierung bezieht sich auf die kontinuierliche Schätzung der Ausrichtung (Extrinisk) zwischen verschiedenen Sensoren – wie Kameras, LiDARe, RADARe und IMUs – während des Systembetriebs, im mathematisch/algorithmischen Sinn „Online". Ebenso können auch andere innere Parameter wie Linsenparameter von Kameras geschätzt werden (Intrinsik). Die Herausforderung besteht darin, Daten unterschiedlicher Modalitäten (z. B. 2D-Bilder vs. 3D-Punktwolken) zu kombinieren, die sich in Struktur, Auflösung und Rauschen unterscheiden, und daraus die Kalibrierung, oder Korrekturen der Grundkalibrierung zu extrahieren, bzw. im statistischen Sinn zu schätzen. Diese Aufgabe ist noch ein aktives Forschungsfeld, Lösungen könnten womöglich in der Zukunft die Notwendigkeit einer Offline-Kalibrierung obsolet machen, aber das ist zurzeit noch nicht möglich.

In unserer Arbeit haben wir einen Deep-Learning-Ansatz gewählt und zwei Modelle trainiert: eines für die **Kamera-zu-LiDAR-Kalibrierung** und eines für die **LiDAR-zu-LiDAR-Kalibrierung**, um eine robuste und echtzeitfähige Kalibrierung zu ermöglichen.

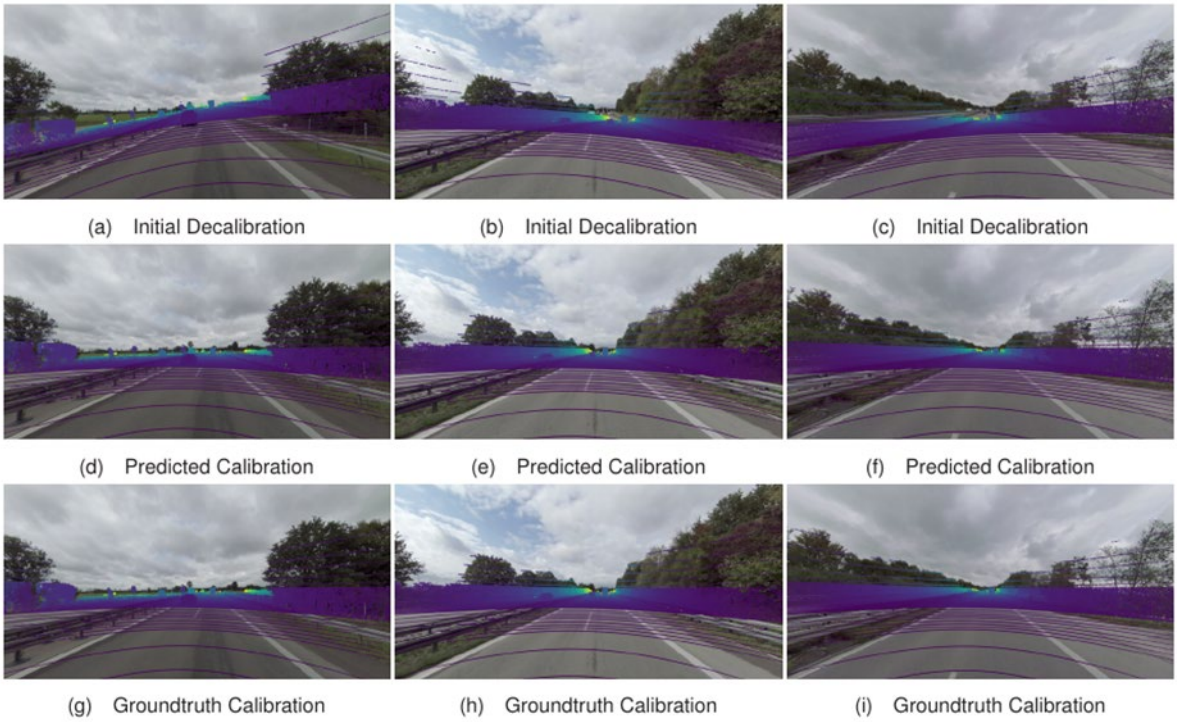



Abbildung 47 Drei Beispiele (vertikal) einer Dekalibrierung der Kamera zu Lidardaten in Autobahnszenarien: (a), (b) und (c) zeigen die künstlich aufgeprägte Dekalibrierung; (d), (e) und (f) die durch das neuronale geschätzte Online-Kalibrierung und (g), (h) und (i) die Ground Truth der Kalibrierung als Vergleich

**CalibViT** zur Kamera-Lidar-Kalibrierung verwendet eine Dual-Branch-Swin-Transformer-Architektur, bei der ein Zweig RGB-Bilder, und der andere Tiefenbilder verarbeitet, um hierarchische Merkmale aus beiden Modalitäten zu extrahieren.

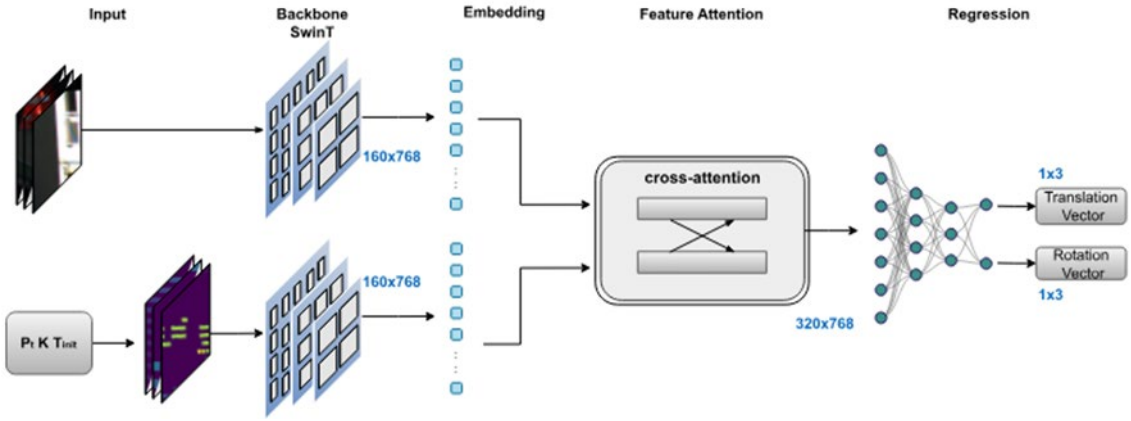



Abbildung 48 Schematische Darstellung der CalibViT Netzarchitektur zur Lidar-Kamera-Kalibrierung

CalibViT erzielt herausragende Ergebnisse bei gleichmäßig verteilten Dekalibrierungen von ±10° Rotation und ±0,25 m Translation. Das Modell erreicht einen niedrigen mittleren Rotationsfehler (MRE) von 0,1389° (X: 0,0578°, Y: 0,2698°, Z: 0,0890°) und einen mittleren Translationsfehler (MTE) von 1,863 cm (X: 2,247 cm, Y: 1,019 cm, Z: 2,323 cm). Diese Ergebnisse zeigen die starke Fähigkeit von CalibViT, RGB- und LiDAR-Daten selbst bei erheblichen Kalibrierungsabweichungen präzise zu alignieren.

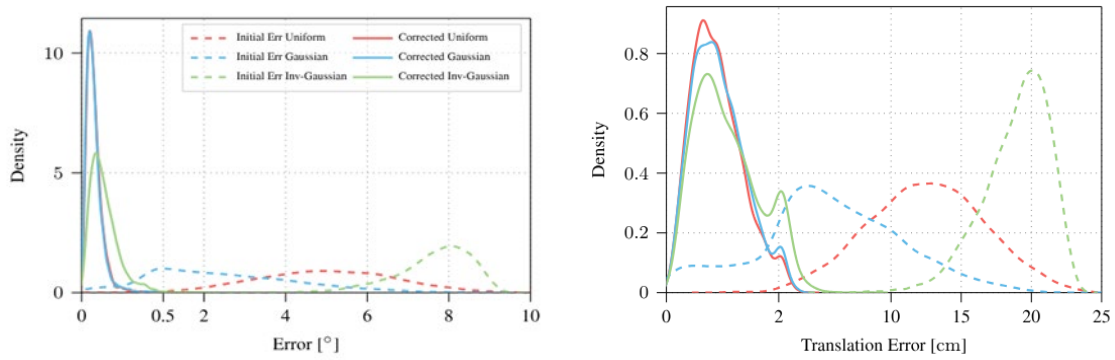



Abbildung 49 Dichteverteilung der Rotationsfehler (links) und Translationsfehler (rechts) über die untersuchten Bandbreiten

Unsere Modellarchitektur zur Lidar-Lidar-Kalibrierung (siehe Abbildung 50) folgt einem grob-zu-fein Ansatz zur Registrierung von Punktwolken und verwendet einen angepassten Point-Transformer v3 (PTv3)-Encoder zur hierarchischen Merkmalsextraktion aus den Eingangspunkten.

Zusätzlich integrieren wir ein Mutual Information (MI)-Modul, das als Trainingsverlust dient und die Konsistenz der Merkmale zwischen Quelle und Ziel maximiert.

Die finale Transformation wird mit dem gewichteten Kabsch-Algorithmus berechnet, was auch bei verrauschten Matches eine robuste Registrierung ermöglicht.

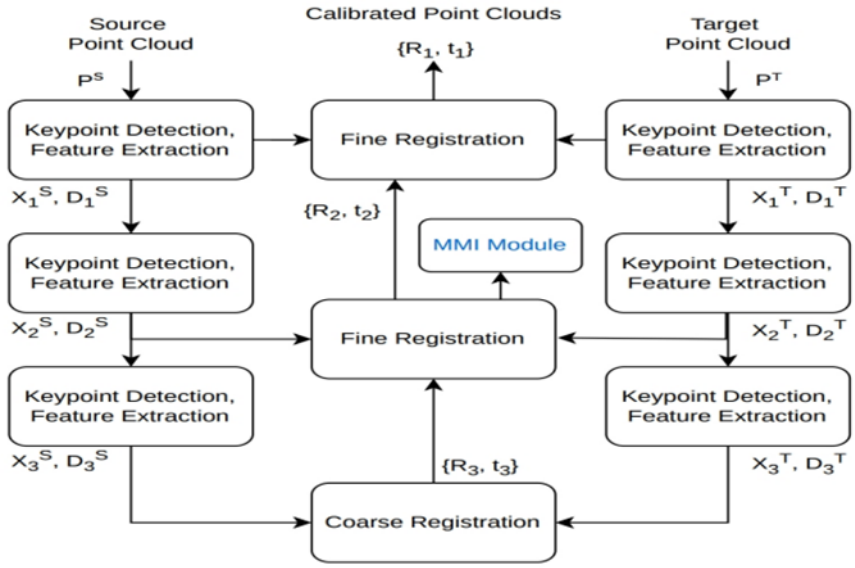



Abbildung 50 Schematische Darstellung unserer Netzarchitektur zur Lidar-Lidar-Kalibrierung

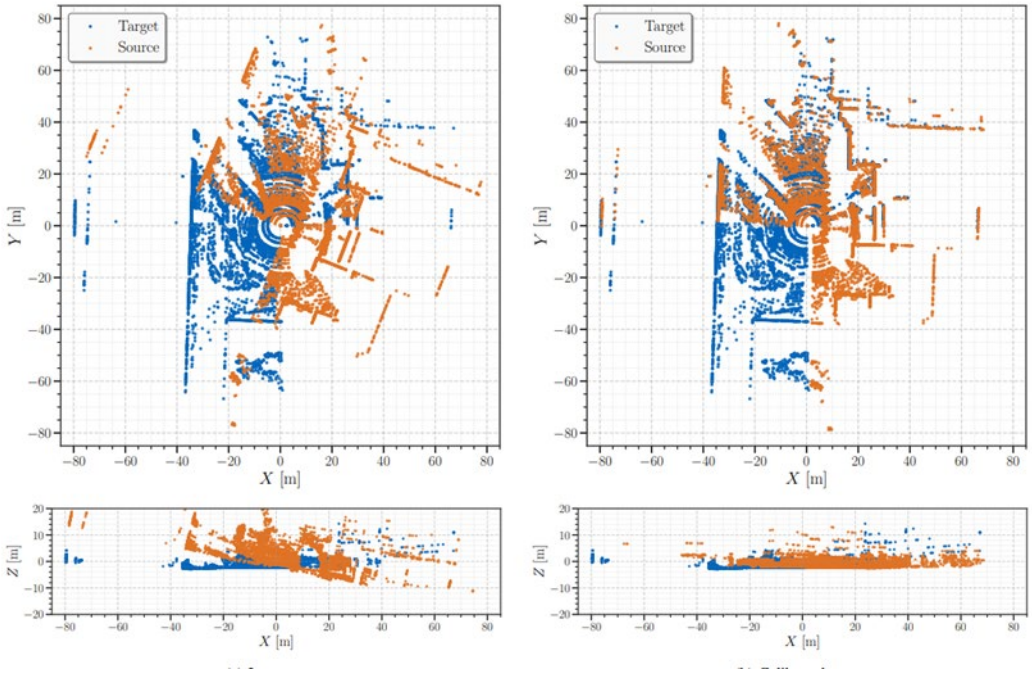



Abbildung 51 Beispiel einer Lidar-Lidar-Dekalibrierung zweier Sensoren (in orange und blau). Links ist ein signifikanter Gier- und Rollwinkel aufgeprägt; rechts ist das Ergebnis der Online-Kalibrierung

Das Modell wird mit Hilfe von Augmentierung durch synthetische Dekalibrierungen von bis zu ±20° Rotation und ±0,50 m Translation trainiert, und erreicht auf dem TruckScenes-Datensatz einen mittleren Rotationsfehler von nur ±0,3° sowie einen Translationsfehler von ±0,09 m – und übertrifft damit herkömmliche Kalibrierungsmethoden deutlich. Der Ansatz ist für den Online-Einsatz konzipiert und eignet sich nicht nur hervorragend für autonome Fahrsysteme, sondern lässt sich auch auf eine Vielzahl robotischer Plattformen übertragen, die eine robuste und echtzeitfähige multimodale Sensorkalibrierung erfordern.

### 3.7.3 Public Dataset

Im Rahmen des Projekts wurde mit „MAN TruckScenes“ der weltweit erste öffentliche Datensatz für Autonomous Trucking erstellt. Die Erstellung des Datensatzes kann in mehrere Arbeitspakete untergliedert werden

- Zielsetzung und Architektur des Datensatzes
- Durchführung der Datenkampagne
- Verarbeitung der Daten und Erstellung des Datensatzes
- Veröffentlichung des Datensatzes

**Planung und Design des Datensatzes**

In der ersten Planung wurden die Charakteristika und Zielsetzungen des Datensatzes geklärt. Folgende grundsätzliche Entscheidungen sind festzuhalten

- Multimodaler Datensatz: Kamera, Lidar und Radardaten sollten neben Fahrzeugeigenbewegungsdaten und Positionsinformationen verwendet werden.
- Szenen: der Datensatz sollte in Szenen untergliedert werden. Eine Szene ist dabei ein 20 s Mitschnitt aller Daten. Damit können die Sensordaten in einem temporalen Zusammenhang genutzt werden, z.B. für Trackingverfahren oder Temporal Fusion. Eine Größenordnung von ca. 700 Szenen wurde angestrebt.
- Annotationen: Für den zu erstellenden Datensatz wurde festgelegt, dass er Annotationen in Form von sog. 3D Bounding-Boxen enthalten sollte. Diese sollten in der Lidar-Domäne mit 2Hz annotiert werden. Es wurde außerdem spezifiziert welche Objekte annotiert werden sollen. Es wurden insgesamt 27 Objektklassen verwendet, von Kfz über Fahrräder bis hin zu Fußgängern und Verkehrsschildern.
- Diverse Umweltbedingungen: Bei der Auswahl von Szenen für das Training sollte auf vielfältige Wetterbedingungen, bauliche Begebenheiten und die Lichtbedingungen geachtet werden.
- Fokus auf Hub-to-Hub Szenarien: Der Datensatz sollte typische Situationen aus dem Hub-to-Hub Verkehr abbilden. Damit lag ein klarer Fokus auf Autobahnsituationen, gefolgt von Fahrten auf Zubringerstraßen und Terminalsituationen.
- Veröffentlichung als frei zugänglicher Datensatz: Ein offen einsehbarer Datensatz generiert großen Mehrwert für die Forschung. Allerdings wurden dadurch auch besonders hohe Ansprüche an Anonymisierung- und Datenschutz gesetzt.
- Datenformat: Das Datenformat definiert wie die Daten in Dateien organisiert sind und zueinander in Verbindung stehen. Da der Datensatz eine weite Verbreitung finden soll, wurde sich für das in der Data-Science Community sehr populäre „nuScenes“-Format entschieden (https://www.nuscenes.org/nuscenes). Damit wurde nicht nur auf ein bewährtes Datenformat gesetzt, sondern auch die Einstiegshürde für die offene Forschung minimiert.

### Durchführung der Datenkampagne

Die Datenkampagne wurde mit dem in Abbildung 52 dargestellten Versuchsträger durchgeführt.

Table 2: Sensor specifications of the MAN TruckScenes setup.

| Sensor | Details |
|---|---|
| Camera | 4× Sekonix SF3324, RGB, 10 Hz, 1928 × 1208, 120° × 73° FoV |
| Lidar | 2× Hesai Pandar64, 10 Hz, 64 layer, 360° × 40° FoV, 200 m@10 % |
| | 4× Ouster OS0, 10 Hz, 64 layer, 360° × 90° FoV, 35 m@10 % |
| Radar | 6× Continental ARS 548 RDI, 20 Hz, 76 GHz, 100° × 28° |
| GNSS | 1× GeneSys ADMA-G-PRO+, 100 Hz, 0.01 m pos., 0.015° heading |
| IMU | 2× Xsens MTi-680G-SK, 100 Hz, 9 DoF |

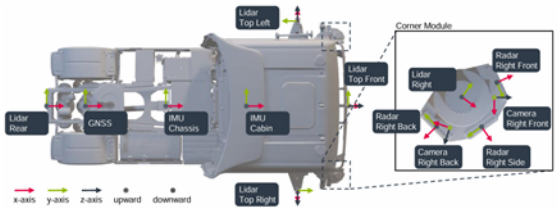



Abbildung 52 Mit diesem Fahrzeug wurden die Daten für den MAN TruckScenes Datensatz eingefahren.

Das Fahrzeug verfügt über ein erprobtes und kalibriertes multimodales Sensorsetup mit sechs Lidaren, vier Kameras, sechs Radare (4D-Radare), zwei IMUs und einer GNSS-Einheit.

Um die gewünschte Vielseitigkeit der Szenen in der ODD zu erreichen, wurden die Messfahrten bezüglich Routenführung und weiteren Randbedingungen gezielt geplant. So spielten Tageszeit, aber auch Saison und Wetterbedingungen eine wichtige Rolle. Den Erfolg dieses Verfahrens zeigt die Auswertung der Szenen-Tags von TruckScenes. Abbildung 53 zeigt die Verteilung der Szenen-Tags für alle 747 Szenen im Datensatz.

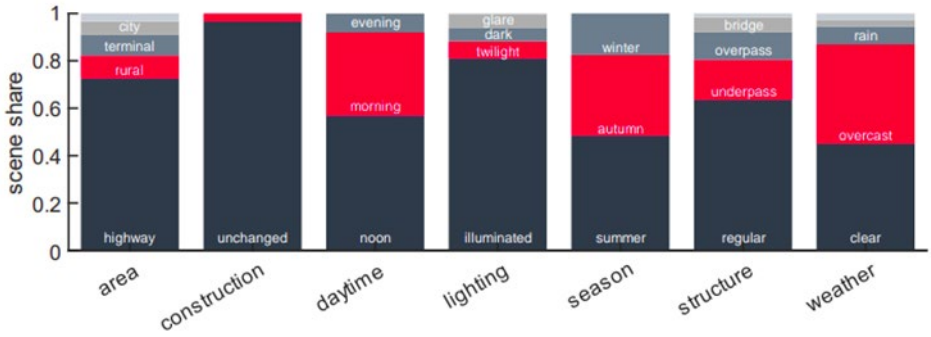



Abbildung 53 Verteilung der Szenen-Tags für alle 757 Szenen im MAN TruckScenes Datensatz.

Die im MAN TruckScenes enthaltenen Szenen wurden auf einer Fläche von ca. 100 $km^2$ gesammelt. Dies kann durch eine Kartierung der Egoposen der 747 Szenen gezeigt werden. Der Schwerpunkt der Aufzeichnungen lag im Raum um München.

### Verarbeitung der Daten und Erstellung des Datensatzes

Die Daten aus den Messkampagnen mussten für die Erstellung des finalen Datensatzes weitergehend verarbeitet werden. Der Ablauf ist in Abbildung 54 schematisch dargestellt.

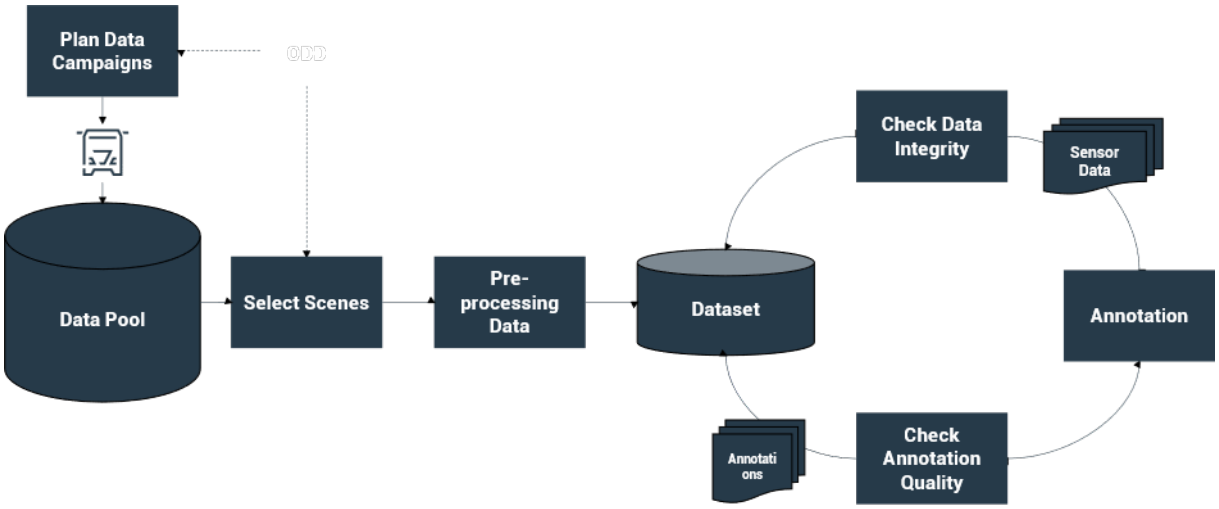



Abbildung 54 Schritte zur Verarbeitung der eingefahrenen Daten zum finalen Datensatz.

Im vorherigen Kapitel wurde bereits beschrieben, wie die Anforderungen an vielseitige Umweltbedingungen und die Fokussierung auf Hub-to-Hub eine ODD aufspannen, die für die Steuerung der Messkampagnen und der Auswahl der Szenen zu berücksichtigen war.

Vor der Weitergabe der anonymisierten Daten an den Annotations-Zulieferer wurden für die Messdaten außerdem umfangreiche Integritätschecks durchgeführt. Diese sollten zum Beispiel die Vollständigkeit der Sensordaten sicherstellen, sowie auch fehlerhafte Daten identifizieren.

Auch die Annotationen wurden Qualitätschecks unterzogen, bevor sie in den finalen Datensatz aufgenommen wurden. Mittels dem entwickelten Tooling, war auch eine visuelle Überprüfung der Sensordaten möglich.

### Veröffentlichung des Datensatzes

Im Dezember 2024 wurde MAN TruckScenes veröffentlicht und zum Download bereitgestellt. Vor diesem Schritt wurden zahlreiche Maßnahmen getroffen, um sowohl das Interesse für den Datensatz zu wecken als auch das Arbeiten mit dem Datensatz zu vereinfachen.


Abbildung 55 Download-Optionen des MAN TruckScenes Datensatzes.

Die Maßnahmen im Detail:

- Downloadbarkeit: MAN TruckScenes kann weltweit heruntergeladen werden. Dafür wurde sich erfolgreich für das „AWS Open Data Sponsorship Program“ beworben, das „die Kosten für die Speicherung von öffentlich verfügbaren hochwertigen Cloud-optimierten Datensätzen“ abdeckt (vgl. Open-Data-Sponsorship-Programm | AWS).
- Es wurde eine umfangreiche Website (www.man.eu/truckscenes) erstellt. Dort finden sich neben Hintergrundinformationen die Links für den Download und Tutorials zur Nutzung des Datensatzes.
- Um den Datensatz komfortabel nutzen zu können, wurde ein sog. „Dev-Kit“ nach der Vorlage von nuScenes entwickelt. Dieses können sich Entwickler komfortabel als pip-Paket installieren.
- Für die Unterstützung wissenschaftlicher Arbeiten wurde der Datensatz unter anderem auf Fachkonferenzen wie der NeurIPS 2024 und der IEEE IV 2025 vorgestellt. Besonders detaillierte Informationen und Auswertungen können auch über das verfasste Paper „MAN-TruckScenes: A multimodal dataset for autonomous trucking in diverse conditions“ (arxiv: 2407.07462) eingesehen werden.
- Um neu entwickelte Ansätze besser vergleichen zu können, wurde auf Huggingface eine 3D-Object-Detection Competition initiiert. Damit können Ansätze automatisiert gegen eine nicht veröffentlichte Ground-Truth evaluiert und gerankt werden.

### 3.7.4 Multimodale Objektdetektion

Im Rahmen dieses Projekts wurde ein KI-gestütztes Verfahren zur dreidimensionalen Objektdetektion entwickelt, das auf multimodalen Sensordaten basiert – darunter Lidar, Kamera und Radar. Diese Sensordaten dienen als Grundlage für das Training eines neuronalen Netzwerks. Zu Beginn erfolgte eine umfassende Analyse des aktuellen Forschungsstands durch eine strukturierte Literaturrecherche. Dabei wurden verschiedene Ansätze hinsichtlich Effizienz, Genauigkeit und Eignung für die projektspezifischen Anforderungen bewertet. Auf Basis dieser Bewertung wurde ein Verfahren ausgewählt, das eine Fusion von Lidar- und Kameradaten nutzt und anschließend implementiert.

#### Implementierung einer modularen Entwicklungsplattform

Zur Bewertung und Erprobung der ausgewählten KI-Verfahren wurde eine modulare Entwicklungsplattform konzipiert und umgesetzt. Diese Plattform ermöglicht eine schnelle, flexible Anpassung der Testumgebung und erlaubt die Durchführung realistischer Testszenarien. Dank ihrer modularen Architektur können neue Verfahren unkompliziert integriert und umfangreiche Evaluierungen effizient durchgeführt werden. Die Plattform bildet somit eine zentrale Grundlage für die iterative Weiterentwicklung und Validierung der Detektionsalgorithmen.

#### Transfer und Anpassung der Verfahren auf Lkw-spezifische Daten

Ein zentraler Schwerpunkt in diesem Arbeitspaket lag auf der Übertragung und Anpassung der entwickelten Verfahren auf Lkw-relevante Einsatzszenarien. Hierfür kam der im Projekt veröffentlichte Datensatz „MAN Truckscenes“ zum Einsatz (siehe Abschnitt 3.7.3 Public Dataset). Die Algorithmen wurden gezielt modifiziert, um mit den spezifischen Anforderungen und Charakteristika des Lkw-Verkehrs – wie Fahrzeugdimensionen, typische Umgebungen und Bewegungsmuster – effektiv umgehen zu können.

Durch die Optimierung von Modellparametern und die Feinjustierung der Sensordatenverarbeitung konnte eine hohe Genauigkeit und Zuverlässigkeit in der Objektdetektion erreicht werden.

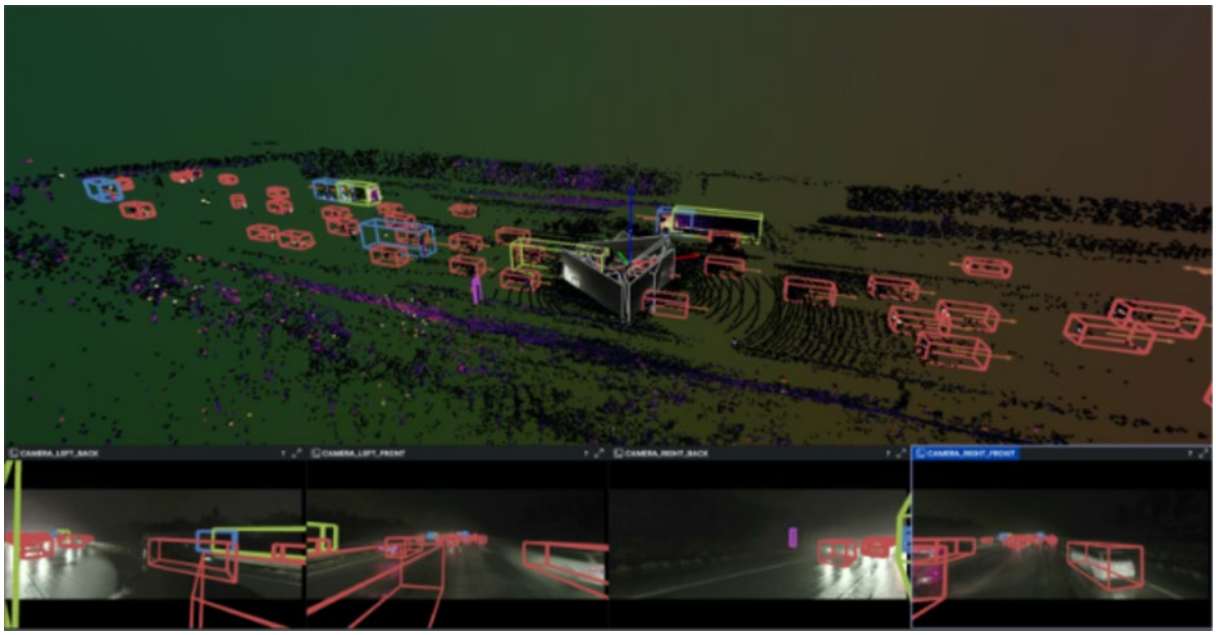


Abbildung 56 Ergebnisse der Objektdetektion für eine Autobahnszene;
oben: 3D Ansicht der Lidardaten und der erkannten Objekte als Boxen; unten: Kameradaten mit den erkannten Objekten als Boxen

**Anpassung an große Distanzen**

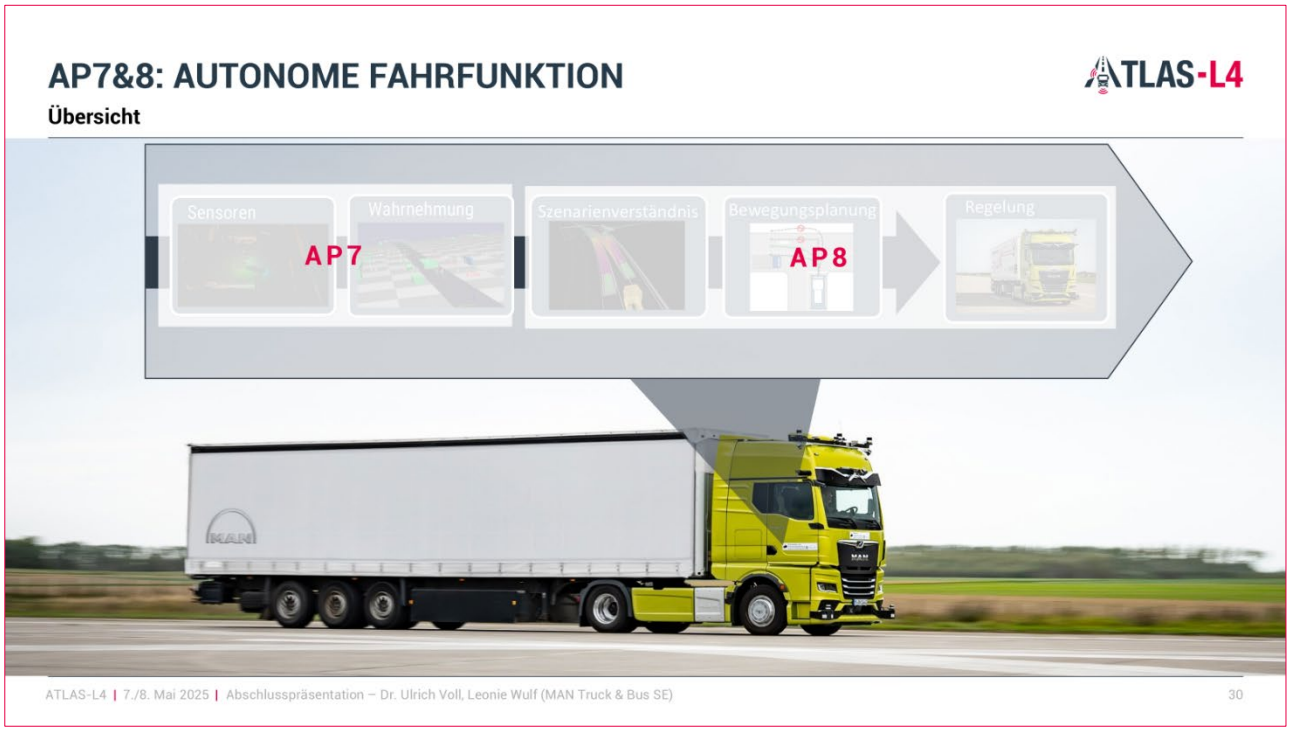
Im Unterschied zum Stand der Forschung ist eine zuverlässige Objektdetektion auch auf großen Entfernungen in Lkw relevanten Einsatzszenarien sehr wichtig. Grund hierfür ist, dass ein Großteil der Forschung auf Pkw Datensätzen, meist aufgenommen im innerstädtischen Bereich, beruht. Diese Datensätze beinhalten Objekte, die üblicherweise eine Entfernung von maximal ±50 m zum Aufnahmefahrzeug aufweisen. Aufgrund der Einsatzszenarien des Fahrens im Autobahnbereichs in Verbindung mit Lkw-spezifischen Charakteristika wie reduziertes Beschleunigungs- und Verzögerungsvermögens durch höhere Masse und Sicherheitsüberlegungen müssen jedoch im Projektszenario Entfernungen von ± 150 m, also insgesamt 300 m gewährleistet werden. Dies erforderte eine Anpassung der Algorithmen, um die Genauigkeit und Leistungsfähigkeit über diese Distanzen hinweg sicherzustellen. Es konnte gezeigt werden, dass auch über große Distanzen mit den ausgewählten Verfahren Objekte zuverlässig erkannt werden. In Abbildung 56 ist ein Beispiel für eine Erkennung von Objekten mit größerem Abstand in einer Autobahnfahrt zu sehen.

**Anpassung für unterrepräsentierte Objektkategorien**

Für die detaillierte Auswertung der Verfahren wurden geeignete Metriken ausgewählt. Diese Metriken ermöglichen eine umfassende Analyse der Leistung und Genauigkeit der Verfahren. Zu den ausgewählten Metriken gehören unter anderem mean average precision (mAP), Translationsfehler und andere relevante Kennzahlen, die eine detaillierte Bewertung und Vergleich der Verfahren ermöglichen.

Im Rahmen der Auswertung mit Hilfe der ausgewählten Metriken wurde festgestellt, dass die Erkennungsleistung für bestimmte Objektkategorien unzureichend war. Die Ursache lag in einer unausgewogenen Verteilung der Trainingsdaten: Während etwa 46 % der Objekte im Datensatz Pkws waren, machten seltene Kategorien wie „Fahrrad“ lediglich 0,16 % aus. Um dennoch eine zuverlässige Detektion auch dieser unterrepräsentierten Klassen zu gewährleisten, wurden gezielte Anpassungen am Modell und am Trainingsprozess vorgenommen. Durch diese Maßnahmen konnte die Erkennungsgenauigkeit deutlich verbessert werden, sodass auch seltene Objekte präzise und robust erkannt werden und eine generelle hohe, dem Stand der Wissenschaft entsprechende Detektionsgüte gewährleistet werden.

### 3.7.5 AP 7 – Vortrag und Poster der Abschlusspräsentation

## AP7: UMFELDWAHRNEHMUNG

**Öffentlicher Datensatz MAN TruckScenes**

**Brückenschlag zwischen Forschungscommunity und Industrie.**

- Öffentliche Datensätze (wie NuScenes, für PKW) werden von vielen Forschergruppen genutzt.
- Erstellung und Veröffentlichung des weltweit ersten Datensatzes für automatisiertes Fahren mit dem LKW„MAN TruckScenes“.
- Er steht der Entwickler-Community, speziell Universitäten und wissenschaftlichen Einrichtungen, frei zur Verfügung.

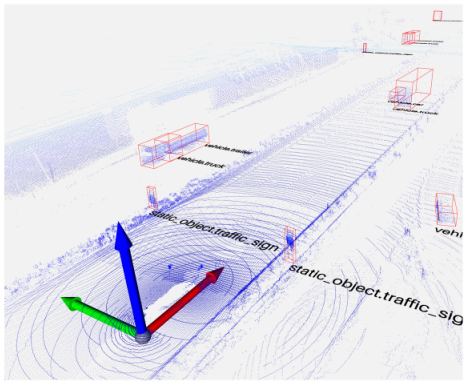
Ergebnisse/Highlights:

Veröffentlicht auf der Konferenz NeurIPS 2024

http://arxiv.org/2407.07462

https://www.man.eu/truckscenes

(-> Fachvortrag Fabian Kuttenreich heute)






## AP7: UMFELDWAHRNEHMUNG

**Algorithmische Fortschritte Sensorfusion**

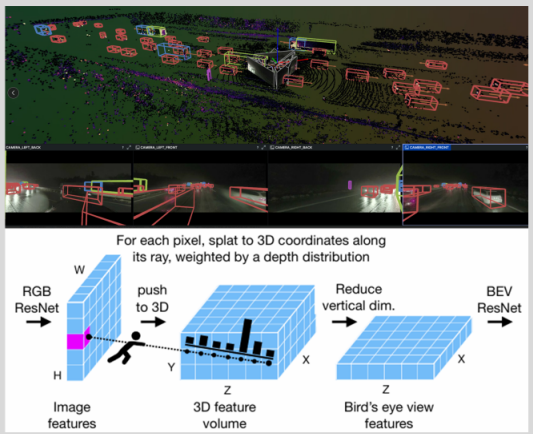
**Die Sensorfusion kombiniert Messdaten in ein Umfeldmodell**

Bisherige Methoden: Neuronale Netzwerke auf isolierten Einzelbildern, pro Kamera, danach klassische Fusion.

Umsetzung aktueller Methoden im industriellen Kontext.

Ergebnisse/Highlights:

- umfassenderer Einsatz von maschinellem Lernen
- multimodal (Kamera, Lidar, … zusammen)
- multitemporal (über die Zeit hinweg)
- Verwendung des Datensatzes MAN TruckScenes



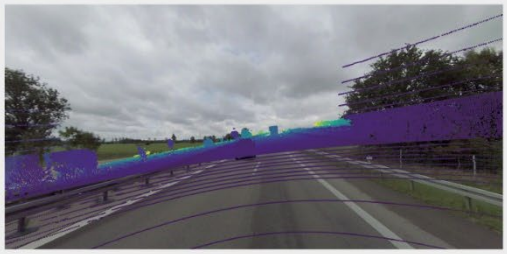

[from: “Simple-BEV: What Really Matters for Multi-Sensor BEV Perception?” arxiv.org/2206.07959]

# MULTI-MODALE ONLINE SENSOR-KALIBRIERUNG

## Perzeption für den Use Case Hub-To-Hub

### MOTIVATION UND ZIELE

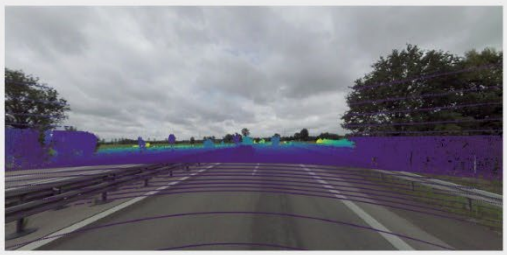
- Wie können wir Fehler durch Vibrationen und Wetterveränderungen kompensieren?
- Wie können wir alle Sensoren ohne manuelle Eingriffe kalibrieren und den Aufwand minimieren?
- Wie können wir die Ausfallzeit durch langwierige Offline-Kalibrierungsprozesse verringern?
- Wie können wir die Sicherheit und Zuverlässigkeit der Wahrnehmungspipeline verbessern?



Dekalibrierte Pointcloud, auf RGB-Bild projiziert

### ARBEITSSCHWERPUNKTE

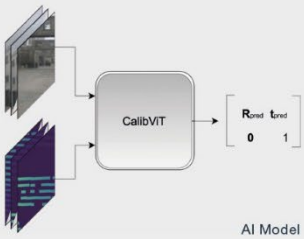
- **Data-driven approach:** Maschinelles Lernen nutzt Echtzeitdaten, um Beziehungen zwischen Modalitäten wie Kamera und LiDAR zu erlernen.
- **Deep Learning Architekturen:** Deep Learning Modelle erfassen komplexe Abhängigkeiten für eine präzise Ausrichtung über mehrere Modalitäten hinweg.
- **Online-Anpassung und Feedback:** Kontinuierliche Aktualisierungen und Anpassungen optimieren die Sensor-Kalibrierung zur Verbesserung der Wahrnehmung.



Kalibrierte Pointcloud, auf RGB-Bild projiziert


### ERGEBNISSE

- Kostenreduktion & Effizienz: Online Calibration minimiert Ausfallzeiten und senkt Betriebskosten für autonomes Fahren. Außerdem entfällt die Notwendigkeit für teure Kalibrierungshallen.
- Online Kalibrierung stellt eine präzise Wahrnehmung und Reaktionsfähigkeit auf die Umgebung des Fahrzeugs sicher, sie erhöht Verfügbarkeit und Sicherheit.




AI Model

# MULTIMODALE FUSIONSALGORITHMEN

## Perzeption für den Use Case Hub-To-Hub

### MOTIVATION UND ZIELE

- Entwicklung eines KI-basierten Verfahrens zur 3D-Objektdetektion
- Nutzung multimodaler Sensordaten (Lidar, Kamera, Radar)

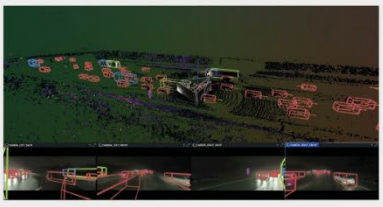
### ARBEITSSCHWERPUNKTE

- Implementierung eines Verfahrens zur Fusion von Lidar- und Kameradaten
- Entwicklung einer modularen Plattform zur Evaluierung und Testen
- Anpassung der Verfahren auf LKW-relevante Daten (Datensatz „MAN Truckscenes“)
- Anpassung für große Distanzen (bis zu 300 Meter)
- Anpassung für seltene Objektkategorien

Beispiel für simulierte Nebeleffekte

### ERGEBNISSE/HIGHLIGHTS

- Hohe Genauigkeit und Zuverlässigkeit der Verfahren
- Erfolgreiche Objektdetektion über große Distanzen
- Zuverlässige Erkennung seltener Objektkategorien durch Modellanpassung
- Auswahl geeigneter Metriken zur Abschätzung der Güte
- Sensitivitätsanalyse zur Bewertung der Robustheit gegenüber Störungen (z. B. Wetterbedingungen, Sensorausfälle, Fehlkalibration)



Beispiel für Ergebnisse der Objektdetektion für Autobahnszene

# MAN TRUCKSCENES
# Weltweit erster öffentlicher Datensatz für das Automatisierte Trucking
## Perzeption für den Use Case Hub-To-Hub

### MOTIVATION UND ZIELE

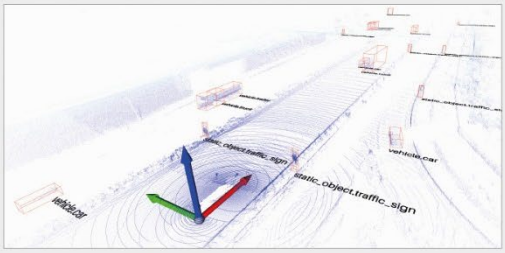
MAN veröffentlicht mit „MAN TruckScenes“ den weltweit ersten öffentlichen Datensatz für Autonomous Trucking.

- beinhaltet Daten für die Entwicklung und Validierung von Ansätzen für automatisierte LKW
- stärkt die datengetriebene Entwicklung und erhöht die Entwicklungsgeschwindigkeit und Sicherheit von KI Ansätzen
- ermöglicht die Einbindung der internationalen Entwicklergmeinschaft in die Erforschung von Lösungen für autonome LKW

Der Datensatz besteht aus 747 Szenen in denen u. a. Kamera, Lidar und Radardaten enthalten sind.

### ARBEITSSCHWERPUNKTE

- Planung und Durchführung von Messfahrten gem. Datensatz-ODD
- Aufbau einer Datenpipeline für Zusammenstellung der (Sensor-)Daten
- Klärung und Umsetzung rechtlicher Aspekte, z. B. Umsetzung von Datenschutzmaßnahmen
- Erstellung von DevKit, Tutorials und einer Projektwebsite




3D Annotationen (rote Boxen) für 27 verschiedene Klassen sind im Datensatz enthalten.

### ERGEBNISSE

- Veröffentlichung des „weltweit erster öffentlicher Datensatz für das Autonome Trucking” im Dezember 2024
- Vorstellung des Datensatzes auf der NeurIPS2024, einer der weltweit renommiertesten KI Konferenzen
- Stärkung und Vereinfachung von Kooperationen mit Universitäten: Datensatz ist bereits Grundlage für mehrere wissenschaftliche Arbeiten
- Informationen zum Datensatz, Tutorials und Downloadlinks sind über die MAN TruckScenes Website auffindbar


www.man.eu/truckscenes

# AP 8: Funktionsentwicklung

Leonie Wulf; Dr. Korbinian Schechner– MAN Truck & Bus SE

## 3.8 AP 8: Funktionsentwicklung

*Arbeitspaketleitung: Leonie Wulf; Dr. Korbinian Schechner;– MAN Truck & Bus SE*

### 3.8.1 Zusammenfassende Ergebnisdarstellung

Im Verlauf des Projekts wurde im Themenbereich Bewegungsplanung und -prädiktion über drei Jahre hinweg ein leistungsfähiges System für automatisiertes Fahren auf Autobahnen entwickelt, integriert und erprobt. Die Entwicklung folgte einem strukturierten, iterativen Vorgehen, das von konzeptionellen Grundlagen über prototypische Implementierungen bis hin zur Integration auf der Zielplattform und umfangreichen Realfahrzeugtests reichte.

Zu Beginn stand die konzeptionelle Fundierung im Vordergrund. Es wurden grundlegende Anforderungen an die Bewegungsplanung definiert, insbesondere im Hinblick auf Schnittstellen zur Trajektorienfolgeregelung und die Modellierung fahrzeugspezifischer Fähigkeiten. Frühzeitig wurde erkannt, dass für Letzteres eine vollständige Abbildung aller Antriebsstrangdetails nicht zielführend ist. Stattdessen wurde ein pragmatischer Ansatz verfolgt, bei dem aggregierte Zustandsinformationen – wie das aktuell verfügbare Beschleunigungspotenzial – in die Planung zurückgeführt werden. Dies ermöglichte eine Reduktion der Komplexität bei gleichzeitig hoher Relevanz für die Fahrdynamik. Insgesamt konnte durch die Modellierung und Rückführung aktueller Fahrzeugfähigkeiten eine deutlich verbesserte Ausführbarkeit der geplanten Trajektorien erreicht werden. Dies führte zu einem verbesserten Trajektorienfolgeverhalten.

In der nächsten Entwicklungsstufe wurde der Fokus auf die Berücksichtigung von Interaktion in der Bewegungsplanung gelegt. Es entstand ein funktionaler Prototyp, der kooperative Szenarien wie Spurwechsel mit einbezieht und das Verhalten anderer Verkehrsteilnehmer in die Bewertung von Trajektorien einfließen lässt. Wie stark ein anderes Fahrzeug aufgrund eines Ego-Manövers zu Reaktion gezwungen wird, in der Regel zu Abbremsen, floss in die Bewertung der Güte der geplanten Trajektorien ein. Die Integration dieser Interaktionslogik führte zu einer deutlich realitätsnäheren Planung, erforderte jedoch auch eine differenzierte Bewertung von Risiken und Reaktionen. Erste simulative Tests zeigten vielversprechende Ergebnisse, insbesondere hinsichtlich Effizienzgewinnen bei Spurwechseln. Gleichzeitig wurde die Kostenfunktion, die das Verhalten des Planers maßgeblich bestimmt, in ein regelbasiertes System überführt, um Transparenz und Nachvollziehbarkeit zu erhöhen.

Mit zunehmender Reife der Module rückte die Integration auf der Zielplattform in den Vordergrund. Die Bewegungsplanung wurde erfolgreich mit der Trajektorienfolgeregelung gekoppelt und auf dem Sensorfahrzeug in Betrieb genommen. In diesem Zusammenhang wurden auch neue Konzepte wie das „Contingency Planning“ eingeführt, dass die parallele Berechnung von Notfalltrajektorien ermöglicht, sowie das „Speed Shaping“, welches eine adaptive Wunschgeschwindigkeit vorgibt. Beide Maßnahmen verbesserten das vorausschauende Verhalten des Systems erheblich und führten zu einer robusteren Planung in Hochgeschwindigkeitsszenarien.

Die anschließende Inbetriebnahme auf der Autobahn – insbesondere auf einem Abschnitt der A9 – markierte einen wichtigen Meilenstein. Hier zeigte sich, dass das System in typischen Autobahnszenarien wie Abstandhalten und Einschermanövern stabil agiert. Gleichzeitig wurden jedoch auch Grenzen der bisherigen Architektur deutlich, insbesondere hinsichtlich der Skalierbarkeit auf eine Vielzahl möglicher Szenarien. Die ursprünglich verfolgte Idee einer szenariospezifischen Parametrierung der Kostenfunktion erwies sich als nicht ausreichend leistungsfähig. Stattdessen wurde ein neuer Architekturansatz entwickelt, der zwei parallel arbeitende Post-Perception-Komponenten vorsieht: einen AI-basierten Nominalplaner für hohe Generalisierbarkeit und einen sicherheitsorientierten Redundanzpfad zur Generierung von Notfalltrajektorien. Diese funktionale Redundanz erlaubt eine risikobewusstere Nominalplanung bei gleichzeitig hoher Sicherheit.

Im letzten Projektabschnitt wurde die Notfalltrajektorienplanung weiterentwickelt und in das ADS integriert. Die Implementierung basiert auf einem suchbasierten Verfahren mit Bewegungsprimitiven und nutzt konservative Erreichbarkeitsmengen anderer Verkehrsteilnehmer als Grundlage. Durch die Berücksichtigung von Unsicherheiten im Bewegungszustand sowie in der Reglerausführung können robuste, kollisionsfreie Trajektorien erzeugt werden. Dieses Verfahren stellt einen wesentlichen Beitrag zur Sicherheitsargumentation des Gesamtsystems dar, insbesondere im Hinblick auf gesetzliche Anforderungen wie das Minimum Risk Maneuver (MRM). Erste Inbetriebnahmetests im Fahrzeug wurden erfolgreich durchgeführt.

Insgesamt zeigen die im Projekt erarbeiteten Ergebnisse eindrucksvoll, wie durch eine systematische, schrittweise Entwicklung ein leistungsfähiges System zur Bewegungsplanung für automatisiertes Fahren realisiert werden kann. Die Kombination aus interaktionsbewusster Planung, vorausschauendem Verhalten, funktionaler Redundanz und sicherheitsausgerichteter Architektur bildet eine belastbare Grundlage für den Einsatz in realen Verkehrsszenarien. Die entwickelten Konzepte sind nicht nur technisch tragfähig, sondern auch anschlussfähig an regulatorische Anforderungen und zukünftige Erweiterungen.

Für die Umsetzung der von der Bewegungsplanung erzeugten Trajektorie wurde eine hochperformante Bewegungsregelung für automatisierte Nutzfahrzeuge im Hochgeschwindigkeitsbetrieb entwickelt. Ausgehend von bestehenden Regelungsansätzen wurde die Trajektorienfolgeregelung umfassend überarbeitet und an die Anforderungen des Autobahnbetriebs angepasst. Die Integration in die Gesamtarchitektur sowie die enge Kopplung mit der Bewegungsplanung führten zu einer signifikanten Verbesserung der Regelgüte. Besonders im Bereich der Querregelung konnten durch gezielte Optimierungen und die Einführung eines stochastischen MPC-Reglers mit Beobachter deutliche Fortschritte erzielt werden. Der bestehende Regler, basierend auf einem Pure-Pursuit-Ansatz, wurde dabei um einen adaptiven Lookahead-Radius sowie einen integrierten PI-Regler auf Quer- und Orientierungsabweichung erweitert, um Abweichungen durch Untersteuern, Fahrbahnquerneigung und andere dynamische Effekte zu minimieren. Als Forschungserweiterung wurde zusätzlich ein stochastischer MPC-Regler entwickelt. Die Regelung wurde erfolgreich auf Teststrecken und öffentlichen Autobahnen validiert. Die folgenden Abbildungen zeigen die Entwicklung der Regelgüte. Abbildung 57 zeigt das Testergebnis vor den Verbesserungen und Optimierungen. Abbildung 58 zeigt das Ergebnis nach den Verbesserungen. Es ist klar erkennbar, dass sich die Fehlerhäufigkeit zugunsten der niedrigen Abweichungen verschoben hat.

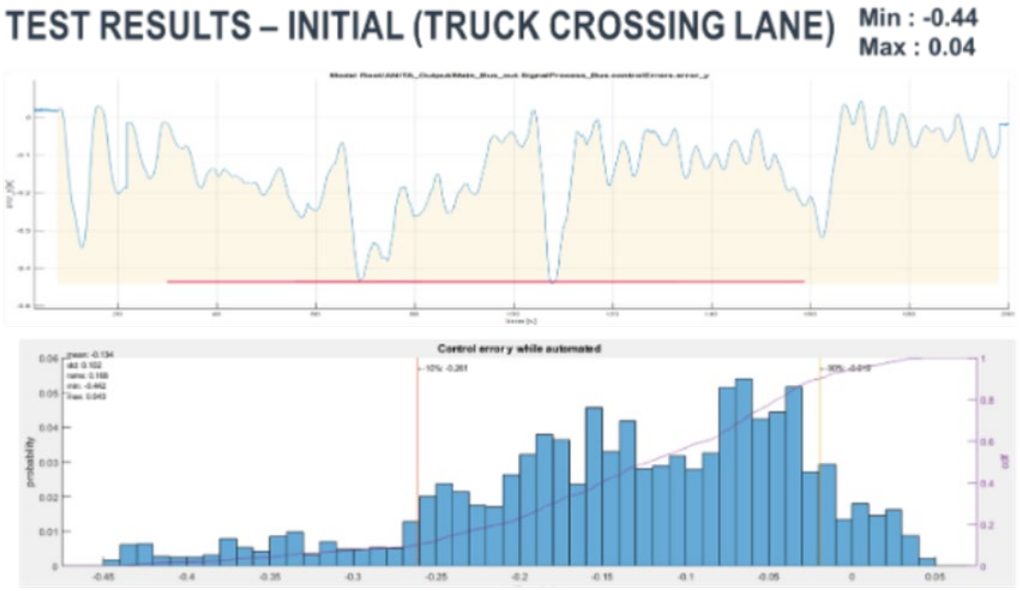



Abbildung 57 Testergebnis vor Verbesserungen und Optimierungen.

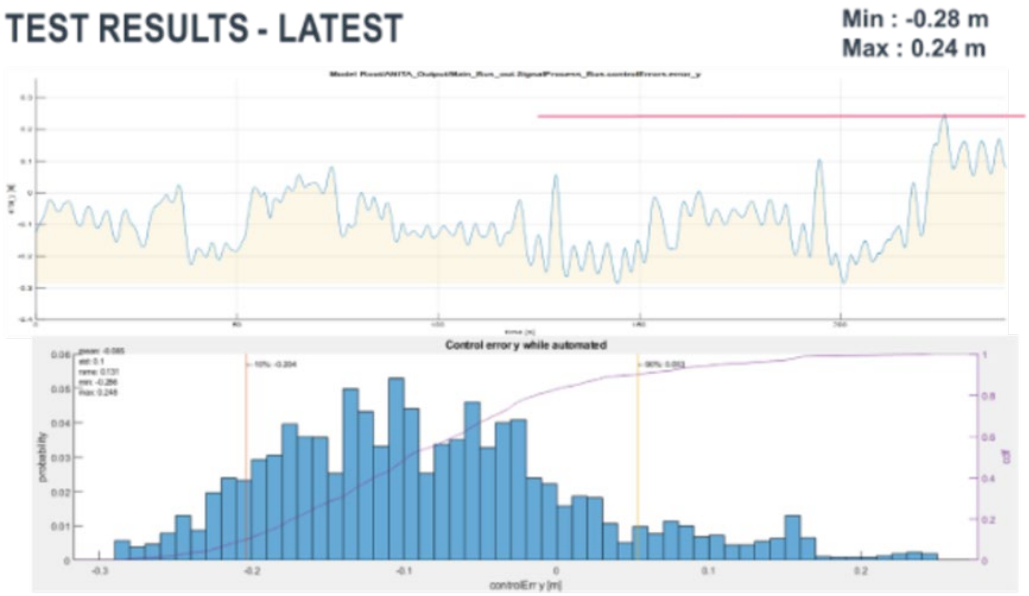



Abbildung 58 Testergebnisse nach Verbesserungen und Optimierungen.

Ergänzend wurde ein Testauswertungsframework entwickelt, das standardisiert Performance-Indikatoren erhebt.

Bei schweren Nutzfahrzeugen prägen die **Antriebsstrangdynamik** und die vergleichsweise **träge Systemantwort** das Fahrverhalten maßgeblich. Insbesondere bei hohen Lasten treten zahlreiche **Gangwechsel** auf, die mit deutlichen Totzeiten und Schwankungen im Beschleunigungsverhalten verbunden sind. Werden diese Effekte in der Bewegungsplanung nicht berücksichtigt, können geplante Geschwindigkeitstrajektorien technisch nicht umsetzbar sein.

Dies zeigt sich in Abbildung 59: Hier ist das Beschleunigungspotenzial fehlerhaft modelliert. Während der Gangwechsel kann das Fahrzeug die geplante Geschwindigkeit nicht einhalten, was zu wachsenden Regelabweichungen in Längsposition (x) und Geschwindigkeit (v) führt.

In der Folge kommt es zu einem Reset des Planers, was Oszillationen und eine insgesamt größere Systemabweichung verursacht.

In Abbildung 60 hingegen wird das Beschleunigungspotenzial korrekt erfasst, wobei insbesondere die Totzeiten während der Gangwechsel berücksichtigt werden. Dadurch ist die geplante Geschwindigkeitstrajektorie realisierbar, die Regelabweichungen bleiben gering, und das Gesamtsystem arbeitet stabil und ohne Oszillationen.

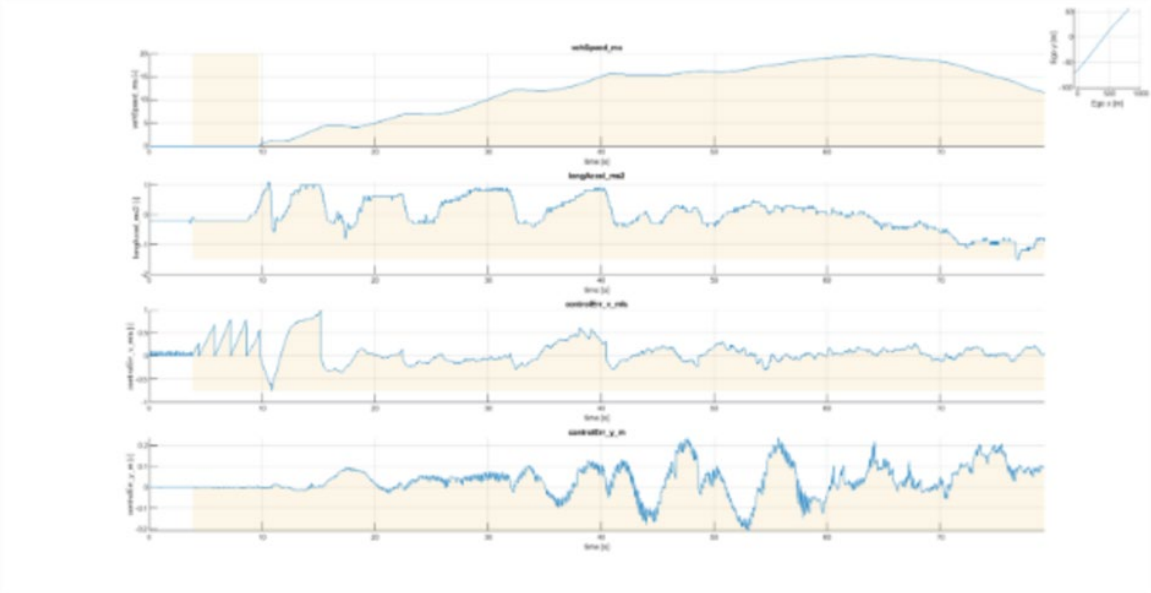


Abbildung 59 Laufzeitplot, Messfahrt auf externem Prüfgelände (ADAC).
Beschleunigungsverhalten mit fehlerhaft definiertem Beschleunigungspotenzial: während der Gangwechsel kann die geplante Geschwindigkeit nicht eingehalten werden. Dies führt zu wachsenden Regelabweichungen, Planer-Resets und Oszillationen.

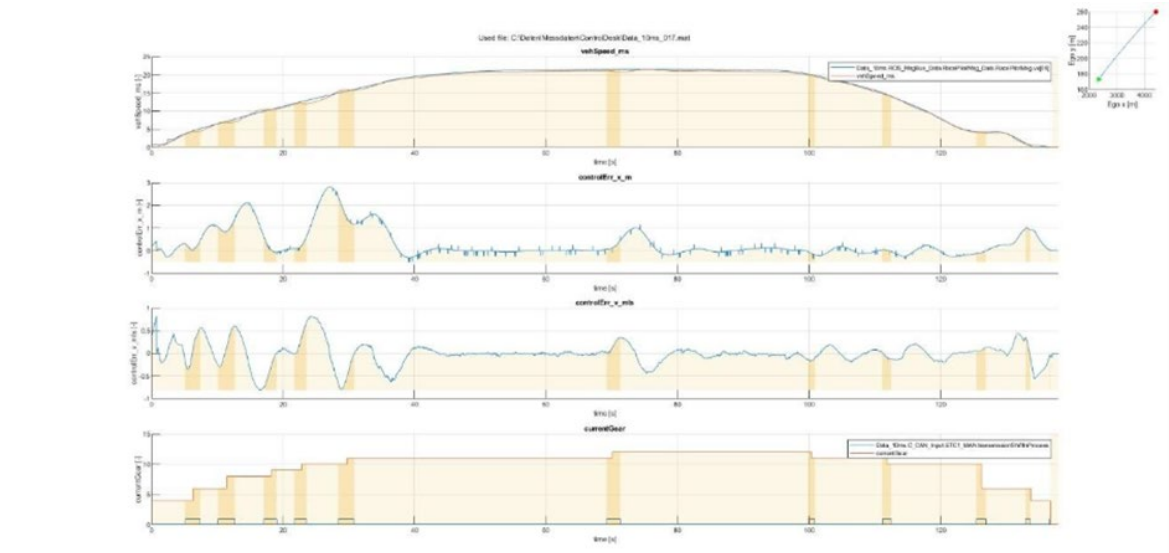


Abbildung 60 Laufzeitplot, Messfahrt auf externem Prüfgelände (ADAC).
Beschleunigungsverhalten mit korrekt modelliertem Beschleunigungspotenzial unter Berücksichtigung der Totzeiten während der Gangwechsel: geplante Geschwindigkeit ist realisierbar, Regelabweichungen bleiben gering, stabiles Systemverhalten ohne Oszillationen und Reset.

Ein weiterer Schwerpunkt lag auf der Anpassung der Regler bei Umschaltung der Aktoren, insbesondere beim Wechsel von einer klassischen Lenkung auf ein Steer-by-Brake-System. Diese Umschaltfähigkeit wurde erfolgreich in die Regelarchitektur integriert und getestet. Die Leistungsfähigkeit der entwickelten Motion-Control-Komponenten konnte im Rahmen der ATLAS-L4-Abschlussdemonstration eindrucksvoll unter Beweis gestellt werden.

Im Bereich Vehicle Control wurde die Fahrzeugregelung konsequent auf die Anforderungen eines fail-operational Base Vehicles ausgerichtet. Nach der erfolgreichen Umsetzung der Grundfunktionalität für zwei Generationen von E/E-Architekturen lag der Fokus auf der Entwicklung und Integration redundanter Aktuatorikpfade für Bremse und Lenkung. In enger Zusammenarbeit mit Projektpartnern wie Bosch und Knorr wurden Sicherheitskonzepte erarbeitet und in die Systemarchitektur überführt. Die Implementierung des System Managements, das zentrale Funktionen wie Selbstüberwachung, Betriebsmodusmanagement und Redundanzsteuerung umfasst, stellte einen Meilenstein dar.

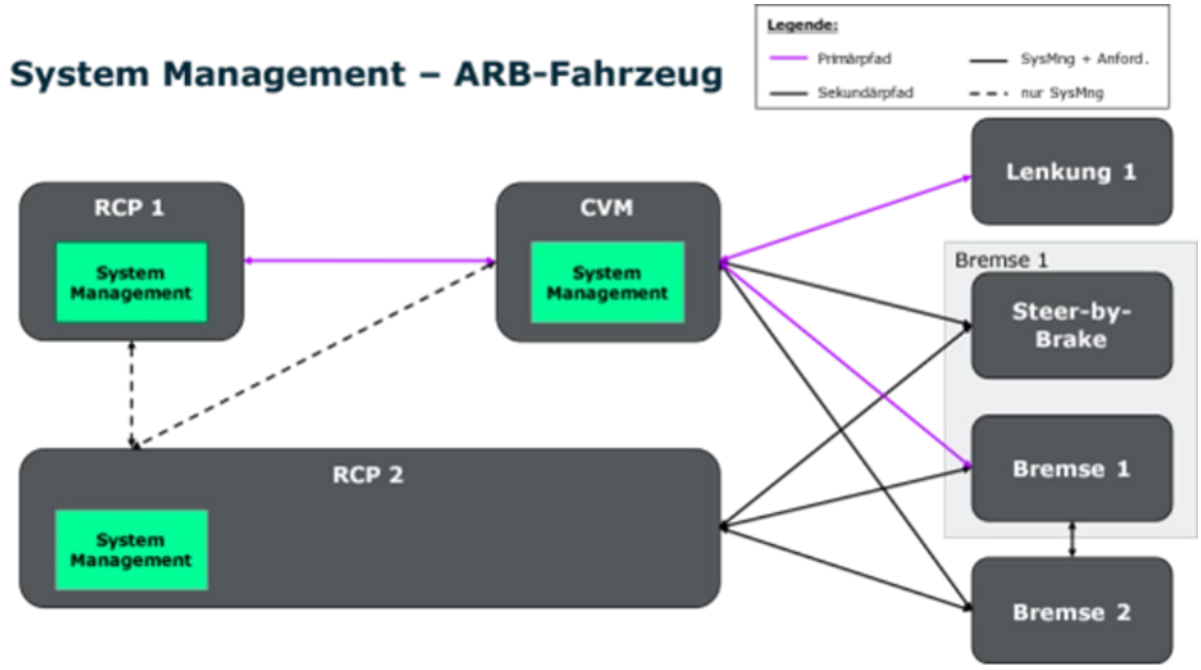



Abbildung 61 Redundanzstruktur in ARB-Fahrzeug und Ausprägung des System Managements mit zwei Rapid Control Protoyping (RCP) Systemen und einen zentralen Fahrzeugsteuergerät (CVM).

Ein zentrales Ergebnis war die erfolgreiche Umsetzung der Umschaltung der Redundanzpfade bei Ausfall einer oder mehrerer Redundanzen. Dabei wurde sichergestellt, dass das Fahrzeug auch bei Ausfall eines primären Aktuators sicher auf einen sekundären Pfad umschalten kann. Die Funktionalität der Vehicle Control wurde erfolgreich im Rahmen der ATLAS-L4-Abschlussdemonstration präsentiert und validiert. Abbildung 61 stellt die Redundanzstruktur und Ausprägung des System Managements im ARB-Fahrzeug dar.

Das Betriebsmodusmanagement wurde als zentrale Steuerinstanz für den automatisierten Fahrbetrieb konzipiert und über alle Projektphasen hinweg systematisch weiterentwickelt. Beginnend mit der Definition gesetzeskonformer Betriebsmodi und deren softwareseitiger Umsetzung, wurde das System sukzessive um Funktionen zur Redundanz- und Fehlerbehandlung erweitert. Die Einführung eines modularen System Managements ermöglichte eine klare Trennung und Koordination von Subsystemen wie Operation Management, Automation Management, Diagnostic Management und Redundancy Management.

Ein besonderer Fokus lag auf der Implementierung und Erprobung eines Redundanzmanagements, das gezielt auf den Ausfall von redundanten Komponenten reagieren kann. Dieses Managementsystem koordiniert die Umschaltung auf verfügbare Alternativpfade und unterstützt die Einleitung eines Minimum Risk Manövers. Die Leistungsfähigkeit des Redundanzmanagements wurde im Rahmen der ATLAS-L4-Abschlussdemonstration erfolgreich demonstriert.

In einem weiteren Themenkomplex entwickelte MAN ein umfassendes System zur Selbstüberwachung des automatisierten Fahrzeugs. Der Fokus lag auf der Eigenbewegungsschätzung des Chassis sowie der Fähigkeitenschätzung zur Bewertung der Systemgrenzen. Zu Beginn wurden verschiedene Odometrieansätze verglichen, wobei das Modul „Egomaster“ als besonders vielversprechend identifiziert und in die Projektarchitektur integriert wurde. Dieses wurde sukzessive an neue EE-Architekturen und Sensorkomponenten angepasst und erfolgreich in Versuchsträgern erprobt. Parallel dazu wurden Konzepte zur Schätzung der Bewegung von Kabine und Trailer entwickelt. Die Modularisierung des Odometrieschätzers ermöglichte eine flexible Portierung und Anpassung an unterschiedliche Entwicklungsframeworks. Die Integration in die Gesamtarchitektur sowie die enge Abstimmung mit angrenzenden Modulen wie der Trajektorienfolgeregelung führten zu einer robusten und leistungsfähigen Lösung. Die kontinuierliche Verbesserung der Signalqualität und Systemrobustheit wurde durch eine automatisierte Infrastruktur zur Auswertung von Messdaten unterstützt. Die Relevanz dieser Funktionalität für den Highway-Use-Case wurde durch erfolgreiche Tests auf dem ADAC-Testgelände bestätigt (siehe Abbildung Testfahrten auf externer, abgesperrter Teststrecke Anfang Oktober 2023).


Abbildung 62 Testfahrten auf externer, abgesperrter Teststrecke Anfang Oktober 2023

#### 3.8.1.1 Self Awareness TU Braunschweig (AP 8.3)

Im Rahmen des Projekts ATLAS-L4 stellte das Thema der Self-Awareness einen zentralen Fokus dar. Eine konzeptionelle Betrachtung erfolgte seitens Mitarbeiter des Instituts für Regelungstechnik insbesondere im Arbeitspaket 3.3, während im Arbeitspaket 8.3 die Auswirkungen auf die Entwicklung von Funktionen des Fahrzeugs im Mittelpunkt stand.

Systeme mit technischer Self-Awareness sind dabei insbesondere in der Lage, auch unter Unsicherheit zu agieren, indem sie diese Unsicherheiten (soweit möglich) explizit repräsentieren. Ein zentraler Aspekt gemäß Projektvorhaben bestand daher in der Untersuchung von Unsicherheiten, die im Kontentext des Betriebs automatisierter Fahrzeuge eine große Rolle spielen. Im Hinblick auf die Entwicklung von automatisierten Fahrzeugen mit Self-Awareness besteht insbesondere das Interesse, Unsicherheiten, die sich im Betrieb bemerkbar machen, auch messen zu können. Zu diesem Aspekt wurden verschiedene grundlegende Techniken zur Identifikation von Unsicherheiten betrachtet, so wie z. B. das Aufstellen von Unsicherheitsmatrizen.

Für die Verhaltensgenerierung zur Laufzeit spielen vor allem die Fähigkeiten des Systems eine Rolle. Die Fähigkeiten des Systems müssen hinreichend sein, um eine gegebene Situation zuverlässig zu meistern. Am Institut für Regelungstechnik der TU Braunschweig wurden daher in der Vergangenheit Ansätze untersucht, wie sich die Fähigkeiten des Systems zur Laufzeit bestimmen lassen. Jeder Fähigkeit sind dabei entsprechende Performanzgrößen zugeordnet. Die Zusammenhänge zwischen den Fähigkeiten bzw. jenen Performancegrößen wird dabei unter anderem durch sogenannte Fähigkeitsgraphen modelliert, die in Vorarbeiten des Instituts um implementierungsspezifische Einflussfaktoren erweitert wurden.

Durch die Betrachtung von Methoden aus dem Bereich der Unsicherheitsanalyse (sowie der Sensitivitätsanalyse und der Merkmalsauswahl) wurde früh erkannt, dass die Beobachtung von Performanzgrößen, die sich den Fähigkeiten des Fahrzeugs zuordnen lassen und die für die Verhaltungsverhaltensentscheidung dienen, häufig nur auf Basis zahlreicher Annahmen und auf einer begrenzten Menge technisch messbarer Größen fußt, die zudem von Unsicherheiten betroffen sein können. Diese Erkenntnis spricht zur Laufzeit für die Nutzung von Schätzverfahren, die eine mathematische Zuordnung der Größen und jenen Performanzgrößen erlauben, die auch diese Unsicherheit berücksichtigt. Das heißt, stochastische und datengetriebene Verfahren spielen hier eine große Rolle.

Um die entsprechenden Zusammenhänge nur noch quantitativ zu modellieren, kann auf eine Vielzahl von Methoden aus dem Bereich der stochastischen und datengetriebenen Modellierungen zurückgegriffen werden. Vor diesem Hintergrund wurden verschiedene Methoden aus der Literatur betrachtet, sowie eine Softwarebibliothek entwickelt, die es erlaubt, verschiedene solcher Modelltypen einzubinden und für die Modellierung der Fähigkeiten zu nutzen. Die Bibliothek wurde dabei in einer Simulation am Beispiel der Bewegungsregelung eines automatisierten Fahrzeugs untersucht. Parallel erfolgte auch eine Aufarbeitung der wesentlichen Fähigkeiten eines Lkws und seiner redundanten Brems- und Längssysteme, die in verschiedenen Fähigkeitsgraphen modelliert wurden.

### 3.8.1.2 Self Awareness TU München (AP 8.3)

Eine sichere autonome Fahrzeugführung bedarf der Kenntnis über die fahrdynamischen Stabilitätsgrenzen. Ein wesentlicher Einfluss ist dabei der Reifen-Fahrbahn-Kontakt. Im Rahmen von ATLAS-L4 wurden daher verschiedene Ansätze zur Schätzung des aktuellen und des zukünftigen Reifenpotentials untersucht. Diese lassen sich in Ursachen- und Effekt-basierte Methoden untergliedern.

Die Ursachen-basierten Ansätze bewerten dabei das Kraftschlusspotential basierend auf Fahrbahnbeschaffenheit und Fahrbahnoberfläche. Hierfür werden in der Regel optische Sensoren (bspw. Kameras) verwendet. Im ATLAS-L4 Projekt wurden zunächst verschiedene Datensätze miteinander verglichen und auf deren Potential untersucht. Der gewählte RoadSaW Datensatz liefert Kamerabilder aus einem Lkw und zugehörige Labels für Fahrbahntyp (Asphalt, Beton, Kopfsteinpflaster) und Wasserfilmhöhe. Anschließend wurden verschiedene Algorithmen miteinander verglichen. Dabei wurde eine Genauigkeit von 97,54% zur Klassifizierung von Fahrbahntyp und Fahrbahnbeschaffenheit (nass/trocken) und von 73,68% zur weiteren Unterteilung in vier Nässe-grade (trocken, feucht, nass, sehr nass) erreicht.

Effekt-basierte Ansätze nutzen messbare Effekte eines veränderten Reibwerts. Hierbei werden Reifenmodelle sowie der gemessene Reifenschlupf verwendet. Die Reifenkraft hängt stark vom aktuellen Reifenzustand (Längs/Querschlupf) ab. Der maximale Reifen-Fahrbahnkraftschluss kann sich dabei bei unterschiedlichen Schlupfwerten ergeben. Entsprechend ist eine direkte Messung des Reifen-Fahrbahn-Kraftschlusspotentials nicht ohne weiteres möglich. Um dennoch einen Referenzwert zu schaffen, wurde ein Open-Source Tool zur Parametrierung von Reifenmodellen erstellt und die verbleibende Unsicherheit basierend auf den Eingangsparametern quantifiziert. Diese Unsicherheiten wurden außerdem mit einer Sensitivitätsanalyse der Parameter des Reifenmodells verglichen, um die Schätzung zu validieren. Zur Schätzung des Reibwerts wurden anschließend verschiedene klassische Methoden (bspw. Kalman Filter) und Machine Learning Ansätze (bspw. Physics Informed Neuronal Networks, Reinforcement Learning) entwickelt. Aufgrund der Parametersensitivität eignet sich jedoch keine dieser Methoden zur Quantifizierung des Kraftschlusspotentials bei niedrigen Anregungen. Entsprechend wurde ein neues Reifenmodell basierend auf Gauss-Prozessen mit zusätzlicher Unsicherheitsquantifizierung entwickelt. Dieses wurde anschließend in eine Fahrzeugzustandsschätzung integriert, um das Potential der zusätzlichen Unsicherheitsschätzung aufzuzeigen.

Die entwickelten Algorithmen können einerseits zur ODD-Erkennung (bspw. nasse Fahrbahn) als auch zum Einsatz in Modellbasierten Zustandsschätzern sowie Planungs- und Regelungsalgorithmen verwendet werden. Die Kamera Detektion ermöglicht dabei eine frühzeitige Erkennung veränderter Umgebungsbedingungen. Die zusätzliche Unsicherheitsquantifizierung kann besonders bei statistischen Ansätzen zur Zustandsschätzung (bspw. Kalman Filter oder Partikelfilter) oder stochastischen Reglerarchitekturen genutzt werden. Der Einsatz wurde in einer Zustandsschätzung auf realen Daten validiert und liefert eine bessere Geschwindigkeits- und Schwimmwinkelschätzung als analytische Reifenmodelle. Zudem konnte die verbesserte Robustheit gegenüber Modellmismatch gezeigt werden.

### 3.8.1.3 Motion Control TU München (AP 8.4)

Dieser Bericht bündelt vier komplementäre Ansätze, die die Trajektorienfolgeregelung autonomer Fahrzeuge im fahrdynamischen Grenzbereich in Echtzeit ermöglichen. Im Mittelpunkt steht die Vereinbarkeit von geringer Regelabweichung, Komfort, kurzen Reaktionszeiten und strikter Nebenbedingungserfüllung mit Robustheit gegenüber Störungen, Schätzfehlern und Modellunsicherheiten bei nichtlinearer Fahrdynamik. Nominale nichtlineare MPC sind rechenintensiv und störanfällig; klassische robuste und stochastische MPC sichern ab, werden durch aufwendige Unsicherheitsfortpflanzung, konservative Leistung und große nichtlineare Optimierungsprobleme jedoch schnell unhandlich. Unsere Ziele lauten daher: (1) robuste Einhaltung aller Nebenbedingungen trotz Unsicherheit, (2) selbstadaptive Parametrierung ohne externe Expert:innen, die sich wechselnden Sensorqualitäten und Betriebsbedingungen anpasst, und (3) skalierbares, automatisiertes Design für heterogene Fahrzeugflotten bei konsequenter Echtzeitfähigkeit. Methodisch setzen wir auf Sicherheitsmargen ohne unnötige Komplexität, eine begrenzte, entscheidungsrelevante Unsicherheitsbehandlung statt Divergenz über lange Horizonte und auf kontextbewusste, sicherheitsabgesicherte Lernmechanismen, die die Struktur des nichtlinearen MPC respektieren.

*Ansatz 1: R²NMPC – reduzierte robustifizierte NMPC*

Der erste Ansatz reduziert robuste NMPC auf die Komplexität einer vergleichbaren nominalen MPC, ohne auf die Absicherung von Nebenbedingungen zu verzichten. Ellipsoidale Unsicherheitsmengen werden nicht als zusätzliche Entscheidungsvariablen in das Optimierungsproblem eingebunden, sondern mithilfe der Sensitivitäten der zuletzt gelösten Aufgabe approximiert. Ebenso werden Backoffs für nichtlineare Nebenbedingungen aus Gradienten der Vorlösung bestimmt. Dadurch entfällt die teure explizite Fortpflanzung von Unsicherheit innerhalb der Optimierung, während die Rückkopplung im Regelkreis die Näherung stützt. Das Ergebnis ist robuste Trajektorienfolge bei hohen Geschwindigkeiten mit hoher Lösungshäufigkeit und belastbarer Nebenbedingungserfüllung – bei deutlich reduzierten Rechenzeiten im Vergleich zu konventionellen robusten NMPC-Varianten.

*Ansatz 2: SNMPC mit Uncertainty Propagation Horizon und Polynomial Chaos*

Der zweite Ansatz adressiert die zentrale Schwäche vieler stochastischer MPCs: die divergierende Unsicherheitsfortpflanzung über lange Prädiktionshorizonte. Kernidee ist der Uncertainty Propagation Horizon (UPH), der die Fortpflanzung auf den tatsächlich wirksamen Zeitraum begrenzt und damit sowohl Konservatismus als auch Rechenlast reduziert. Zur effizienten Quantifizierung von Erwartungswerten und Varianzen nichtlinearer Größen wird Polynomial Chaos eingesetzt. Wahrscheinlichkeitsnebenbedingungen werden deterministisch approximiert und in die Optimierung integriert. Das Resultat sind echtzeitfähige Lösungen, eine nachweislich geringere Regelabweichung gegenüber nominalen MPCs bei Störungen und eine verbesserte Machbarkeit zuvor infeasibler stochastischer Formulierungen, selbst bei ungenauen Unsicherheitsannahmen. Nach unserem Kenntnisstand handelt es sich zugleich um die weltweit erste SNMPC, die in Echtzeit sowohl in der Simulation als auch im Realfahrzeug zuverlässig betrieben wurde.

*Ansatz 3: Adaptive SNMPC mit vorausschauendem Reinforcement Learning*

Der dritte Ansatz erweitert die stochastische MPC um eine adaptive Ebene, die zwei wirksame Stellhebel kontextsensitiv bestimmt: den Robustifizierungsgrad und die Länge des UPH. Ein vorausschauender Agent bezieht aktuellen Fahrzeugzustand, angenommene Störstatistiken, Gütemaße und den bevorstehenden Trajektorienverlauf ein und wählt eine für die anstehende Fahrsituation passende Konfiguration. So können in ruhigen Phasen konservative Backoffs reduziert und in kritischen Szenarien gezielt erhöht werden; der UPH wird nur so lang gewählt, wie es die Situation erfordert. Die Ergebnisse belegen verbesserte Machbarkeit unter starken, zeitvarianten Störungen und robuste Trajektorienfolgeregelung bei hohen Geschwindigkeiten, ohne die Echtzeitfähigkeit zu gefährden.

*Ansatz 4: Safe RL getriebene weights-varying MPC auf Basis eines Pareto-Katalogs*

Der vierte Ansatz löst das praktische Tuningproblem der MPC-Kostenfunktion. Die manuelle Parametrierung der Gewichte ist zeit- und personalintensiv, liefert oft suboptimale Kompromisse und skaliert schlecht auf unterschiedliche Fahrzeugtypen und wechselnde Einsatzbedingungen; ein automatisiertes, datengetriebenes Tuning ist daher essenziell. Statt kontinuierlich im sensiblen Gewichtsraum zu lernen, wird zunächst mittels multiobjektiver Bayes'scher Optimierung ein sicherer Katalog an Pareto-optimalen Gewichtssätzen aufgebaut. Ein RL-Agent agiert dann über eine diskrete, sicherheitsabgesicherte Aktionsmenge: Er wählt situativ den passenden Gewichtssatz aus dem Katalog. Diese Zweistufigkeit koppelt Sicherheit und Performance: Untrainiert verhält sich das System bereits Pareto-optimal; nach Training übertrifft es die ursprüngliche Paretofront, indem es die Gewichtsentscheidung kontextsensitiv antizipiert. Darüber hinaus bildet das Verfahren die Grundlage für ein automatisiertes, skalierbares Gewichtstuning, das die schnelle Übertragung auf unterschiedliche Fahrzeugtypen und große Flotten mit minimalem manuellem Aufwand ermöglicht.

*Validierung und Leistungsfähigkeit*

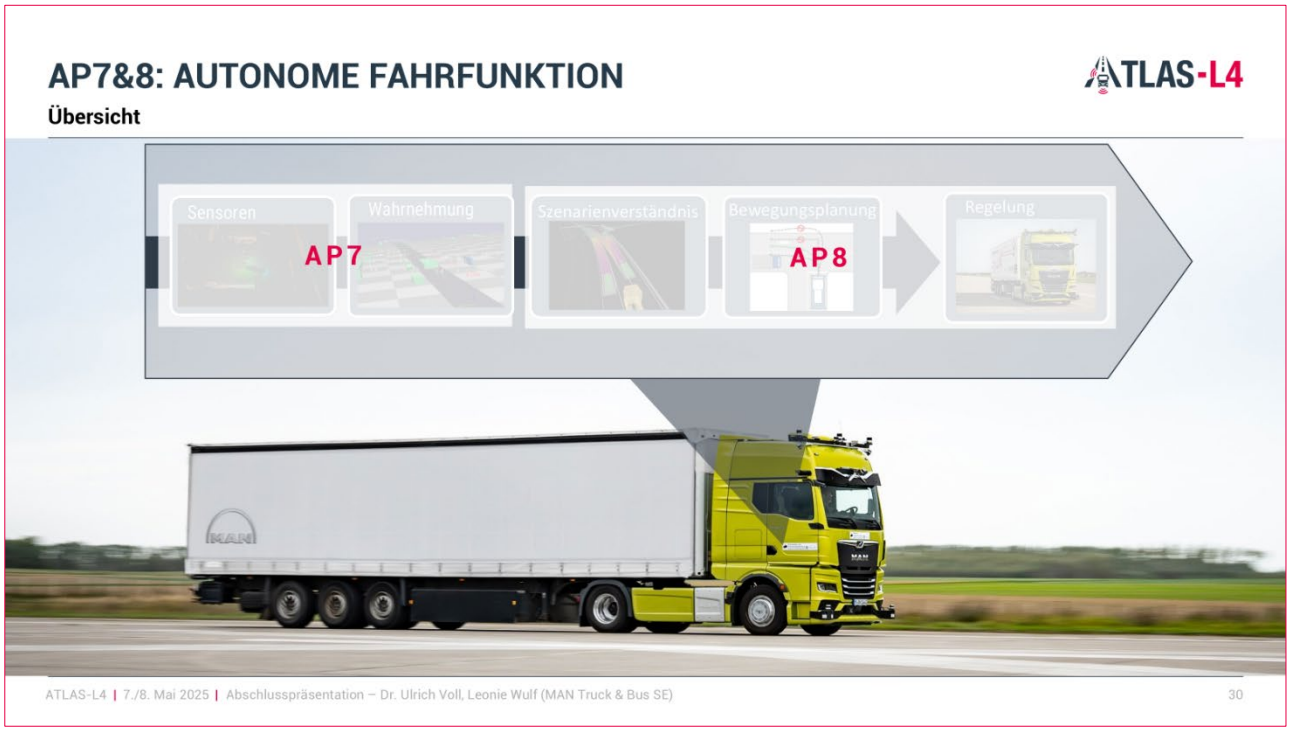
Alle vier Ansätze wurden in einem gestuften Verfahren validiert: systematische Simulationen mit variierenden Störungen, Strecken und Grenzsituationen sowie Erprobung auf universitären Fahrzeugplattformen. Gemeinsam ist den Verfahren, dass sie hohe Lösungshäufigkeiten im zweistelligen bis dreistelligen Hertz-Bereich erreichen, die Trajektorienfolgeregelung auch bei hohen Geschwindigkeiten stabil bleibt und Nebenbedingungen deutlich zuverlässiger eingehalten werden als bei nominalen Referenzen. Der UPH-Ansatz wandelte zuvor nicht lösbare stochastische Aufgaben in lösbare, das adaptive Verfahren minimierte Maximalabweichungen unter starken Störungen, und die reduzierte robuste Formulierung erzielte robustes Verhalten bei der Rechenlast einer nominalen MPC. Die Safe-RL-Kopplung zeigte darüber hinaus, dass selbst ohne Training ein sicheres, effizientes Verhalten möglich ist, und mit Training zusätzliche Leistungsgewinne erzielt werden.

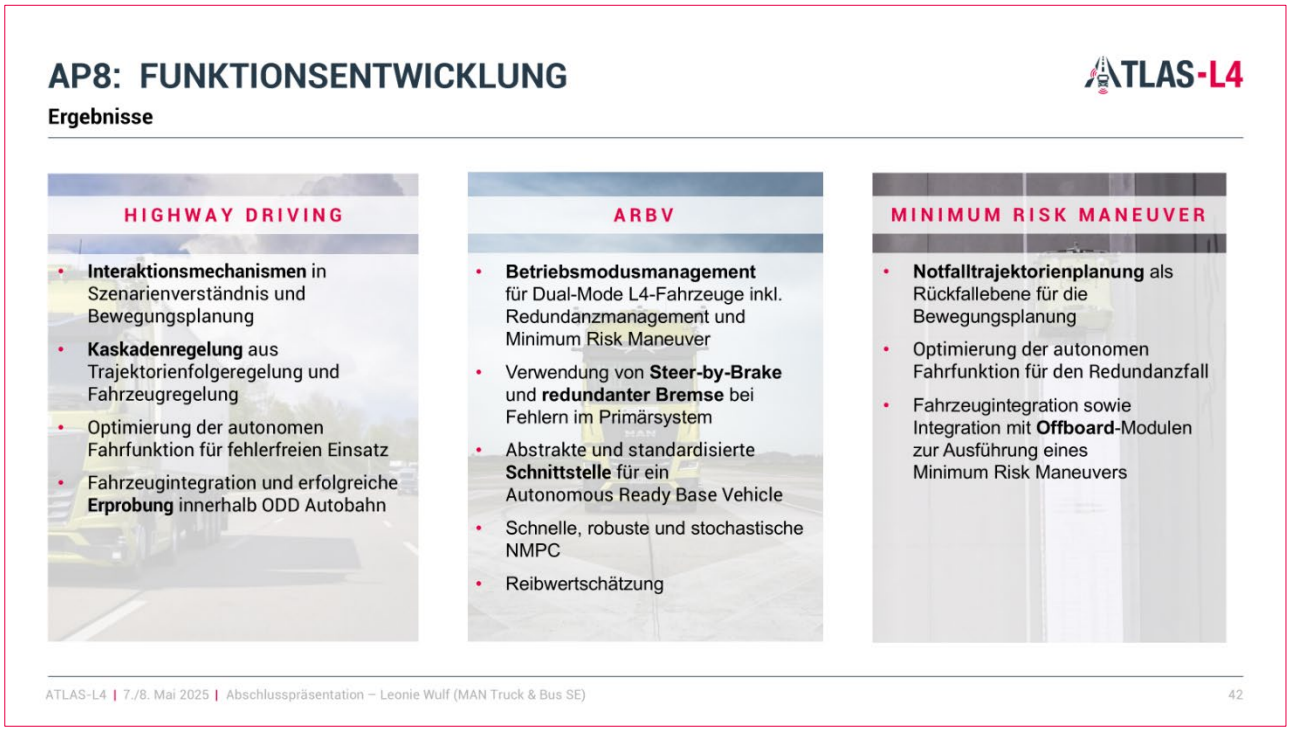
Im Rahmen der Abschlusspräsentation wurden die Fähigkeiten am realen TUM-Passagierfahrzeug demonstriert. Gezeigt wurde ein adaptiver, RL-getriebener stochastischer MPC unter ausgeprägten Unsicherheiten: fehlende Quer- bzw. Schräglaufwinkelmessung, große Zustandschätzunsicherheiten, Sensorsignalstörungen, externe Störungen wie Seitenwind und spürbare Aktuatorverzögerungen. Das Fahrzeug wurde in hochdynamischen Szenarien mit hohen Geschwindigkeiten, engen Kurven und deutlichen Längs- und Querbeschleunigungen bis in den Bereich von etwa 0,6 g stabil mit geringer Regelabweichung geführt.

*Nutzen, Mehrwert und Fazit*

Die vorgestellten Verfahren erhöhen die Sicherheit durch systematische Nebenbedingungsabsicherung, verbessern die Regelgüte durch geringe Regelabweichung und kontextgerechte Gewichtung der Zielgrößen und steigern die Effizienz durch geringe Rechenlast und echte Echtzeitfähigkeit selbst bei komplexen, nichtlinearen Modellen. Der Entwicklungsaufwand sinkt durch automatisierte, kontextbewusste Parametrierung und ein skalierbares Gewichtstuning, das die schnelle, reproduzierbare Übertragung auf unterschiedliche Fahrzeugklassen und ganze Flotten ermöglicht. Insgesamt entsteht eine belastbare Brücke zwischen verlässlicher Optimierung und adaptiver Intelligenz: Die Kombination aus reduzierter robuster NMPC, stochastischer MPC mit begrenzter Unsicherheitsfortpflanzung, adaptiver SNMPC mit vorausschauendem Lernen und sicherheitsgekoppelter Gewichtsadaption löst den Zielkonflikt zwischen Sicherheit, Performance und Echtzeitfähigkeit. Das Ergebnis ist ein praxisnahes, übertragbares Regelungssystem, das im Grenzbereich konsequent Nebenbedingungen wahrt, Rechenbudgets einhält und kontextbewusst die bestmögliche Leistung abruft. Der offene Quellcode erleichtert die Weiterführung und den Transfer in neue Plattformen und Anwendungsdomänen und legt die Basis für zunehmend autonome, sichere und effiziente Fahrzeugführung im realen Einsatz.

### 3.8.2 AP 8 – Vortrag und Poster der Abschlusspräsentation



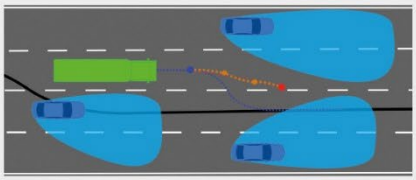
# FUNKTIONSENTWICKLUNG
## Übersicht

### MOTIVATION UND ZIELE

Zur Weiterentwicklung der autonomen Fahrfunktion werden algorithmische Erweiterungen im Bereich des Szenarienverständnisses, der Bewegungsplanung und der Trajektorienfolgeregelung umgesetzt. Ziel: Erweiterung der Funktionen hinsichtlich Betriebsbedingungen (Autobahn, alle Witterungsbedingungen) und Anforderungen für fahrerlosen Betrieb (Redundanzen, technische Aufsicht) sowie Erprobung im öffentlichen Raum.


### ARBEITSSCHWERPUNKTE

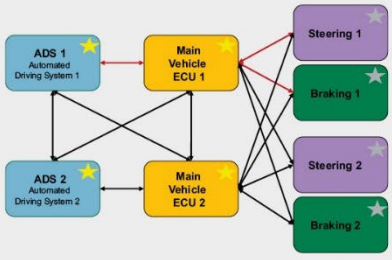
- Entwicklung eines umfassenden Verständnisses der Verkehrssituation
- Generierung einer Solltrajektorie im Bewegungsplaner inkl. Rückfallebene
- Eigenzustandsschätzung, Reibwertschätzung, Aktionspotentiale und Folgen von Ausfällen sowie Selbstüberwachung auf Fahrzeug- und Automatisierungssystemebene sowie hinsichtlich Systemgrenzen
- Kaskadenregelung aus Trajektorienfolgeregelung und Vehicle Control
- Umsetzung antriebsspezifischer Fahrzeugansteuerung
- Definition des Betriebsmodusmanagements



Bewegungsplanung mit Solltrajektorie und Notfalltrajektorie

### ERGEBNISSE

- Anpassung Szenarienverständnis und Bewegungsplanung für Autobahn-Anwendung, Fahrzeugintegration und erfolgreiche Erprobung innerhalb ODD Autobahn
- Implementierung einer Notfalltrajektorienplanung als Rückfallebene für die Bewegungsplanung, Fahrzeugintegration und Integration mit Offboard-Modulen zur Ausführung eines Minimum Risk Maneuvers (MRM)
- Implementierung eines Betriebsmodusmanagements für Dual-Mode L4-Fahrzeuge inkl. Redundanzmanagement und Minimum Risk Maneuver (MRM)
- Verwendung von Steer-by-Brake und redundanter Bremse bei Fehlern im Primärsystem
- Optimierung der Trajektorienfolgeregelung sowohl für den fehlerfreien Einsatz auf der Autobahn als auch für den Redundanzfall

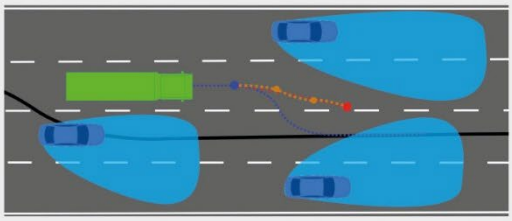



Redundantes Fahrzeugsystem mit verteiltem Betriebsmodusmanagement.

# AUTONOMES FAHREN AUF AUTOBAHNEN
## Funktionsentwicklung

### MOTIVATION UND ZIELSETZUNG

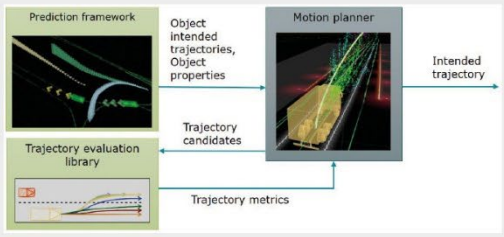
Das Fahren von LKW auf Autobahnen erfordert eine hochperformante autonome Fahrfunktion, da es sich um eine dynamische Umgebung mit hohen Geschwindigkeiten handelt. Der oft dichte Verkehr, komplexe Manöver wie das Einfädeln auf die Autobahn sowie unterschiedliche Wetterbedingungen stellen zusätzliche Herausforderungen dar. Ziel dieses Projektes war die Entwicklung der Module Szenarienverständnis und Bewegungsplanung, um einen autonomen LKW erfolgreich auf der Autobahn zu erproben.



Bewegungsplanung mit Solltrajektorie und Notfalltrajektorie

### METHODIK

- Abbildung von Interaktion in den Modulen Szenarienverständnis und Bewegungsplanung
- Erhöhte Robustheit und Sicherheit durch Generieren von Nominal- und zugehöriger Notfalltrajektorie
- Verbesserung der Fahrbarkeit von Trajektorien durch Rückführung von Beschleunigungspotentialen




Software-Architektur für interaktionsbewusste Bewegungsplanung

### ERGEBNISSE

Autonome Fahrfunktionen wurden erfolgreich auf Autobahnen getestet, einschließlich der Bewältigung von Cut-ins und interaktionsbehaftetem Verhalten bei Einscherern. Die resultierenden Fahrmanöver waren komfortabel und intuitiv. Eine erhöhte Robustheit wurde durch funktionale Redundanz und Fail-Safe-Planung sichergestellt.

Erprobung der Fahrfunktion innerhalb der Zielumgebung Autobahn

# ROBUSTE TRAJEKTORIEN-FOLGEREGELUNG FÜR LEVEL 4 AUTOMATISIERTES FAHREN

## Funktionsentwicklung

### MOTIVATION UND ZIELE

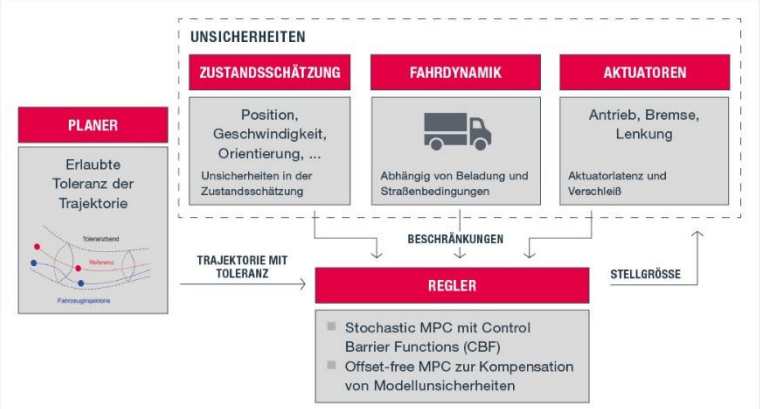
- **Level 4** automatisiertes Fahren: Es muss sichergestellt werden, dass die Fahrzeugtrajektorie innerhalb eines vorgegebenen Toleranzbandes um die Referenztrajektorie bleibt
- **Unsicherheiten** von Aktuatoren, Fahrzeugzustand oder der Umgebung erschweren einen „allgemein gültigen" Regleransatz
- **Steer-by-brake** als redundante Lenkung

Welche Unsicherheiten müssen für den Reglerentwurf modelliert werden?

### VORGEHEN UND LÖSUNGSANSATZ

- Modellierung von Unsicherheiten für den Reglerentwurf
- Stochastic Model Predictive Control (MPC) in Kombination mit Control Barrier Functions (CBF)
- Offset-free MPC Ansatz zur Schätzung und Kompensation von Abweichungen in der MPC-Modellierung

Entwicklung eines robusten Reglers für die Trajektorien-folgeregelung.




Verbesserung der Planer-Regler Interaktion durch Schätzung von Modellierungsfehlern.

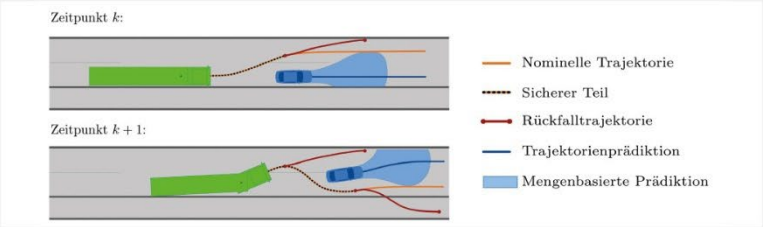
### AUSBLICK

Weiterentwicklung des automatisierten Fahrens vom derzeitigen Status quo hin zur Reife für einen kommerziellen, fahrerlosen Betrieb.

# MINIMUM RISK MANEUVERS: Wie Rückfalltrajektorien den Betrieb autonomer LKWs absichern

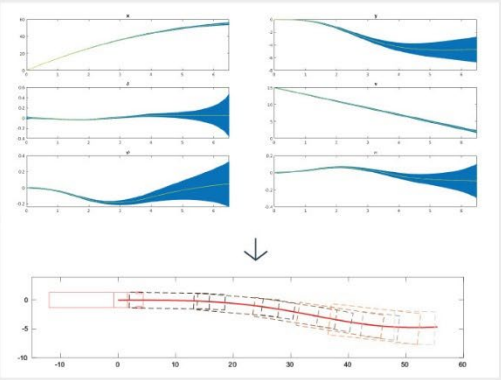
## Funktionsentwicklung

### ONLINE-VERIFIKATION VERHINDERT SELBSTVERSCHULDETE KOLLISIONEN

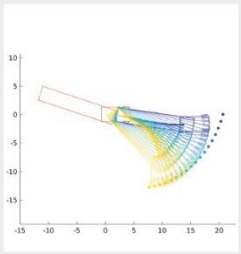



**Wir können Abweichungen von der geplanten Rückfalltrajektorie durch Nutzung von Erreichbarkeitsanalyse kompensieren.**

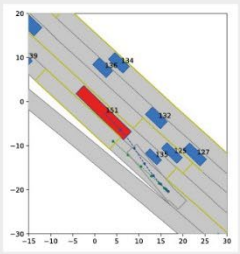
Messunsicherheiten und Modellungenauigkeiten führen zu Abweichungen von der geplanten Rückfalltrajektorie:



*Problem:* Erreichbarkeitsanalyse ist **nicht echtzeitfähig**.
*Lösung:* Durch die Verwendung vordefinierter **Bewegungsprimitive** für die Planung der Rückfalltrajektorie kann die **Erreichbarkeitsanalyse offline** durchgeführt werden.

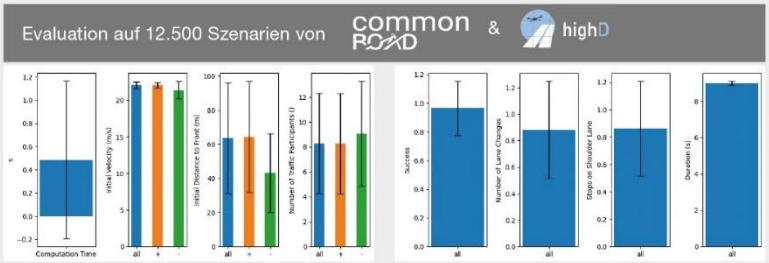


Offline: Generierung von Bewegungsprimitiven mit Erreichbarkeitsmengen



Online: Interaktive Planung mit den Primitiven gegen die mengenbasierte Prädiktion der anderen Fahrzeuge

### ERGEBNISSE




Planungszeit, Anfangsgeschwindigkeit, initialer Abstand zum vorausfahrenden Fahrzeug, und Anzahl der Verkehrsteilnehmer für die evaluierten Szenarien, unterteilt nach Planungserfolg

Erfolgsrate, Anzahl der Spurwechsel, Anteil der Stops auf dem Seitenstreifen, und Dauer für die geplanten Rückfalltrajektorien

# REIBWERTSCHÄTZUNG
## Funktionsentwicklung

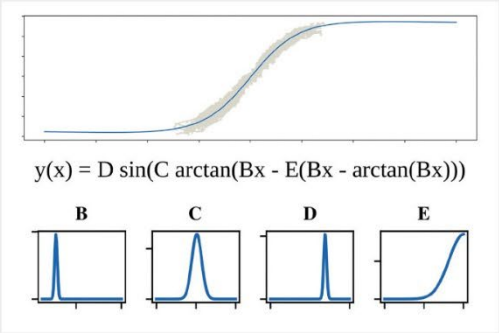
### MOTIVATION UND ZIELE

Eine sichere autonome Fahrzeugführung bedarf der Kenntnis über die fahrdynamischen Stabilitätsgrenzen. Ein wesentlicher Einfluss ist dabei der Reifen-Fahrbahn-Kontakt. Im Rahmen von ATLAS-L4 wurden daher verschiedene Ansätze zur Schätzung des aktuellen und des zukünftigen Reifenpotentials untersucht.

Kamera-basierte Fahrbahnzustandserkennung

### ARBEITSSCHWERPUNKTE

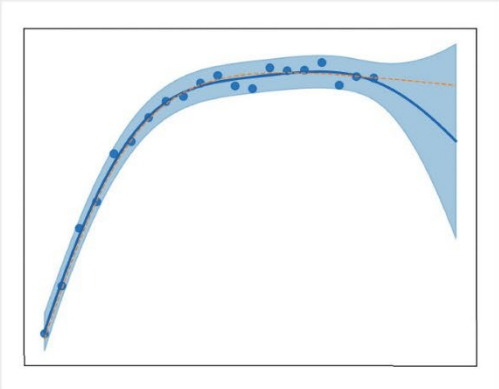
- Prädiktive Fahrbahnzustandsschätzung
- Quantifizierung von Parameterunsicherheiten
- Entwicklung eines statistischen Reifenmodells




Modellparametrierung und Unsicherheitsquantifizierung

### ERGEBNISSE

- Ursachenbasierte Reibwertschätzung
  - Klassifizierung Nass / Trocken
  - Unterscheidung Untergrundklassen
  - Wassertiefenschätzung
- Quantifizierung von Parameterunsicherheiten
  - Sensitivitätsanalyse
  - Stochastical Variational Inference
  - Open-Source Parametrierungstool
- Statistische Reifenmodellierung
  - Gauss-Prozess-Reifenmodell
  - Integration in 3D-Fahrzeugzustandsschätzung



Statistische Reifenmodellierung

# Fusion von DRL und MPC für adaptive, stochastische und robuste nichtlineare Trajektorienfolgeregelung autonomer Fahrzeuge

## Funktionsentwicklung

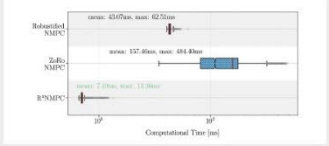
✓ Schnelle robuste und stochastische NMPCs
✓ Selbstadaptive Unsicherheitsparameter für verschiedene Umgebungen
✓ Sicheres DRL-gesteuertes, gewichtsvariables Kostenfunktionsdesign

GitHub


### ROBUSTE UND STOCHASTISCHE NMPCs

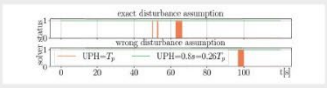
Reduced Robustified NMPC (R²NMPC)

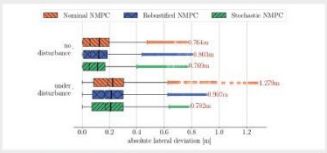
$$\min_{\boldsymbol{x}(\cdot),\boldsymbol{u}(\cdot)} \int_{\tau=0}^{T_p} l(\boldsymbol{x}(\tau),\boldsymbol{u}(\tau))d\tau + m(\boldsymbol{x}(T_p))$$
$$\text{s. t.} \quad \boldsymbol{x}(0) = \boldsymbol{x}_0,$$
$$\dot{\boldsymbol{x}}(t) = f(\boldsymbol{x}(t),\boldsymbol{u}(t),\boldsymbol{O}_{m_s}), \qquad t \in [0,T_p),$$
$$\boldsymbol{h}(\boldsymbol{x}(t),\boldsymbol{u}(t)) + \boldsymbol{h}_{\text{back}}(\boldsymbol{x}(t),\boldsymbol{u}(t),\boldsymbol{\Sigma}(t)) \leq \bar{\boldsymbol{h}}, \qquad t \in [0,T_p),$$
$$\boldsymbol{h}^e(\boldsymbol{x}(T_p)) + \boldsymbol{h}_{\text{back}}^e(\boldsymbol{x}(T_p),\boldsymbol{\Sigma}(T_p)) \leq \bar{\boldsymbol{h}}^e$$




Stochastic NMPC (SNMPC) with Polynomial Chaos Expansion

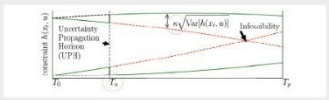
$$\min_{\substack{\boldsymbol{x}(\cdot),\\ \boldsymbol{u}(\cdot)}} \int_{\tau=0}^{T_p} l(\mathbb{E}[\boldsymbol{x}(\tau)],\boldsymbol{u}(\tau))d\tau + m(\mathbb{E}[\boldsymbol{x}(T_p)])$$
$$\text{s. t.} \quad \boldsymbol{x}(0) = \boldsymbol{x}_0,$$
$$\dot{\boldsymbol{x}}(t) = f(\mathbb{E}[\boldsymbol{x}(t)],\boldsymbol{u}(t)), \qquad t \in [0,T_p),$$
—transformed chance constraints
$$\mathbb{E}[h(\boldsymbol{x},\boldsymbol{u})] + \kappa\sqrt{\text{Var}[h(\boldsymbol{x},\boldsymbol{u})]} \leq \bar{h}, \qquad t \in [0,T_p),$$
$$\mathbb{E}[h^e(\boldsymbol{x}(T_p))] + \kappa\sqrt{\text{Var}[h^e(\boldsymbol{x}(T_p))]} \leq \bar{h}^e,$$
—hard nonlinear constraints
$$g(\mathbb{E}[\boldsymbol{x}(t)],\boldsymbol{u}(t)) \leq \bar{\boldsymbol{g}}, \qquad t \in [0,T_p),$$
$$g^e(\mathbb{E}[\boldsymbol{x}(T_p)]) \leq \bar{\boldsymbol{g}}^e,$$
—hard linear constraints
$$J_{\text{bx}}\mathbb{E}[\boldsymbol{x}(t)] \leq \bar{\boldsymbol{x}}, \qquad t \in [0,T_p),$$
$$J_{\text{bx}}^e\mathbb{E}[\boldsymbol{x}(T_p)] \leq \bar{\boldsymbol{x}}^e$$
$$J_{\text{bu}}\boldsymbol{u}(t) \leq \bar{\boldsymbol{u}}, \qquad t \in [0,T_p),$$



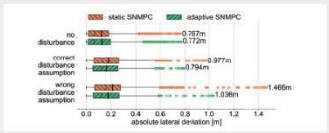




| Berechnungszeiten (Intel i7-11850H 2.5 GHz) | | |
|---|---|---|
| NMPC | 953 | 465 |
| SNMPC | 172 | 97 |
| R²NMPC | 144 | 82 |

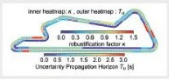
### DEEP REINFORCEMENT LEARNING – SNMPC

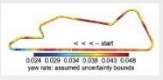


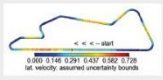

Geschlossene Regelungsleistung auf der Monte-blanco-Rennstrecke mit Referenzgeschwindigkeiten von bis zu 37,5 m/s (Vergleich: statisches vs. adaptives SNMPC)

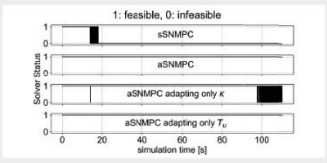


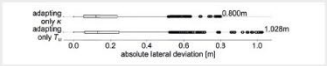

Optimale Entscheidungen des DRL-Agenten zur Anpassung verschiedener stochastischer/robustifizierter NMPC-Parameter
(z. B. *k – Robustifizierungsfaktor der Nebenbedingungen , T_u – Unsicherheitspropagationshorizont und Annahmen über Standardabweichungen der Unsicherheit)*



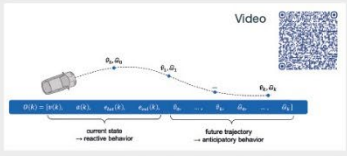



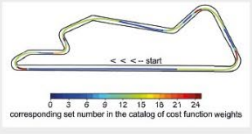



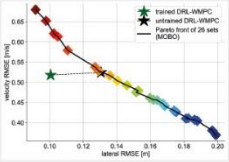

→ Anpassung der **UPH-Länge** verbessert die **Realisierbarkeit**
→ Anpassung des **Robustifizierungsfaktors** verbessert die geschlossene **Regelungsleistung**

### VORAUSSCHAUENDES SICHERES RL – GEWICHTSVARIABLES MPC


Sicherer RL-Aktionsraum
→ Auswahl eines Satzes von Kostenfunktionsgewichten aus einer **Pareto-Front mit 26 Sets,** die mit **Multi-Objective Bayesian Optimization (MOBO)** bestimmt wurden.




### REAL-WORLD EXPERIMENTS

Echtzeit-DRL passt 5 Unsicherheitsparameter eines SNMPC für die kombinierte Längs- und Querregelung an einem realen Passagierfahrzeug an.

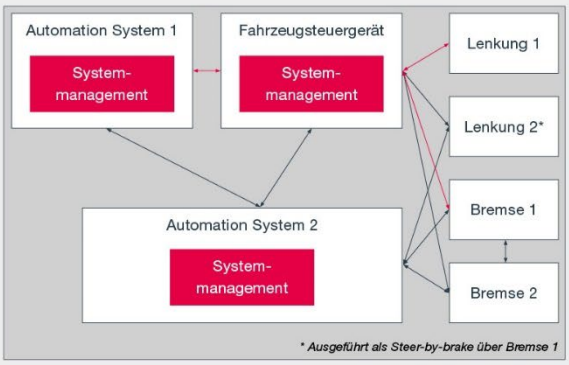

Video

# REDUNDANZ & SYSTEM MANAGEMENT

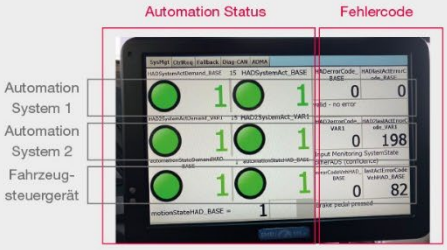
## Ausführung eines Minimum Risk Manövers nach Komponentenverlust

### DEMONSTRATIONSINHALTE

- Simulation des Ausfalls einer oder mehrerer Redundanz-Komponenten während der autonomen Fahrt mithilfe von Trennschaltern
- Selbständige Überführung des Fahrzeugs in einen sicheren Zustand:
  - Einschalten des Warnblinkers
  - Durchführen eines Minimum Risk Manövers: Spurwechsel und Bremsen in den Stillstand
  - Einlegen der Parkbremse
- Darstellung eines verteiltem System Managements zur Überwachung der Fahrzeugsysteme und Bestimmung eines konsistenten Systemzustandes




Fahrzeugarchitektur des Versuchsträgers




Visualisierung der Zustände und Diagnosen des System Managements


Trennschalter für Redundanz-Komponenten

### BESCHREIBUNG DES VERSUCHSTRÄGERS

- TGX 18.510 4x2 LL, 375 kW / 510 PS
- Integration L4-fähiger Aktuatoren
  - Redundante Bremse mit Steer-by-Brake Fähigkeit (Knorr-Bremse)
  - Lenksystem mit neuem autonomem Modus (Bosch)
- Einbau einer Echtzeitkinematik für hochgenaue GPS-Positionierung
- Keine Verwendung von weiterer Sensorik für autonomes Fahren


Autonomous-Ready Base Vehicle (ARB-Fahrzeug)

# AP 9
# Control Center und Teleoperation

Lavinia Stollfuß, MAN Truck & Bus SE

## 3.9 AP 9: Control Center und Teleoperation

*Arbeitspaketleitung: Lavinia Stollfuß, MAN Truck & Bus SE*

Das Arbeitspaket 9 Control Center und Teleoperation widmete sich der Entwicklung und Umsetzung eines zentralen Leitstands zur Überwachung und Steuerung hochautomatisierter Fahrzeuge und Fahrzeugflotten. Ziel war es, einer technischen Aufsicht zu ermöglichen, die Fahrzeuge zu überwachen (Remote Monitoring), in komplexen Situationen zu unterstützen (Remote Assistance) oder bei Bedarf vollständig per Teleoperation fernzusteuern (Remote Driving). Dabei wurden sicherheitsrelevante Funktionen wie der Not-Halt sowie die Interaktion mit Autonomiemodulen berücksichtigt. Hierfür wurden alle relevanten Fahrzeugdaten erfasst, visualisiert und auf einer multimonitorfähigen Control Center Benutzeroberfläche bereitgestellt.

Ein weiterer Schwerpunkt lag auf der Analyse technischer und rechtlicher Anforderungen, insbesondere im Hinblick auf Mensch-Maschine-Interaktion, Sicherheitsaspekte und gesetzliche Rahmenbedingungen für Teleoperation. Die Konzeption des Control Centers umfasste neben dem Leitstand auch den Teleoperator-Arbeitsplatz, inklusive HMI- und Schulungskonzepten sowie der Interaktion mit Fahrzeugen und Infrastruktur.

Besonders sicherheitskritisch war die Betrachtung von Bildqualität und Latenz, deren Auswirkungen auf das Situationsbewusstsein und die Leistungsfähigkeit des Operators systematisch untersucht wurden. Hierbei wurden geeignete Bewertungsmetriken entwickelt und in einer Probandenstudie validiert, um die Sicherheit der Teleoperation unter realistischen Bedingungen messbar zu machen. Zudem wurde ein in die Simulation eingebundener Teleoperatorplatz aufgebaut, der zum einen als Untersuchungswerkzeug dient, um teleoperationsspezifische Effekte (z. B. Auswirkung unterschiedlicher Latenzen) zu untersuchen und zum anderen geeignet ist, (noch) nicht in Realität darstellbare Use Cases zu demonstrieren.

Ergänzend wurde das bereits in Kapitel 3.1 beschriebene digitale Managementsystem BEA (Betriebsbereichs- und Ereignismanagement auf Autobahnen) zur dynamischen Verwaltung von Betriebsbereichen entwickelt, welches infrastrukturseitige Informationen in den Entscheidungsprozess integriert und über eine Schnittstelle zum Control Center verfügt. Während im Kapitel 3.1 insbesondere auf die Funktion der Betriebsbereichsgenehmigung eingegangen wurde, liegt der Fokus bei BEA in diesem Kapitel auf der Verwaltung der Betriebsbereiche und der Interaktion mit dem Control Center.

Die Ergebnisse flossen in die Konzeption, technische Umsetzung und Erprobung eines prototypischen Control Centers ein, das die sichere Überwachung und Fernsteuerung automatisierter Fahrzeuge im Use Case „Autobahn“ ermöglicht.

Im Folgenden wird beschrieben, welche Ergebnisse speziell in den einzelnen Arbeitsschwerpunkten in gemeinsamer Zusammenarbeit von den Partnern erarbeitet wurden.

### 3.9.1 Anforderungsanalyse für das Control Center (AP 9.1)

Im Rahmen des Projekts ATLAS-L4 haben die beteiligten Partner gemeinsam einen umfassenden Anforderungskatalog für ein Control Center zur technischen Aufsicht und Teleoperation hochautomatisierter Fahrzeuge erarbeitet. Ausgangspunkt war eine detaillierte Analyse des Stands der Technik, ergänzt durch Erkenntnisse aus der Praxis – unter anderem durch die Besichtigung der Verkehrszentrale der Autobahn GmbH in Frankfurt am Main. Dabei wurden Arbeitsabläufe, technische Ausstattung und Human-Factors-Aspekte untersucht, um Anforderungen an zukünftige Leitstände realitätsnah abzuleiten.

Die Projektpartner haben technische, rechtliche und prozessuale Anforderungen systematisch zusammengetragen. Dazu zählen unter anderem die gesetzlichen Vorgaben zur technischen Aufsicht gemäß StVG sowie europäische Regelungen zur Fernsteuerung automatisierter Fahrzeuge. Auf dieser Basis wurden Anforderungen an die Mensch-Maschine-Schnittstelle, die Systemarchitektur, die Kommunikation mit Infrastruktur und Einsatzkräften sowie die Sicherheit und Datenschutzkonformität des Systems definiert. Die Prozesse von BEA basieren ebenfalls auf den Regelungen des StVG sowie der AFGBV. So ist es einer für den Betriebsbereich zuständigen Behörde beispielsweise möglich bei Genehmigungserteilung einschränkende Nebenbestimmungen zu definieren (§9 AFGBV) oder die Betriebsbereichsgenehmigung temporär ruhen zu lassen (§10 AGBV).

Ein zentrales Element der Anforderungsdefinition war die Gestaltung eines sicheren und intuitiven Teleoperator-Arbeitsplatzes, der eine zuverlässige Steuerung des Fahrzeugs auch in komplexen Situationen ermöglicht. Um die Anforderungen praxisnah zu erheben, wurde ein strukturierter Fragebogen entwickelt, der mit den Partnern im Arbeitspaket 9 abgestimmt und durch diese ausgefüllt wurde. Im Rahmen eines Workshops am WIVW wurden die Ergebnisse gemeinsam diskutiert und daraus die HMI- und Human-Factors-Anforderungen für den Teleoperatorarbeitsplatz abgeleitet. Die Anforderungen umfassen unter anderem die visuelle Darstellung sicherheitsrelevanter Fahrzeugdaten, die Kommunikation mit dem Fahrzeug und die Möglichkeit zur Auslösung von Notfallmanövern. Technische Vorgaben zur Datenübertragung, Latenzregelung, Redundanz und IT-Sicherheit wurden ebenfalls spezifiziert.

Als Ergebnis liegt eine Anforderungssammlung vor, die getrennt nach drei Use Cases (Remote Driving ≤ 20 km/h, Remote Driving ≤ 80 km/h, Remote Assistance) die Merkmale Sichtdarstellung, Geräuschdarstellung, Fahrstand, grafische Benutzeroberfläche, dargestellte Informationen zu Fahrzeug und Fahrt, Transitionen (z. B. Übernahmeaufforderung), Überwachung (z. B. Datenaufzeichnung) und Kommunikationsverbindung.

Ein beispielhafter Auszug aus der Ergebniszusammenfassung ist in Abbildung 63 dargestellt.

| Sichtdarstellung | RD ≤20 km/h | RD ≤80 km/h | RA |
|---|---|---|---|
| Bildauflösung pro Frontsichtkanal | MAN: 500x1000 Pixel<br>TU<br>W<br>Finding: Spezifikation wenig sinnvoll; andere Qualitätsmaße (Videoparameter, Größe des Sichtbereichs) entscheidend; zudem stark latenzabhängig | MAN: 500x1000 Pixel | MAN: 500x1000 Pixel |
| Horizontaler Sichtbereich Außenspiegel | 60° (Begründung aus minimalen Anforderungen an Fahren im Realfahrzeug) | | |
| Virtuelle Perspektive für Steuerung | Fahrersitz ODER mittig hinter Fahrzeug | Fahrersitz ODER mittig hinter Fahrzeug | Fahrersitz ODER mittig hinter Fahrzeug<br>Feature: Möglichkeit zum Wechsel zwischen Fahrersicht und mittiger Anzeige |
| Einstellbarkeit der Perspektive | Nein | | |
| Weitere Sichthilfen | Vogelsicht, Egofahrzeugprädiktion | | Vogelsicht, Egofahrzeugprädiktion<br><br>Replayfunktion: Möglichkeit zum Replay der vorangehenden Fahrsituation bei Request an TO |
| Visualisierung weiterer relevanter Größen in der Fahrszenerie | Egotrajektorie mit geschwindigkeitsabhängiger Längendarstellung<br><br>Mindestabstand/Bremsweg | Egotrajektorie mit geschwindigkeitsabhängiger Längendarstellung<br><br>Mindestabstand/Bremsweg<br><br>Tatsächlicher Abstand zu und Geschwindigkeit des Vorderfahrzeugs | Egotrajektorie mit geschwindigkeitsabhängiger Längendarstellung<br><br>Mindestabstand/Bremsweg |

Abbildung 63 Auszug aus Workshopergebnissen: Sichtdarstellung.

Darüber hinaus wurden konkrete Use Cases für die technische Aufsicht und Teleoperation entwickelt, die den praktischen Betrieb des Control Centers abbilden. Diese reichen von der Echtzeitüberwachung von Fahrzeugen und Missionen über die Auslösung und Analyse von Notfallmanövern bis hin zur Routenplanung und Geofencing.

Abschließend wurden Anforderungen an das Remote-Assistance Konzept Perception Modification definiert. Im Fokus des Konzeptes steht die Modifikation von Objekten, um Fehler in der Objekterkennung (z. B. False-Positives, Falsche Objektklassen oder Bewegungsprädiktionen) zu adressieren. Zur Erfüllung dieser Aufgabe wurden Anforderungen an die Gestaltung des Human-Machine-Interfaces (HMI) abgeleitet. Darin inbegriffen sind Anforderungen an die Visualisierung von Umfeldmodell- und Sensordaten, des Remote-Assistance Arbeitsplatzes und Interaktionsmöglichkeiten der Teleoperatoren.

Die Erkenntnisse aus der gemeinsamen Arbeit bildeten die Grundlage für die technische Umsetzung und Validierung des Control Centers im weiteren Projektverlauf.

### 3.9.2 Konzeption des Control Centers (AP 9.2)

Die Anforderungsanalyse zeigte, dass aufgrund der divergierenden Anforderungen der Primäraufgaben des Control Centers an die Arbeitsplatzgestaltung und die Bediener die Funktionalitäten des Control Centers nicht an einem einzelnen Arbeitsplatz umgesetzt werden können. Stattdessen erfordern sie räumlich gebündelte, jedoch funktional klar getrennte Arbeitsplätze. Die Notwendigkeit der Trennung ergibt sich zusätzlich aus der Tatsache, dass das Monitoring der Flotte kontinuierlich erfolgen muss und nicht durch das Steuern oder Unterstützen einzelner Fahrzeuge unterbrochen werden kann. Daher werden Unterstützungsanforderungen einzelner Fahrzeuge vom Remote Monitoring an die funktionell getrennten Arbeitsplätze für Remote Driving und Remote Assistance weitergeleitet.

Aus der Aufgabe des Remote Monitoring, die Gesamtflotte kontinuierlich zu überwachen, ergibt sich die Anforderung, dass die Flotteninformationen in ihrer Gesamtheit möglichst übersichtlich dargestellt werden, um die Identifikation möglicher Probleme zu ermöglichen. Daher ist der von MAN entwickelte Remote Monitoring Arbeitsplatz so konzipiert, dass die gesamte Flotte stets übersichtlich dargestellt wird, während gleichzeitig Detailinformationen zu den einzelnen Fahrzeugen abgerufen werden können.

Im Gegensatz zum Remote Monitoring, bei dem der Gesamtüberblick über die Gesamtflotte im Fokus steht, erfolgt die Interaktion beim Remote Driving und der Remote Assistance gezielt mit einem Fahrzeug. Dadurch rückt die latenzarme Darstellung fahrzeugspezifischer Sensor-, Automations- und Steuerungsdaten sowie die zuverlässige Eingabe von Kontrollsignalen in den Fokus der Arbeitsplatzgestaltung.

Für die Ausführung der Fahraufgabe beim Remote Driving sind spezielle Eingabegeräte wie Lenkrad und Pedalerie sowie ein Bedienfeld mit Tasten zur Steuerung sekundärer Funktionen erforderlich. Dahingegen genügen für die Remote Assistance klassische Eingabemodalitäten wie Maus und Tastatur. Aus diesem Grund ist der Remote Driving Arbeitsplatz von Fernride als ergonomisch optimierter Fahrstand konzipiert, wohingegen der Remote Assistance Arbeitsplatz der TU München als Schreibtischarbeitsplatz ausgestaltet ist.

Für das Remote Driving ist die benutzerzentrierte Gestaltung von Teleoperationsarbeitsplätzen von zentraler Bedeutung. Um teleoperationsspezifische Effekte wie Latenz gezielt untersuchen und Human-Factors-Fragestellungen (z. B. zu Workload, Situationsbewusstsein oder Fahrperformance) empirisch bearbeiten zu können, wird ein flexibles und modular aufgebautes Simulationswerkzeug benötigt, das zudem Schulungsmöglichkeiten für zukünftige Teleoperatoren bietet. Auf Basis der in AP 9.1 erarbeiteten und mit den Arbeitspaketpartnern abgestimmten Anforderungen wurde am WIVW ein entsprechender Teleoperationssimulator entwickelt. Dieser erlaubt vielfältige Variationen der Komponenten und eignet sich sowohl zur Evaluation unterschiedlicher HMI-Konzepte und Setups als auch als Demonstrator spezifischer Use Cases.

Im Rahmen des AP 9.2 wurde ebenfalls ein umfassendes Schulungskonzept für die Rollen im Control Center entwickelt, das die sichere Fernüberwachung und -steuerung automatisierter Fahrzeugflotten ermöglicht. Das Konzept gliedert sich in die drei Hauptbereiche: Remote Monitoring, Remote Assistance und Remote Driving. Für jede dieser Rollen wurden spezifische Anforderungen, Aufgabenprofile und Trainingsinhalte definiert.

Im Bereich Remote Monitoring liegt der Fokus auf der technischen Aufsicht, die für die Überwachung der Fahrzeugflotte, die Freigabe von Fahrten und das Eingreifen bei Störungen verantwortlich ist. Die Schulung umfasst die Bedienung des multimonitorfähigen Control Centers, die Interpretation von Fahrzeug- und Systemdaten sowie die Durchführung von Maßnahmen wie dem Auslösen eines Minimal Risk Manövers (MRM) und der Koordination mit externen Partnern.

Für die Rolle des Remote Assistant wurde ein Schulungskonzept zum Perception Modification System entwickelt. Es basiert auf gesetzlichen Anforderungen, Auswahlkriterien und einem strukturierten Ablauf aus Theorie, Praxis und regelmäßiger Wiederholung. Die Inhalte reichen von Human-Factors-Herausforderungen über Systemgrenzen bis hin zu konkreten Szenarien und Bewertungsmetriken, die objektiv die Sicherheit und Effizienz der Assistenzmaßnahmen erfassen.

Im Bereich Remote Driving wurde ein simulationsgestütztes Trainingskonzept erarbeitet, das die besonderen Herausforderungen der Teleoperation adressiert. Dazu zählen Latenz, Bildqualität, fehlende physische Präsenz und die Notwendigkeit eines schnellen Situationsbewusstseins.

Um die Einsatzmöglichkeiten von Fahrsimulationen im Training von Teleoperatoren für das Remote Driving aufzuzeigen, wurden am WIVW entsprechende Use Cases mit Fokus auf den im Projekt adressierten Anwendungsfall für Teleoperation identifiziert.

Die Identifikation relevanter Szenarien bzw. Trainings-Use-Cases fußte dabei auf zwei Säulen: Zum einen wurden anhand einer Analyse des Fahraufgabenkatalogs für die relevanten Fahrerlaubnisklassen einzelne Fahraufgaben und damit auf granularer Ebene Fahrmanöver identifiziert, die für den angedachten Anwendungsfall (Remote Driving im Last-Mile-Transport) von Bedeutung sind. Es handelt sich um Manöver, die unter den speziellen Anforderungen des Remote Driving (z. B. Fahren unter Latenz, Jitter oder verminderter Bildqualität) hinsichtlich Workload, Situation Awareness und Fahrperformanz potenziell als besonders kritisch zu bewerten sind. Zum anderen wurden exemplarisch Use Cases abgeleitet, die im Zusammenhang mit der Automation stehen und ggf. über den derzeit angedachten Einsatzbereich im Rahmen des Projekts hinausgehen. Ein Beispiel dafür könnte die Wiedereingliederung des Fahrzeugs in den fließenden Verkehr und die Übergabe an die Automation nach Auslösung eines Minimal Risks Manövers sein.

Tabelle 4 Auszug aus den identifizierten simulationsbasiert trainierbaren Fahraufgaben.

| # | Grundfahraufgabe | Relevanz für den Last-Mile-Transport | Notwendigkeit von Training unter Teleoperationsbedingungen |
|---|---|---|---|
| 1 | Fahren nach rechts rückwärts | Rangieren erforderlich (z.B. nach Abbiegen in falsche Richtung) | Potenziell negative Effekte durch Latenz auf Querführung aufgrund großer notwendiger Lenkeingaben |
| 5 | Befahren von Einfädelungsstreifen | Auffahren auf Autobahn mit anschließender Übergabe an Automation | Einschätzung von Ego- und Geschwindigkeit anderer Verkehrsteilnehmer sowie Abständen zwischen Verkehrsteilnehmern durch Latenz und ggf. verminderte Bildqualität potenziell erschwert |
| 13 | Haltestellen, Fußgängerüberwege | Auftreten im Rahmen von Last-Mile-Transport | Verspätete Wahrnehmung von vulnerablen Verkehrsteilnehmern (z.B. von Bus verdeckte Fußgänger) aufgrund latenzbedingter Verzögerungen in der visuellen Darstellung besonders kritisch |

Insgesamt zeigt das Schulungskonzept, dass eine gezielte, praxisnahe und wiederkehrende Qualifizierung der beteiligten Personen essenziell ist, um die Sicherheit und Effizienz im Betrieb automatisierter Fahrzeugflotten zu gewährleisten. Die Kombination aus theoretischer Wissensvermittlung, praktischer Übung und simulationsgestütztem Training bildet eine robuste Grundlage für den Einsatz von Teleoperatoren und technischen Aufsichten im realen Betrieb.

Darüber hinaus wurde im Zuge dieses Arbeitspaketes auf Basis der in AP 9.1 definierten Anforderungen und dem aktuellen Stand der Wissenschaft ein Konzept für die Perception Modification entwickelt. Die Interaktion mit dem Umfeldmodell gliedert sich in die Phasen

„Scenario Analysis“, „Modification Planning“ und „Modification Active“. Die Phase „Scenario Analysis“ steht am Anfang der Interaktion zwischen Teleoperator und dem Automated Driving System (ADS) und wird durch eine Unterstützungsanfrage seitens des ADS initiiert, sobald es zu einem Disengagement kommt, das das Fahrzeug zur Ausführung eines Minimal Risk Manövers (MRM) zwingt. Während dieser Phase werden Rohsensordaten (z. B. Videos und LiDAR-Punktewolken) sowie Automationsdaten (z. B. Objektlisten, geplante Trajektorien und Statusinformationen) vom Fahrzeug an den Remote Assistance Arbeitsplatz übertragen. Die Aufgabe des Teleoperators in dieser Phase ist die Identifikation von möglichen Diskrepanzen zwischen dem aktuellen Umgebungsmodell und der realen Umgebung, die das Disengagement verursacht haben könnten. Sofern eine Diskrepanz festgestellt wird, fährt der Teleoperator mit der Phase „Modification Planning“ fort, in der mithilfe der verfügbaren Modifikationsmodi (z. B. Modifikation von Objekten) Anpassungen am Umgebungsmodell vorgenommen werden. Das Fahrzeug liefert kontinuierlich Feedback an den Teleoperator, indem es Trajektorien auf Basis des modifizierten Umfeldmodells plant. Hat der Teleoperator eine passende Lösung identifiziert, wird die Phase „Modification Active“ eingeleitet. Das Fahrzeug führt die geplanten Trajektorien basierend auf dem modifizierten Umfeldmodell aus. Die Gültigkeit der Modifikationen wird vom Teleoperator kontinuierlich überwacht, um bei Bedarf einzugreifen. Nach erfolgreicher Bewältigung des Szenarios werden die Modifikationen durch den Teleoperator deaktiviert und die Verbindung zum Fahrzeug wird beendet.

Das HMI für die Perception Modification hat zwei zentrale Aufgaben: die Visualisierung von Rohsensor- und Automationsdaten sowie die Eingabe von Modifikationen. Die Anzeige gliedert sich in ein zentrales Fenster zur Darstellung eines dreidimensionalen Umgebungsmodells, mehrere Fenster für Videostreams und weitere Fenster zur allgemeinen Bedienung des Teleoperationssystems (z. B. Verbindungsaufbau, Fahrzeugauswahl und Statusanzeigen). Die Modifikationen werden direkt im Umgebungsmodell mittels Maus, Tastatur und GUI-Elementen vorgenommen. Der Remote-Assistance-Arbeitsplatz ist als gewöhnlicher Büroarbeitsplatz konzipiert und besteht aus einem großen zentralen Bildschirm (55″), mehreren seitlich angeordneten kleineren Bildschirmen (27″), sowie Maus und Tastatur.

Außerdem wurde die Modifikation von Objekten untersucht, wozu notwendige Schnittstellen für die Open-Source Automation Autoware konzipiert wurden. Neben einer Schnittstelle zur Objektliste, die eine Modifikation der darin enthaltenen Objekte und deren Eigenschaften ermöglicht, umfasst das Integrationskonzept auch Schnittstellen zu Trajektorien und zum Setzen des Automationsmodus.

Bei der Konzeption von BEA wurden zunächst die Ziele bei der Verwaltung von Betriebsbereichen definiert. Anschließend wurden die dafür notwendigen Ein- und Ausgänge definiert und dann die Abläufe innerhalb von BEA entwickelt. Als Infrastrukturbetreiberin hat die Autobahn GmbH eine Verkehrssicherungspflicht für die Straßen in ihrem Verantwortungsbereich. Das übergeordnete Ziel von BEA ist es, die Verkehrssicherungspflicht auch beim zukünftigen Serienbetrieb von autonomen Fahrzeugen zu gewährleisten und das autonome Fahren zudem in das Verkehrsmanagement zu integrieren. Mit diesen Grundannahmen konnte das Konzept entwickelt werden. BEA ist mit dem Control Center vernetzt und ermöglicht es, das autonome Fahren zu monitoren und bei dynamischen Ereignissen – z. B. Arbeitsstellen – Anordnungen zu Fahrteinschränkungen für autonome Fahrzeuge zu übermitteln. Dadurch können zukünftig Informationen über autonome Fahrzeuge in das Verkehrsmanagement miteinfließen und durch die Möglichkeit bei besonderen Ereignissen Fahrteinschränkungen anzuordnen, kann der Verkehrssicherungspflicht Rechnung getragen werden. Die aktuellen dynamischen

Ereignisse werden von AutobahnOS, dem Betriebssystem für die Verkehrszentralen der Autobahn GmbH bezogen.

### 3.9.3 Technische Umsetzung des Control Centers (AP 9.3)

In der technischen Umsetzung des Control Centers im AP 9.3 wurden zunächst sämtliche Schnittstellen zwischen Fahrzeug, Control Center und BEA identifiziert, spezifiziert, implementiert und integriert. Weiterhin wurden für das Control Center die Funktionen des Leitstandes, inklusive des Systems zur Streckenverwaltung und der Teleoperation, sowie deren Kommunikation mit der Infrastruktur implementiert. Speziell wurde im Rahmen dieses Arbeitspakets das Control Center als multimonitorfähige Browserapplikation bereitgestellt, das zentrale Funktionen für die Fernüberwachung (Monitoring), Fernunterstützung (Assisting) sowie die Missionsabwicklung (Mission Handling) integriert. Ergänzend dazu wurde das System BEA zur dynamischen Streckenverwaltung entwickelt und über eine Schnittstelle direkt mit dem Control Center verbunden. Über diese Schnittstelle sendet das Control Center Informationen autonomer Fahrzeuge auf der Strecke an BEA, umgekehrt übermittelt BEA Anordnungen zu Fahrteinschränkungen an das Control Center.

Darüber hinaus erfolgte die technische Kopplung des Control Centers mit dem Automatisierungssystem, wodurch eine durchgängige und koordinierte Steuerung ermöglicht wurde. Die Funktionalität des integrierten Systems wurde im Anschluss umfassend prototypisch mit einem Fahrzeug erprobt und die Funktionsfähigkeit in der erforderlichen Qualität im definierten Use Case „Autobahn“ nachgewiesen.

Für die direkte Kommunikation zwischen dem Teleoperator und dem Fahrzeug über den Teleoperations-Arbeitsplatz ist eine spezielle Fahrzeugausstattung erforderlich. Dazu stellte der Hauptpartner MAN ein Fahrzeug (Teleoperationsfahrzeug) mit einem Drive-by-Wire-System (DBW) und einem Autobox-Modul zur Verfügung. Fernride übernahm die Entwicklung einer Teleoperation Station inklusive Hardwareauswahl und Softwareentwicklung für die Kommunikation innerhalb der Station sowie mit dem Fahrzeug. Zusätzlich wurde die Architektur und der Hardware-Stack für die Fahrzeugausstattung konzipiert und die Software zur Integration des eigenen Stacks mit dem MAN-System entwickelt. Die technische Umsetzung des Control Centers umfasste die Programmierung, Softwareintegration, Schnittstellenentwicklung zwischen Fahrzeug und Control Center sowie Integrationstests, Softwarequalifikation und Release-Freigabe.

Zur Umsetzung des in AP 9.2 definierten Perception Modification Konzepts wurde die am Lehr-stuhl für Fahrzeugtechnik der TU München entwickelte Teleoperationssoftware weiterentwickelt. Die Architektur der Software wurde überarbeitet, um die Integration von Remote Assistance Konzepten, die Anbindung an verschiedene ADS und die Entwicklung konzeptspezifischer HMIs zu ermöglichen. Die TUM Teleoperationssoftware [14] wurde auf dem IEEE Intelligent Vehicles Symposium 2025 vorgestellt und dient als Forschungsumgebung zur Untersuchung von Remote Driving und Remote Assistance Konzepten. Aufbauend auf den Basisfunktionen der weiterentwickelten Teleoperationssoftware, wurde das Perception Modifikation Konzept zur Modifizierung von Objekten umgesetzt. Die Implementierung ermöglicht das Vernachlässigen von Objekten, die Anpassung von Objektklassen und -prädiktionen. Ein besonderes Augenmerk lag auf der Modularität des Konzepts, um eine einfache Erweiterung der Implementierung um weitere Modifikationsmodi zu ermöglichen. Zur Entwicklung und Untersuchung der prototypischen Implementierung wurde eine Simulationsframework

entwickelt, das Autoware an den Open-Source Simulator CARLA anbindet. Das Framework [15] wurde auf der IEEE International Conference on Systems, Man, and Cybernetics (SMC) 2024 veröffentlicht. Die notwendigen Schnittstellen zur Modifizierung von Objekten wurden in der Automation Autoware implementiert.

Der am WIVW entwickelte Teleoperationssimulator stellt ein ergänzendes Werkzeug dar, das dazu dienen kann, teleoperationsspezifische Effekte systematisch zu untersuchen, neue HMI-Konzepte zu evaluieren, Use Cases zu demonstrieren und evtl. auch dazu, Teleoperatoren zu trainieren. Der Simulator wurde als modulares, variables Konzept umgesetzt, sodass er schnell an die Anforderungen der verschiedenen Stakeholder adaptiert werden kann. Die Konzeptentwicklung und Umsetzung des Simulators wurde in Form eines Workshopbeitrags („Praxis-Workshop autonomes und teleoperiertes Fahren“) im Rahmen der safe.tech Tagung 2025 des TÜV Süd in München vorgestellt [16].

### 3.9.4 Bildqualität zur sicheren Teleoperation (AP 9.4)

Da in der Teleoperation Videostreams die primäre Informationsquelle über die Umgebung dar-stellen, ist eine zuverlässige Einschätzung ihrer Qualität von zentraler Bedeutung. Nur so lassen sich Rückschlüsse auf die Auswirkungen verminderter Videoqualität auf den Operator und dessen Leistungsfähigkeit ziehen. Vor diesem Hintergrund wurden im Projekt zwei Schwerpunkte verfolgt: (1) die Untersuchung der Effekte unterschiedlicher Videoqualitäten auf den Operator und (2) die Entwicklung einer geeigneten Metrik zur quantitativen Bewertung dieser Qualität.

Im ersten Teil wurden mehrere Nutzerstudien durchgeführt, um den Einfluss der Bildqualität systematisch zu analysieren:

1. Auswirkungen der Bildqualität auf die Informationsverarbeitung während der Teleoperation von Straßenfahrzeugen,
2. Einfluss der Bildqualität auf die Erkennung von Verkehrszeichen,
3. Untersuchung der sicheren Pfadfolge bei der Teleoperation autonomer Fahrzeuge, und
4. Analyse der Wechselwirkungen zwischen Latenz und Bildqualität auf Leistungsfähigkeit und Arbeitsbelastung der Operatoren.

Die Ergebnisse verdeutlichten die Relevanz einer objektiven Bewertungsmöglichkeit von Videostreams für die Teleoperation. Daher wurden im zweiten Schritt etablierte Qualitätsmetriken hinsichtlich ihrer Eignung für sicherheitskritische Teleoperationsszenarien untersucht. Als Ausgangspunkt wurde VMAF von Netflix gewählt, das nach gezielten Anpassungen mit Daten aus dem Zenseact-Datensatz sowie mit menschlichen Bewertungen aus einer Online-Nutzerstudie neu trainiert und evaluiert wurde. Das resultierende Modell ermöglicht eine teleoperationsspezifische Einschätzung der Videoqualität. Zudem kam die neu trainierte VMAF-Metrik in der TUM Teleoperationssoftware zum Einsatz, die eine Echtzeit-Bewertung und Visualisierung der Videoqualität ermöglichte.

### 3.9.5 Evaluation und Auswertung (AP 9.5)

Im Arbeitspaket 9.5 des Projekts ATLAS-L4 wurde die abschließende Evaluation und Auswertung der zuvor erarbeiteten Komponenten des Control Centers durchgeführt. In der letzten

Phase des Projektzeitraums wurde das Gesamtsystem – bestehend aus Technischer Aufsicht, Control Center und Projektfahrzeug – mittels regelmäßiger Testfahrten intensiv getestet. Die Testfahrten dienten zudem der objektiven Erfassung wichtiger Leistungskennzahlen (KPIs) des „Hub2Hub"-Use-Cases, wie etwa Fahrzeiten, Geschwindigkeiten und GPS-basierte Fahrpräzision.

Die korrekte Funktionsweise der Schnittstelle zwischen Control Center und BEA wurde im Rahmen gemeinsamer Test-Meetings sichergestellt.

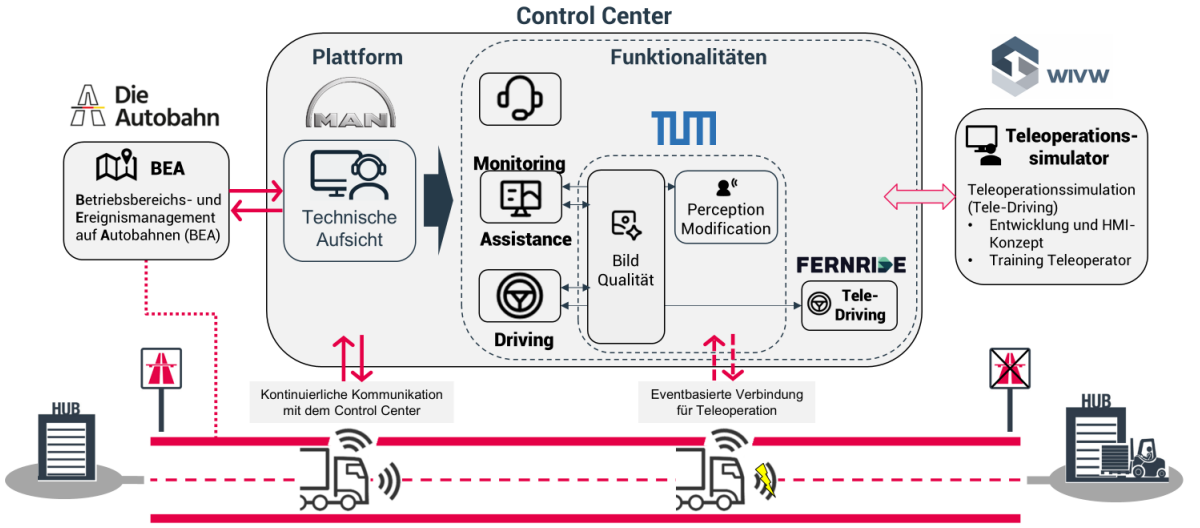
Die Bewertung des Perception Modification Konzepts und dessen prototypischer Umsetzung erfolgte iterativ. Das grundlegende Konzept wurde im Rahmen eines Expertenworkshops gegenüber anderen Remote-Driving und -Assistance Konzepten bewertet. Die Ergebnisse des Workshops [17] wurden im IEEE Open Journal of Intelligent Transportation Systems veröffentlicht. Das Konzept zur Visualisierung von Rohsensor- und Automationsdaten als Teil des HMI der Perception Modification wurde im Rahmen einer Probandenstudie evaluiert. Drei unterschiedliche Anzeigekonzepte wurden hinsichtlich der Kriterien Situationsbewusstsein, Workload, korrekte Situationslösung und Usability beurteilt. Die Ergebnisse der Studie werden auf der IEEE International Conference on Systems, Man, and Cybernetics (SMC) 2025 vorgestellt. Die Interaktion zwischen der Automation, dem Perception Modification System und dem TO wurde während der Entwicklung fortwährend mit dem eigens entwickelten Simulationsframework erprobt. Nach erfolgreichen Tests in der Simulation wurde das System auf dem Forschungsfahrzeug der TU München (EDGAR) in Betrieb genommen und auf dem Testgelände sowie im öffentlichen Straßenverkehr erprobt. Abschließend wurde das System im Rahmen der Abschlusspräsentation auf dem ADAC-Testgelände in Penzing vorgestellt. Dabei wurde EDGAR vom Remote-Assistance Arbeitsplatz des Control Centers aus mittels Modifikation von Objekten in Szenarien unterstützt, welche die Automation nicht eigenständig lösen konnte.

Am WIVW wurde eine Evaluationsstudie durchgeführt, die zwei Ziele hatte: Zum einen sollten bekannte Auswirkungen von Latenz auf das teleoperierte Fahren repliziert werden, um zu verdeutlichen, dass der simulationsbasierte Ansatz eine geeignete Methode zur Untersuchung von Human-Factors-Fragestellungen im Kontext des Remote Driving darstellt. Zum anderen sollte im Rahmen der Studie untersucht werden, ob und inwieweit die Verteilung der Gesamtlatenz auf Up- und Downlinklatenz das teleoperierte Fahren beeinflusst. Die Studie wurde mit 20 Versuchspersonen aus dem Versuchspersonenpanel des WIVW durchgeführt. Im Ergebnis zeigte sich, dass höhere Latenzen von den Versuchspersonen wahrgenommen werden und erwartungsgemäß den Workload erhöhen und die subjektive Fahrperformanz reduzieren. In vielen der untersuchten objektiven Maße können – insbesondere bei höheren Gesamtlatenzen (200 ms) – die erwarteten Effekte beobachtet werden, wobei die Aufteilung der Gesamtlatenz auf Up- und Downlink keine relevante Auswirkung hat. Im Rahmen der Evaluationsstudie konnte somit gezeigt werden, dass bekannte Auswirkungen von Latenz auf das teleoperierte Fahren mit einem simulationsbasierten Ansatz repliziert werden können. Somit kann davon ausgegangen werden, dass der Simulator eine geeignete Methode zur Untersuchung bestimmter Human-Factors-Fragestellungen im Kontext des Remote Driving darstellt. Die Ergebnisse der Evaluationsstudie zum Teleoperationssimulator wurden im Rahmen eines Fachvortrags auf der Abschlussveranstaltung in Penzing und als Konferenzbeitrag auf dem IEEE Intelligent Vehicles Symposium 2025 vorgestellt [18].

## 3.9.6 AP 9 - Vortrag und Poster der Abschlusspräsentation

### AP 9: CONTROL CENTER UND TELEOPERATION

**Entwicklungsschritte und Vernetzung**



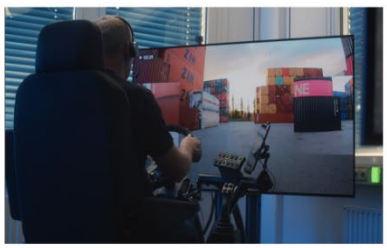

ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Lavinia Stollfuß, MAN Truck & Bus SE 47

### AP 9: CONTROL CENTER UND TELEOPERATION

**Projektergebnisse (1/2)**

- Anforderungskatalog mit technischen und prozessualen Anforderungen an die Funktionalitäten im Control Center
- Schulungskonzept für die Teleoperation/Teleoperatoren
- Aufbau und Evaluation eines Teleoperationsarbeitsplatzes und Anbindung an Simulationsumgebung
- Aufbau einer Teleoperation-Station für Echtzeit-Teleoperation als Tele-Driving-Konzept des Control Centers
- Aufbau des teleoperierten Fahrzeugs für Tele-Driving

Aufbau eines prototypischen, simulations-gestützten Fahrstands für das Tele-Driving



Teleoperatorarbeitsplatz von FERNRIDE und MAN

Kamerasystem am teleoperierten Fahrzeug

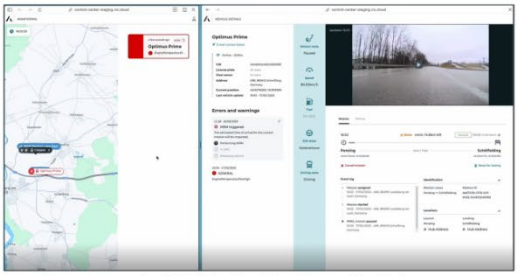
ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Lavinia Stollfuß, MAN Truck & Bus SE 48

## AP 9: CONTROL CENTER UND TELEOPERATION

**Projektergebnisse (2/2)**

- Prototypische Umsetzung und Untersuchung des Remote-Assistance Konzeptes *Perception Modification*
- Metriken zur Erfassung der Einflüsse der Bildqualität auf die Sicherheit der Teleoperation
- Aufbau einer digitalen Benutzeroberfläche zum Remote Monitoring & Assisting für die Tele-Überwachung und Koordination einer autonomen Fahrzeugflotte im Betrieb
- Entwicklung des Systems BEA (**B**etriebsbereichs- und **E**reignismanagement auf **A**utobahnen) für die digitale Genehmigung und Verwaltung von Betriebsbereichen inkl. Anbindung an das Control Center

Bildqualität: Beispiel eines komprimierten Bildes
(links: Original, rechts: komprimiert)



Control Center Benutzeroberfläche (links: Übersicht, rechts: Detailansicht)


BEA-Übersichtskarte

ATLAS-L4 | 7./8. Mai 2025 | Abschlusspräsentation – Lavinia Stollfuß, MAN Truck & Bus SE 49

# CONTROL CENTER UND TELEOPERATION
## Übersicht

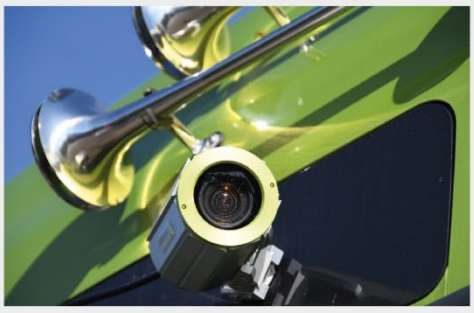
### MOTIVATION UND ZIELE

In diesem Arbeitspaket werden die Anforderungen an ein Control Center zur Überwachung und Steuerung von automatisierten Fahrzeugen erhoben. Dabei werden die Aufgaben des Control Centers in drei Säulen unterschieden: Remote Monitoring, Remote Assistance und Remote Driving. Für jeden dieser Bereiche werden Konzepte erstellt und mithilfe geeigneter Methoden untersucht.

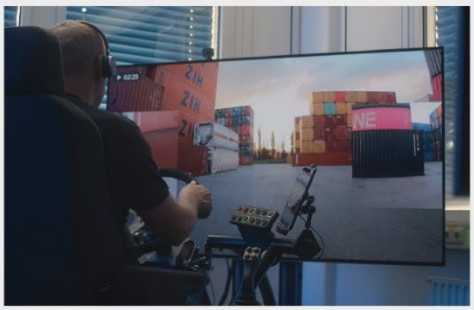
| REMOTE MONITORING 1:N | REMOTE ASSISTANCE 1:1 | REMOTE DRIVING 1:1 |
|---|---|---|
| ■ Überwachung der Fahrzeuge: Position, Geschwindigkeit, ...<br>■ Fahrzeugumgebung: Kamera,...<br>■ ODD Grenzen: Wetter, Verkehr,...<br>■ Detailinfos zu Fahrzeug abrufen<br>■ Wahrnehmung der Aufgaben der technischen Aufsicht | ■ ADS Freigabe + Deaktivierung<br>■ Trajektorienfreigabe<br>■ Umfeldmodellmodifikation<br>■ Risikominimalen Zustand auslösen<br>■ Wahrnehmung der Aufgaben der technischen Aufsicht | ■ Direkte Steuerung: Längs- und Querführung<br>■ Assistierte Steuerung = shared control (z. B. Level 2 Automatisierung)<br>■ Trajektorienvorgabe / Pfadvorgabe + manuelle Beschleunigung<br>■ Sekundäre Fahraufgaben (Blinken, Licht, Warnblinker, Hupe, ...) |
| CONTROL CENTER | | |

### ERGEBNISSE

- Anforderungskatalog mit technischen und prozessualen Anforderungen an Remote Driving und Remote Monitoring im Control Center
- Schulungskonzept für die Teleoperation/Teleoperator
- Aufbau und Evaluation eines Teleoperationsarbeitsplatzes und Anbindung an Simulationsumgebung
- Aufbau einer Teleoperation-Station für Echtzeit-Teleoperation als Tele-Driving-Konzept des Control Centers
- Aufbau des teleoperierten Fahrzeugs für Remote Driving
- Prototypische Umsetzung und Untersuchung des Remote-Assistance Konzeptes Perception Modification
- Metriken zur Erfassung der Einflüsse der Bildqualität auf die Sicherheit der Teleoperation
- Entwicklung des Systems BEA (Betriebsbereichs- und Ereignismanagement auf Autobahnen) für die digitale Genehmigung und Verwaltung von Betriebsbereichen inkl. Anbindung an das Control Center



Kamerasystem am Lkw

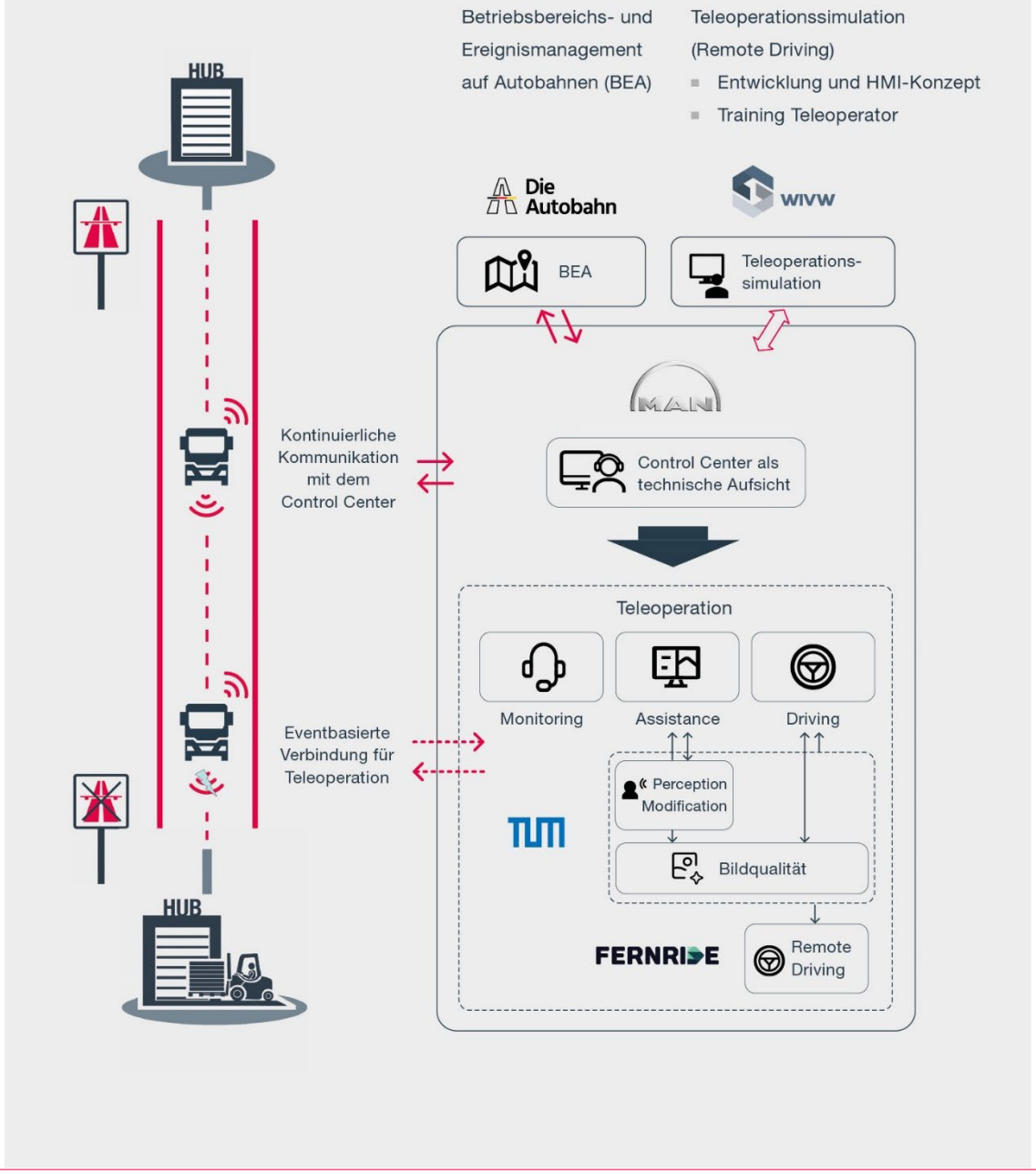


Teleoperatorarbeitsplatz von FERNRIDE und MAN

# CONTROL CENTER UND TELEOPERATION

## Übersicht

### ENTWICKLUNGSSCHRITTE UND VERNETZUNG



# BEA: BETRIEBSBEREICHS- UND EREIGNISMANAGEMENT AUF AUTOBAHNEN

## Control Center und Teleoperation

### GEWÄHRLEISTUNG DER VERKEHRSSICHERUNGSPFLICHT

Um die Verkehrssicherungspflicht zu gewährleisten und zukünftig autonomes Fahren in das Verkehrsmanagement zu integrieren, hat die Autobahn GmbH das digitale Managementsystem BEA (Betriebsbereichs- und Ereignismanagement auf Autobahnen) entwickelt.

Verkehrszentrale Deutschland der Autobahn GmbH

### VERNETZT MIT DEM CONTROL CENTER UND AutobahnOS

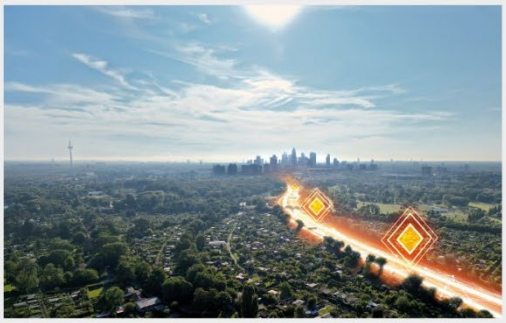
BEA ist mit dem Control Center vernetzt und ermöglicht es, das autonome Fahren zu monitoren und bei dynamischen Ereignissen – wie z. B. Arbeitsstellen – Anordnungen zu Fahrteinschränkungen für autonome Fahrzeuge zu übermitteln. Informationen über aktuelle dynamische Ereignisse werden von AutobahnOS, dem Betriebssystem für die Verkehrszentralen der Autobahn GmbH, bezogen.


Architektur

### GEMEINSAM AN EINEM STRANG

Durch die frühzeitige Zusammenarbeit von Fahrzeughersteller und Straßenbetreiber konnten in folgenden Bereichen die Grundlagen für eine gesamtheitliche Begleitung des autonomen Fahrens gelegt werden:

- Genehmigung und Verwaltung von Betriebsbereichen
- Abstimmung zum Minimum Risk Manoeuvre
- C-ITS-Direktkommunikation zur Warnung vor Gefahrenstellen



# EINFLUSS DER BILDQUALITÄT AUF REAKTIONSZEITEN SOWIE DIE ERKENNUNG UND VERFOLGUNG DES STRASSENVERLAUFS

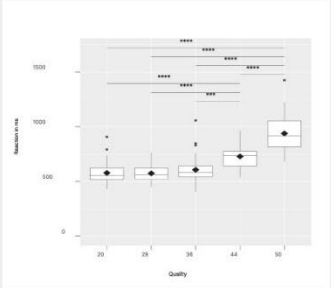
## Control Center und Teleoperation

In der Teleoperation ist eine präzise und schnelle Erkennung dynamischer Objekte essenziell für die Sicherheit. Diese Studien analysieren, welche potenziellen Risiken durch reduzierte Bildqualität entstehen (Simon Hoffmann).

### Erkennung von dynamischen Objekten

Reduzierte Bildqualität verlängert die Reaktionszeit auf dynamische Objekte signifikant.

- **Sicherheitsrisiko:** Ab Q36 überschreiten einige Teilnehmer die erforderliche Reaktionszeit zur Kollisionsvermeidung.
- **Kollision:** Ab Q50 war eine Reaktion der Versuchspersonen auf Objekte nicht mehr möglich.

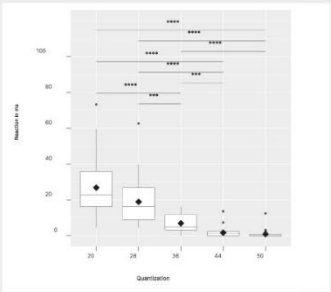


Reaktionszeit auf ein dynamisches Hindernis

### Erkennung von statischen Objekten und Verkehrszeichen

Reduzierte Bildqualität verlängert die Reaktionszeiten auf statische Objekte und Verkehrsschilder.


- **Sicherheitsrisiko:** Verzögerte Reaktionen können sicherheitskritische Folgen haben.
- **Fehlreaktionen:** Bei Hindernissen nehmen sie signifikant zu, bei Verkehrsschildern nicht.

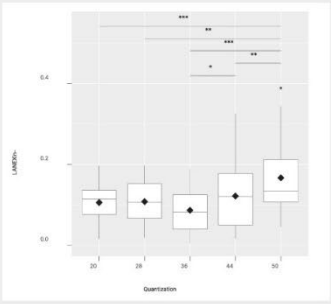


Abstand zum statischen Hindernis nach einer korrekten Reaktion.

### Erkennen und Verfolgen des Straßenverlaufs

Eine reduzierte Bildqualität beeinträchtigt die Fahrstabilität und erhöht den kognitiven Aufwand für die Steuerung.

- **Spurhaltung und Steueraufwand:** Reduzierte Bildqualität führt zu häufigeren Spurabweichungen und erhöhtem Steueraufwand, signifikant erst bei hohen Quantisierungsstufen.
- **Erkennung von Fahrbahnmarkierungen:** Eingeschränkte Sichtbarkeit erfordert Anpassungen im Steuerverhalten.
- **Kognitive Belastung:** Steigt mit abnehmender Bildqualität, signifikant jedoch nur bei den niedrigsten Qualitätsstufen.



Außerhalb der Fahrspur gefahrene Strecke im Verhältnis zur Gesamtstrecke

# BEWERTUNG DER VIDEOQUALITÄT

## Control Center und Teleoperation

### PROBLEME IN DER TELEOPERATION

Instabile Mobilfunkverbindungen erschweren die Datenübertragung zwischen Fahrzeug und Operator, was eine Kompression der Videostreams erforderlich macht. Dabei besteht ein Zielkonflikt zwischen niedriger Datenrate und ausreichender Bildqualität, die für die sichere Durchführung der Fahraufgabe essenziell ist. Eine geeignete Metrik zur Bewertung der Bildqualität im Kontext der Teleoperation wurde bislang jedoch nicht entwickelt oder validiert.

Beispiel eines komprimierten Bildes
(links: Original, rechts: komprimiert)

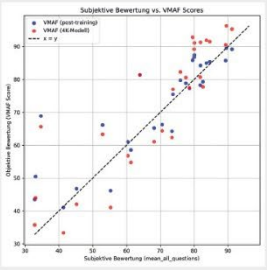
### ToFMaF

Um in Echtzeit situationsabhängige Anpassungen an verringerte Bildqualität vornehmen zu können, bedarf es einer geeigneten Bewertungsmetrik. Für den Bereich des Videostreamings wurde von Netflix die Metrik „VMAF“ (Video Multimethod Assessment Fusion) entwickelt, die sich als Industriestandard etabliert hat. Neumeier et al. [1] zeigen jedoch, dass VMAF für den speziellen Anwendungsfall des teleoperierten Fahrens nicht ausreichend geeignet ist. Dennoch diente VMAF aufgrund seines etablierten Status als Ausgangspunkt für die Entwicklung der ToFMAF-Metrik.

[1] *Neumeier, Stefan & Stapf, Simon & Facchi, Christian. (2020). The Visual Quality of Teleoperated Driving Scenarios How good is good enough?. 1-8. 10.1109/ISNCC49221.2020.9297343.*

### STUDIE

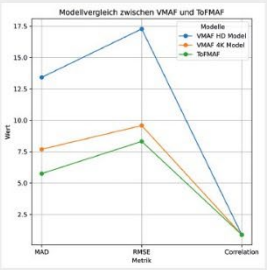
- Teilnehmende bewerteten Videopaare (komprimiert vs. Original)
- Bewertung anhand Fragen zur visuellen Qualität hinsichtlich der Fahraufgabe
- Erstellung eines subjektiven Scores aus den Nutzerbewertungen
- Verwendung dieses Scores als Trainingsgrundlage für das neue VMAF-Modell




Vergleich der menschlichen Bewertungen vs neu trainiertes und 4K VMAF Modell

### ERGEBNISSE

- Höhere Übereinstimmung des ToFMAF-Modells mit menschlicher Bewertung als bei bestehenden Modellen
- Potenzial zur weiteren Verbesserung bei Verfügbarkeit größerer Datenmengen




HD und 4K VMAFModel vs neu trainiertes ToFMAF

# PERCEPTION MODIFICATION
## Remote-Assistance auf Perception Level
### Control Center und Teleoperation

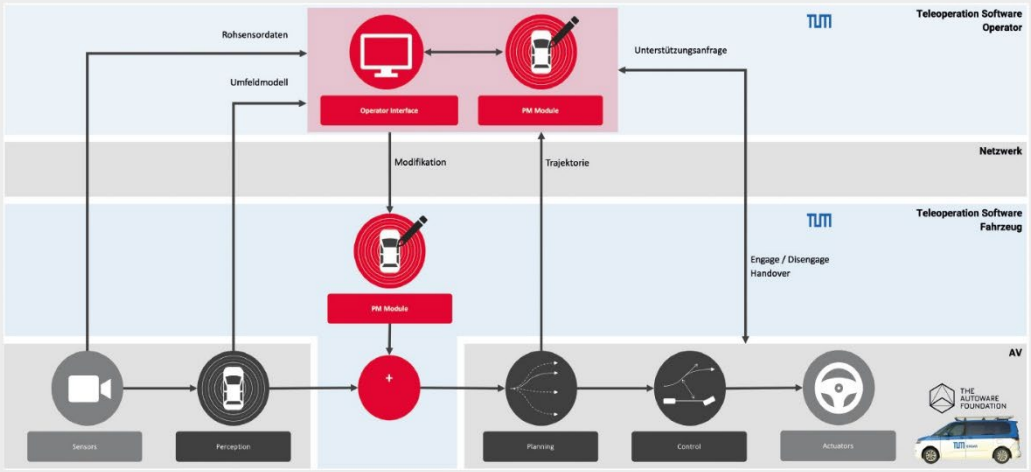



Abb.1: Übersicht Perception Modification Gesamtkonzept

## MOTIVATION

- Großer Anteil der Disengagements automatisierter Fahrzeuge ist direkt oder indirekt auf Fehler in der Wahrnehmung zurückzuführen [1, 2].
- Potenzial zur Verringerung der mentalen Belastung der Teleoperatoren [2] durch den Ersatz der zeitkritischen, kontinuierlichen Aufgaben im Remote Driving durch eine zeitdiskrete Entscheidung zur Unterstützung der Umfeldwahrnehmung.

## ERGEBNISSE

- Identifikation von Use-Cases der Perception Modification
- Weiterentwicklung der TUM Teleoperation Software
- mit dem Ziel, Konzepte der Remote-Assistance zu integrieren
- Modulare Gesamtkonzept der Perception Modification
- Umsetzung des Konzeptes mit der TUM Teleoperation Software und Autoware
- Proof-of-Concept durch Umsetzung der Object Modification
- Erprobung in der Simulation und mit Forschungsfahrzeug EDGAR
- Weiterentwicklung der Visualisierung der TUM Teleoperation Software und Untersuchung verschiedener HMIs für die Perception Modification

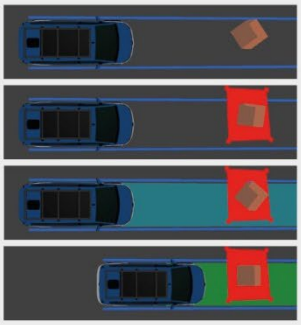


Abb. 2: Object Modification: Ignorieren einer Objektdetektion

## AUSBLICK

- Evaluation des Gesamtsystems im Rahmen einer Probandenstudie
- Weiterentwicklung des Systems auf Basis der Studienergebnisse und der identifizierten Use-Cases

[1] *Banerjee et al.: „Hands Off the Wheel in Autonomous Vehicles?: A Systems Perspective on over a Million Miles of Field Data", 2018*
[2] *Feiler: „Modifizierung der maschinellen Wahrnehmung mittels Teleoperation", 2022*

# PERCEPTION MODIFICATION
# Visualisierung von Umfeldwahrnehmungsgsdaten für die Remote-Assistance automatisierter Fahrzeuge
## Control Center und Teleoperation

### MOTIVATION UND ZIELE

Bei der Perception Modification müssen Teleoperatoren Rohsensordaten mit dem aktuellen Umgebungsmodell des Fahrzeuges abgleichen, um mögliche Fehlwahrnehmungen zu identifizieren.
Eine zentrale Rolle spielt dabei die Visualisierung der Daten – Sie verschafft dem Teleoperator ein hinreichendes Situationsbewusstsein und bildet somit die Grundlage für sichere Entscheidungen. Ziel der Studie ist es, Visualisierungsansätze hinsichtlich ihrer Eignung für die Perception Modification zu untersuchen.

a. Separate View

b. Merged View Ground Truth (GT)

c. Merged View Neural Depth Completion (DC)

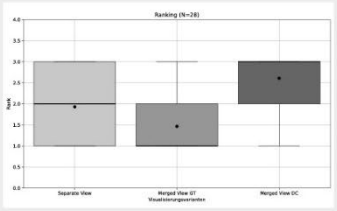
Abb. 1: Visualisierungsvarianten

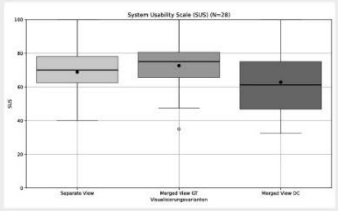
### STUDIENDESIGN

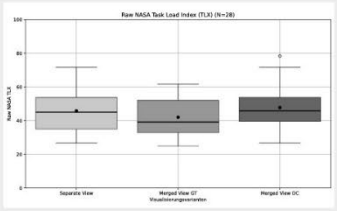
- **Design:** Online Studie mit aufgezeichneten Disengagement Szenarien im Within-Subject Design
- **UV:** Drei unterschiedliche Ansätze zur gemeinsamen Visualisierung von 2D (z. B. Video) und 3D Daten (z. B. Punktewolken) (vgl. Abb. 1)
- **Aufgabe:** Identifikation von Wahrnehmungsfehlern mit Hilfe der Visualisierungsvarianten und Entscheidung für einen Lösungsansatz in vier Szenarien je Variante.
- **AV:** Beanspruchung, Usability, Situational Awareness und Lösungsansatz

### ERGEBNISSE

- 28 Studienteilnehmer mit ingenieurwissenschaftlichem Hintergrund überwiegend im Bereich Automotive



# TELEOPERATION

## Control Center und Teleoperation

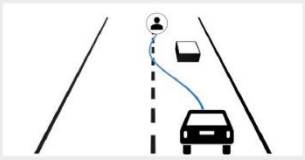
### KONZEPTE

Teleoperation stellt eine zuverlässige Rückfallebene für automatisierte Fahrzeuge in komplexen Szenarien dar. Aus diesem Grund forschen wir an verschiedenen Teleoperationskonzepten.


### REMOTE DRIVING

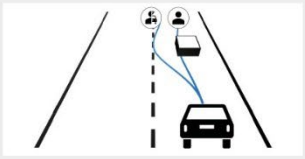
**Direct Control**

Der Operator übernimmt die Fahraufgabe durch kontinuierliche Vorgabe von Steuersignalen.



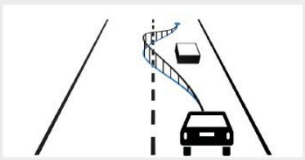
**Shared Control**

Der Operator übernimmt die Fahraufgabe und wird dabei fortlaufend vom System unterstützt.



**Trajectory Guidance**

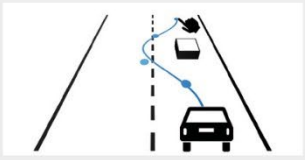
Der Operator übernimmt die Fahraufgabe durch Vorgabe von Trajektorien.



### REMOTE ASSISTANCE

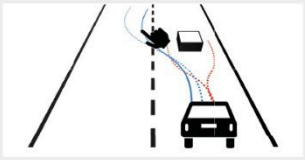
**Waypoint Guidance**

Der Operator unterstützt die Pfadplanung durch Vorgabe von Wegpunkten.



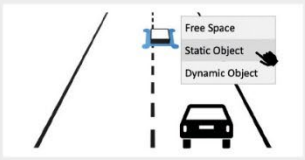
**Collaborative Planning**

Der Operator unterstützt die Pfadplanung durch Auswahl eines Pfades aus vorgeschlagenen Optionen.



**Perception Modification**

Der Operator unterstützt die Umfeldwahrnehmung durch Korrektur des Umfeldmodells.




*D. Brecht, N. Gehrke, T. Kerbl, N. Krauss, D. Majstorović, F. Pfab, M.-M. Wolf, and F. Diermeyer, „Evaluation of Teleoperation Concepts to Solve Automated Vehicle Disengagements", IEEE Open Journal of Intelligent Transportation Systems, vol. 5, pp. 629–641, 2024.*

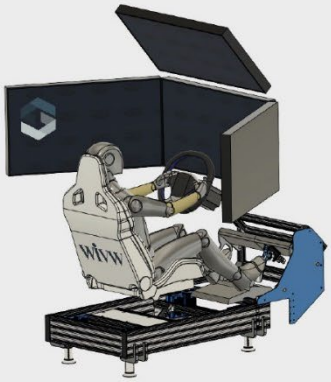
*D. Majstorović, S. Hoffmann, F. Pfab, A. Schimpe, M. -M. Wolf and F. Diermeyer, „Survey on Teleoperation Concepts for Automated Vehicles", 2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Prague, Czech Republic, pp. 1290-1296, 2022.*

# SIMULATION DES TELEOPERIERTEN FAHRENS

## Control Center und Teleoperation

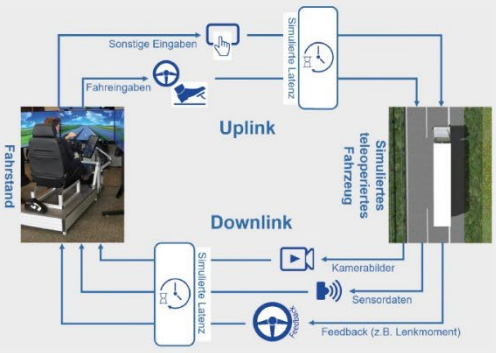
### ZIEL

- Aufbau eines prototypischen, simulationsgestützten Fahrstands für die Teleoperation (Remote Driving) eines LKW
- Evaluation der Eignung als Forschungs- und Trainingsinstrument



### IMPLEMENTIERUNG

- Modulares Konzept für optimale Variabilität im Versuchs- und Trainingsbetrieb
- Konstruktion aus Aluminium-Schienenprofilen
  - Basis für Montage von Fahrersitz, Lenkrad und Pedalerie
  - 4 x 48 Zoll Bildschirme
  - 5.1-Surround-Soundanlage
- Haptische Aktoren (D-Box), Kraftrückmeldung der Pedalerie (passiv, Feder-Dämpfer-Kennlinie) und Momentrückmeldung am Lenkrad (Direct Drive)
- Rechnernetz mit 6 PCs, Fahrsimulation mit SILAB® 7.2




### ERGEBNISSE UND AUSBLICK

- Die Teleoperationssimulation ermöglicht die kontrollierte Variation von Parametern, die das Remote Driving beeinflussen können (z. B. Sichten, Videoqualität, Latenz) und stellt ein effizientes Forschungstool dar
  - Empirische Untersuchung von Human-Factors Herausforderungen (z. B. Workload, Situation Awareness, Präsenzgefühl)
  - Gestaltungsempfehlungen für Arbeitsplatz der Teleoperierenden (z. B. bzgl. Sicht- und Geräuschdarstellung, Transitionen und Warnungen, Graphical User Interface, Assistenzsysteme)
- Trainingstool für das Fahren unter teleoperationsspezifischen Anforderungen
  - Fahraufgaben (z. B. Rangieren)
  - Szenarien (z. B. Übernahme aus Stillstand, Wechsel zwischen Fahrzeugen)

# AUSWIRKUNGEN VON UP- UND DOWNLINK-LATENZ AUF DAS TELEOPERIERTE FAHREN – Eine Probandenstudie im Teleoperationssimulator

## Control Center und Teleoperation

### ZIEL

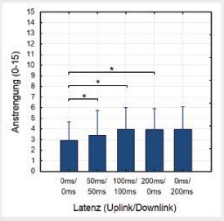
- Untersuchung von Auswirkungen unterschiedlicher Latenzzeiten zwischen Fahrstand und teleoperiertem Fahrzeug auf das Fahrverhalten, die Fahrperformanz und die Arbeitsbelastung der Teleoperierenden
- Spielt die Aufteilung der Latenzzeit in Uplink- und Downlink-Latenz eine Rolle?
- Eignung des Teleoperationssimulators als Forschungsinstrument

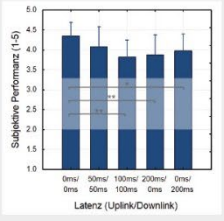
### METHODEN

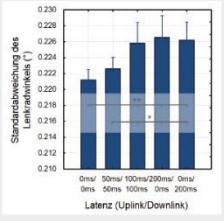
- Simulation des teleoperierten Fahrens (Remote Driving) mit SILAB®
- N = 20 Probanden, within-Versuchsdesign
- Unabhängige Variablen
  - Latenz (Uplink/Downlink): 0/0ms, 50/50 ms,100/100 ms, 200/0 ms, 0/200 ms
  - Szenario/Fahraufgabe: Autobahn mit Fahrzeugfolgen, Landstraße mit verschiedenene Kurven
- Abhängige Variablen: Latenzwahrnehmung, Workload, Performanz (objektiv, subjektiv)

### ERGEBNISSE

- Im Durchschnitt wird eine Veränderung der Latenz von den Probanden erkannt *(F(4,76) = 4.25, p = .004)*
  - Jedoch auch Personen, die bei Latenzen von 200 ms keine Latenz wahrnehmen
- Bei einer Latenz von 200 ms steigt die Anstrengung *(F(4,76) = 4.09, p = .005)* und die subjektive Performanz sinkt *(F(4,76) = 5.28, p = .001)*
  - Abstandshaltung vor allem bei hoher Downlink-Latenz beeinträchtigt
- Kein signifikanter Effekt der Latenz auf die Spurhaltung *(SDLP; Beispiel Landstraße: F(4,76) = 0.67, p = .616).* Der Aufwand für die Spurhaltung steigt jedoch bei Latenzen von 200 ms *(LS: F(4,76) = 13.42, p <.001).*
  - Als Kompensation wird bei Latenz häufiger gebremst und Geschwindigkeit reduziert.



# MINIMUM RISK MANEUVER (MRM)

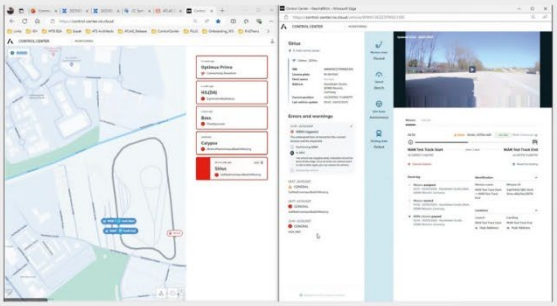
## im Zusammenspiel mit Technischer Aufsicht im Control Center und Vehicle-to-X Kommunikation

### DEMONSTRATIONSINHALTE

- Minimum Risk Maneuver als Rückfallebene für Fehler und kritische Situationen im Betrieb autonomer Fahrzeuge, mit dem Ziel, das Fahrzeug in einen risikominimalen Zustand zu überführen.
- Wahl des Maneuvers und des Anhaltepunkts als Gesamtrisikoabwägung in Abhängigkeit von Verkehrssituation und Einschränkung der Fähigkeiten des Systems
- Auslösung des MRM erfolgt im Regelfall automatisch
- Schnittstelle zur Technischen Aufsicht zur ferngesteuerten Auslösung und Überwachung, Information anderer Verkehrsteilnehmer, visuell und über Vehicle-to-X Kommunikation


Minimum Risk Maneuver mit sicherem Halt auf Seitenstreifen


Warnung anderer Verkehrsteilnehmer via V2X



MRM: Visualisierung in Control Center Benutzeroberfläche

### BESCHREIBUNG DES VERSUCHSTRÄGERS

- Sattelzug und Begleit-PKW
- Ausrüstung mit autonomer Fahrfunktion
- Konnektivität mit Technischer Aufsicht im Control Center über Mobilfunk
- Warnung anderer Verkehrsteilnehmer über V2X (IEEE 802.11p)

Demonstrationsfahrzeug

# Zusammenfassung und Technologie-bewertung; Verwertbarkeit der Ergebnisse

Projektkoordinator: Sebastian Völl, MAN Truck & Bus SE

# 4 Zusammenfassung und Technologiebewertung; Verwertbarkeit der Ergebnisse

## 4.1 Zusammenfassung

Im Projekt ATLAS-L4 konnten zwölf Projektpartner aus Industrie, Wissenschaft und Softwareentwicklung sowie Infrastrukturbetreiber innerhalb von dreieinhalb Jahren Projektlaufzeit einen ganzheitlichen konzeptionellen Ansatz zur Darstellung und zum Test eines autonomen Lkws (mit Sicherheitsfahrer) im öffentlichen Straßenverkehr in Deutschland vor dem Hintergrund des Gesetzes zum autonomen Fahren realisieren. Neben Anforderungsdefinition, Safety- und Securitybetrachtung für ein Level-4-System wurde ein Validierungskonzept erstellt, um effizientes Testen der Fahrzeugfunktionalitäten sowie des sicheren Fahrzeugverhaltens zu ermöglichen. Die Implementierung eines Control Centers für die Aufgaben der Technischen Aufsicht (Remote Monitoring und Remote Assistance) sowie zur Realisierung teleoperierten Fahrens (Remote Driving) wurde durchgeführt.

Innerhalb des Projekts wurden vier Fahrzeuge aufgebaut, mit denen die jeweiligen Konzepte und Technologien auf Machbarkeit hin untersucht wurden. Ein Sensorfahrzeug insbesondere zur Darstellung des Sensorkonzepts, ein ARB-Fahrzeug zur Entwicklung der redundanten Komponenten Bremse und Lenkung, ein Bordnetzfahrzeug für die Entwicklung des redundanten Bordnetzes und ein Demonstrationsfahrzeug mit den konzeptionellen Inhalten des Automatisierungssystems für die Abschlusspräsentation. Für das Sensor- und Demonstrationsfahrzeug wurde dazu jeweils eine Erprobungsgenehmigung nach AFGBV erwirkt, um die Level-4-Konzepte im öffentlichen Straßenverkehr auf der Autobahn (mit Sicherheitsfahrer aufgrund der prototypischen Implementierung) demonstrieren zu können.

Die erzielten Ergebnisse wurden am 7. und 8. Mai 2025 dem interessierten Fachpublikum auf der Abschlusspräsentation auf dem ADAC Testgelände in Penzing erfolgreich vorgestellt. Zirka 220 Gäste konnten sich an den beiden Tagen in der Fachausstellung über die Detailergebnisse der neun Arbeitspakte informieren. Die Gäste konnten die jeweiligen Fahrzeugimplementierungen in sechs Fahrdemonstrationen erleben.

## 4.2 Technologiebewertung

Tabelle 5 zeigt eine Übersicht über die Bewertung der verschiedenen entwickelten und eingesetzten Technologien hinsichtlich ihres Reifegrads / Relevanz für die weitere Nutzung. Dabei ist zu beachten, dass der vorgegebene Rahmen eines öffentlich geförderten Projekts bei einigen eingesetzten Technologien auch bereits einen Rahmen vorgibt, wie weit diese innerhalb des Projekts entwickelt werden können. Die in Tabelle 1 genannten Kerninnovationen sind ebenfalls in dieser Übersicht dargestellt.

Tabelle 5 Übersicht Technologiebewertung

| Technologie | Bewertung | Kommentar |
|---|---|---|
| ODD-Beschreibung | Mittel-Hoch | ODD-Konzept erstellt. Konkrete ODD-Beschreibung für Testbetrieb im Rahmen der AFGBV-Freigabe erstellt und umgesetzt. Darüber hinaus zahlreiche L4 Aspekte abgebildet. |

| Technologie | Bewertung | Kommentar |
|---|---|---|
| Safety-Konzept Level-4 | Hoch | Konzept bzgl. MRM, Redundanzen, Sicheren Zuständen umfassend betrachtet. Teilweise bereits in den Prototypen-Fahrzeugen umgesetzt.<br>Safety-Konzept für L4 Testbetrieb vollständig erstellt und im Rahmen der AFGBV-Freigabe implementiert und genutzt. |
| Security-Konzept Level-4 | Hoch | Konzepte für Automated Driving System und Control Center vollständig, keine Implementierung im Projekt vorgesehen |
| Erstellung und Umsetzung Testkonzepte | Mittel | Prototypisches Testkonzept für die Sicherheitsvalidierung des L4-Planers |
| Testlösungen und -werkzeuge für das szenarienbasierte Testen | Mittel-Hoch | Prototypische Toolkette zum szenarienbasierten Testen des L4-Planers in virtueller Simulationsumgebung |
| Umsetzung des Sensorkonzepts im Fahrzeug | Niedrig | Teilweise A-Muster der Sensoren mit prototypischer Sensorsoftware |
| Redundante Bremse | Mittel | B-Musterstand mit Straßenfreigabe |
| Redundante Lenkung | Mittel | B-Muster mit Sonderstraßenfreigabe |
| Redundantes Bordnetz | Mittel | Redundantes Bordnetz im B-Musterstand<br>Intelligenter Leistungsverteiler im<br>A-Musterstand |
| Konzept zur Fahrzeugarchitektur | Mittel - Hoch | konzeptioneller Reifegrad für die Umsetzung in der Vorentwicklung erreicht |
| Umsetzung des Architekturkonzepts im Fahrzeug | niedrig | A-Musterstand in Hardware |
| Funktionsimplementierung der Automatisierungsfunktion | Mittel | Prototypische Darstellung der Automatisierungsfunktion |
| Konzept und Umsetzung einer technischen Aufsicht automatisierter Fahrzeuge | Niedrig | A-Musterstand in Software |
| Teleoperation und Teleoperatorarbeitsplatz für schwere Nutzfahrzeuge | Hoch | Das Fernride Teleoperationssystems wurde erfolgreich in den MAN Truck verbaut, getestet und während der Demo im Mai 2025 gezeigt. Die entwickelte Lösung bildet eine solide Grundlage für zukünftige autonome und teleoperierte Anwendungen bei schweren Nutzfahrzeugen. |

Zusammenfassend lässt sich sagen, dass sich insbesondere auf der konzeptionellen Ebene eine hohe Bewertung der Technologien erzielt wurde. Hier konnte in Anlehnung an

bestehende und bekannte Standards der Konzeptumfang auf Level-4-Fahren erweitert werden, ohne dass es signifikante Anpassungen an die jeweiligen Prozesse benötigte.

Die Umsetzung der Konzepte in Hardware im Fahrzeug hat dazu im Vergleich eine niedrigere Bewertung. Dies liegt insbesondere an den Vorteilen von A-Mustern für die schnelle und kostengünstige Darstellung sowie Implementierung von Funktionalitäten in frühen Entwicklungsstadien. Kombiniert mit der Anforderung der Kompatibilität mit bestehenden prototypischen Entwicklungstoolketten ergibt sich die Notwendigkeit des Einsatzes von Hardware, die eine schnelle Softwareänderung zulässt und gleichzeitig dokumentierbar bleibt. Teile der eingesetzten Software können bereits als Basis für eine spätere Serienimplementierung verwendet werden, wohingegen andere Teile spezifisch für die ATLAS-L4-ODD oder zur Ermöglichung des Testbetriebs mit Sicherheitsfahrer prototypisch implementiert wurden.

## 4.3 Verwertbarkeit der Ergebnisse

Insbesondere die in ATLAS-L4 erarbeiteten Konzepte für eine Level-4-Funktionalität eines Automatisierungssystems bieten eine sehr gute Grundlage für eine spätere Industrialisierbarkeit. Dies wird auch durch die Dokumentation in entsprechenden Tools und Datenbanken sichergestellt, die das Wissen entsprechend konservieren und für eine spätere Vor- und Serienentwicklung verfügbar halten.

Die Verwertbarkeit der Security-Ergebnisse gründet auf der im Projekt weiterentwickelten, für Level-4-Automatisierung spezialisierten Security-Risikoanalyse-Methode, der konsolidierten Analyse relevanter Security-Standards und einem prototypischen, bereichsübergreifenden Security-Management-Tool. Mit dieser Methode können Akteure der Automobilbranche unterstützt werden, Level-4-Systeme und -Funktionen strukturiert hinsichtlich Sicherheitsrisiken zu prüfen. Sie schafft eine belastbare Grundlage, Konformität mit ISO/SAE 21434 und UN Regulation No. 155 auch für Level-4-Funktionen und -Systeme im Zusammenspiel mit ergänzenden organisatorischen und technischen Maßnahmen zu erreichen. Die zusammengeführten Anforderungen und Empfehlungen fördern den Aufbau eines einheitlichen, bereichsübergreifenden Security-Standard-Managements. Das prototypische Tool kann gemeinsam mit interessierten Unternehmen zu einer vollwertigen, anpassbaren Softwarelösung weiterentwickelt und in bestehende Prozesse integriert werden. Die Ergebnisse werden über Fachkonferenzen, Gremien und Verbände verbreitet, fließen in die Lehre der Partnerhochschulen ein und sind auf angrenzende Domänen wie Industrieautomation, Know-how- und Produktschutz, Smart Grid, Telekommunikation und hardwarenahe Security übertragbar. Ferner bilden sie die Basis für Anschlussprojekte und anwendungsnahe Dienstleistungen.

Die konkrete Implementierung der Hardware des Automatisierungssystems im Fahrzeug kann für weiterführende Machbarkeitsanalysen herangezogen werden. Allerdings ist eine Verwertung hinsichtlich eines Seriensystems nicht zielführend. Zum einen zeigt die Konstellation von entsprechender Sensorik und Steuergeräten den Stand zum Ende des Projekts, was vermutlich in dieser Form nicht mehr wieder identisch aufgebaut werden wird. Zum anderen wurde insbesondere Wert darauf gelegt, dass entsprechende Sensorik und Komponenten ihren funktionalen Zweck während der Projektlaufzeit erfüllen. Weitere Anforderungen für die genutzten Komponenten für eine spätere Serienverwendung wurden in ATLAS-L4 nicht betrachtet.

Zur Entwicklung des redundanten Bremssystems wurde bei Knorr-Bremse ein Projekt nach dem Standard des firmeneigenen Product Development and Commercialization (PDC) Prozesses aufgesetzt, dem auch Serienprojekte folgen. Dieser stellt eine zielgerichtete Entwicklung bis hin zu einem verkaufsfähigen, serienreifen System sicher. Qualitätssicherung Maßnahmen, wie die saubere Dokumentation von Arbeitsergebnissen, Risikomanagement oder regelmäßige Projektreviews sind dabei mit inbegriffen. Im Rahmen von ATLAS-L4 wurde der PDC bis zum sogenannten Gate 30 durchlaufen. Hier erfolgt auf Basis der erfolgreich abgesicherten B-Muster (Produkt und Systemebene) und im Übrigen auch final abgestimmter und dokumentierter Requirements der Designfreeze. Die so geschaffene Grundlage ist die ideale Ausgangsposition für eine weitere Entwicklung und Kommerzialisierung des Vorhabens, die im nächsten Schritt das Auslösen der Serienwerkzeuginvestitionen vorsieht (C-Muster).

Das entwickelte und validierte Energiebordnetzkonzept zielt auf das automatisierte Fahren des SAE-Level 4 ab und grenzt sich deutlich gegenüber dem aktuellen Stand der Technik ab. Insbesondere die schnelle Isolation von Kurzschlüssen durch elektronische Sicherungen, die Rückwirkungsfreiheit zwischen Kanälen und Bordnetzen tragen zur erhöhten Verfügbarkeit der Einzelsysteme und der sicherheitsrelevanten Verbraucher bei.

Die nächsten Schritte zur Weiterentwicklung des Konzepts wären eine Optimierung der Architektur im Hinblick auf kundenspezifische Anforderungen sowie eine technische und wirtschaftliche Betrachtung eines Konzepts mit ausschließlich elektronischen Sicherungen im Vergleich mit dem hier gewählten hybriden Ansatz.

Die Toolkette zum szenarienbasierten Testen des L4-Planers wurde prototypisch und beispielhaft in einer virtuellen Simulationsumgebung in einem realistischen industriellen Rahmen eingesetzt. Diese simulative Testmethode scheint daher in Zukunft ein vielversprechender Ansatz für die Sicherheitsvalidierung von autonomen Lkws zu sein. Die Toolkette kann in verschiedenen Kontexten wiederverwertet werden. Die ODD „Autobahn“ kann beispielsweise erweitert werden, z.B. für den Stadtverkehr, was sich v. a. in der Spezifikation der Szenarien widerspiegeln würde. Es könnten andere Fahrzeugtypen wie z.B. Pkws in die Werkzeugkette integriert und getestet werden. Zudem lässt sich die Simulationsumgebung durch eine andere austauschen.

Die Konzepte und Implementierung des Control Centers mit den Aufgaben der technischen Aufsicht aus ATLAS-L4 bilden die Basis für weitergehende Entwicklungen und zur Vervollständigung der Anforderungen nach dem Straßenverkehrsgesetz. Hier wurde zur Projektlaufzeit Dokumentation, Implementierung und Projektteam so aufgesetzt, dass nach dem Abschluss von ATLAS-L4 an der Funktionalität weitergearbeitet werden kann.

Gemäß dem Gesetz zum autonomen Fahren von 2021 ist die Autobahn GmbH für die Genehmigung von Betriebsbereichen auf Autobahnen für autonome Fahrzeuge zuständig. Um diese Aufgabe umzusetzen, wurde in ATLAS-L4 das digitale Managementsystem BEA (Betriebsbereichs- und Ereignismanagement auf Autobahnen) entwickelt. Zum einen dient BEA Antragstellenden als digitale Genehmigungsplattform für die Betriebsbereichsgenehmigung, zum anderen kann die Autobahn GmbH mittels die BEA die Betriebsbereiche verwalten und das autonome Fahren bei bestimmten dynamischen Ereignissen wie z. B. Arbeitsstellen einschränken. Dazu verfügt BEA über eine Schnittstelle zum Control Center. Nachdem im Rahmen von ATLAS-L4 das Konzept erarbeitet, BEA implementiert und der Datenaustausch mit dem Control Center umgesetzt und erfolgreich erprobt wurde, wird BEA nun von der Autobahn GmbH weiterentwickelt und auf einen zukünftigen Regelbetrieb vorbereitet.

Die wissenschaftliche Verwertbarkeit der ATLAS-L4 Ergebnisse zeigt sich in der unmittelbaren Nutzbarkeit der Projektinhalte in Forschung und Lehre der beteiligten Forschungspartner. Die ganzheitliche Betrachtung eines automatisierten Nutzfahrzeugs – von Software und Hardware über Gesetzgebung bis zu Sicherheitskonzepten – dient als anschauliche Basis für Vertiefungsveranstaltungen, Labore und Abschlussarbeiten und wird zur Weiterentwicklung bestehender Lehrinhalte eingesetzt. Dadurch konnten Lehrveranstaltungen bereits verbessert und an den aktuellen Stand der Wissenschaft und Technik angepasst werden. Als Resultat konnte und kann das Grundwissen der Studierenden in Bezug auf die Entwicklung und das Testen automatisierter Fahrzeuge erweitert werden, sodass ihnen nach Abschluss des Studiums der Anschluss an die in der Industrie verwendeten Werkzeuge und Methoden erleichtert wird. Auf diese Weise wird auch die Industrie durch eine erhöhte Startgeschwindigkeit der Berufseinsteigenden gestärkt.

Erkenntnisse zu Sicherheitskonzepten zukünftiger Fahrzeuge, Selbstwahrnehmung und Fahrdynamikregelung, Control Center und Technischer Aufsicht sowie zu Methoden und Werkzeugen des szenarienbasierten Testens werden auf einschlägigen Fachkonferenzen publiziert und als Referenz für die Serienentwicklung automatisierter Fahrzeuge über Level 3 hinaus nutzbar gemacht. Der Wissenstransfer wird durch die aktive Mitarbeit in nationalen und internationalen Gremien und Verbänden sowie durch die Fortführung gemeinsamer Forschungsvorhaben sichergestellt.

Zudem sind während der Projektlaufzeit verschiedene wissenschaftliche Veröffentlichungen entstanden sowie mehrere Dissertationen geplant, in die die im Projekt ATLAS-L4 gewonnenen Erkenntnisse einfließen werden.

Die Gesamtergebnisse und auch einzelne Teilaspekte des Projekts ATLAS-L4 wurden im Laufe der Jahre 2023-2025 auf diversen Konferenzen / Veranstaltungen vorgestellt, darunter:

- escar Europe 2023, 15./16. November 2023 in Hamburg
- NeurIPS 2024, 10.-15. Dezember 2024 in Vancouver, Kanada
- VDI Autonomous Trucks, 12./13. März 2025 in Düsseldorf
- Safe.tech, 20./21. Mai 2025 in München
- Chassis.tech, 03./04. Juni 2025 in München
- VDI Nutzfahrzeuge, 04./05. Juni 2025 in Celle
- IEEE Intelligent Vehicles Symposium, 22.-25. Juni 2025 in Cluj, Rumänien
- IEEE ETFA 2025, 09.-12. September 2025 in Porto, Portugal
- IAA Mobility, 09.-14. September 2025 in München
- IEEE International Conference on Systems, Man, and Cybernetics (SMC 2025), 05.-08. Oktober in Wien, Österreich
- Bayern Innovativ Fachtagung autonomes und vernetztes Fahren, 07.10.2025 in Ingolstadt
- TUM/TÜV SÜD Automatisiertes Fahren, 19./20. November 2025 in Erding

# 5 Quellenverzeichnis


[1] M. Loba, N. F. Salem, M. Nolte, A. Dotzler, D Ludwig, D. und M. Maurer (2025), „Towarda Harmonized Approach - Requirement-based Structuring of a Safety Assurance Argumentation for Automated Vehicles “, Vorveröffentlichung (zur Veröffentlichung angenommen in 2025 IEEE 28th International Conference on Intelligent Transportation Systems (ITSC), Broadbeach, Australien, 18.-21. November), https://arxiv.org/abs/2505.03709

[2] M. Loba, und K. Lamm. (2025), „Towards a Safety Argumentation for a Driverless Truck“, Vortrag, 8th International VDI Conference „Autonomous Trucks“, 12.-13. März 2025, Düsseldorf, Deutschland.

[3] D. Angermeier et al, (2023), “Security Risk Assessments: Modeling and Risk Level Propagation”, ACM Transactions on Cyber-Physical Systems, Volume 7, Issue 1, https://doi.org/10.1145/356945

[4] P. Wagner et al. (2025), „Cross-Divisional Cybersecurity Risk Management in Automotive: Requirements and Current Practices”, IEEE 30th International Conference on Emerging Technologies and Factory Automation (ETFA), 09.-12. September 2025, Porto, Portugal, doi: 10.1109/ETFA65518.2025.11205792

[5] S. Tatschner (2025), “Towards a More Sustainable and Secure Software Tooling in Free/Libre Open Source Software Environments”, Submitted to the University of Limerick for the degree of Philosophie Doctor (PhD)

[6] N. F. Salem, M. Nolte, V. Haber, T. Menzel, H. Steege, R. Graubohm und M. Maurer (2024), „An Ontology-Based Approach Toward Traceable Behavior Specifications in Automated Driving“, IEEE Access, Bd. 12, S. 165203–16226, doi: 10.1109/ACCESS.2024.3494036.

[7] M. Nolte (2025), „Werte- und fähigkeitsbasierte Bewegungsplanung für autonome Straßenfahrzeuge – Ein systemischer Ansatz“, Dissertation Technische Universität Braunschweig, Braunschweig, 2024.

[8] F. Grün, M. Nolte und M. Maurer, (2024) „Towards Scenario- and Capability-Driven Dataset Development and Evaluation: An Approach in the Context of Mapless Automated Driving“, in 2024 IEEE Intelligent Vehicles Symposium (IV), S. 2176–2183. doi: 10.1109/IV55156.2024.10588871.

[9] N. F. Salem, T. Kirschbaum, M. Nolte, C. Lalitsch-Schneider, R. Graubohm, J. Reich und M. Maurer (2024), „Risk Management Core—Toward an Explicit Representation of Risk in Automated Driving“, IEEE Access, Bd. 12, S. 33200–33217, doi: 10.1109/ACCESS.2024.3372860.

[10] N. F. Salem, M. Nolte, R. Graubohm, O. Franke, T. Schenkel und M. Maurer (2025), „Towards a Model-based Approach for Behavioral Safety Concepts in Automated Driving“, Veröffentlichung ausstehend.

[11] A. Ahlbrecht, N. F. Salem, L. Putze, I. Stierand, U. Durak, M. Nolte und E. Böde (2025). “Tailoring STPA for SOTIF: Terminology, Mapping and Methodological Extension". In: IEEE Access. Submitted for publication.

[12] R. Graubohm (2026), „Beitrag zur Entwicklung von Sicherheitskonzepten im Entwurf automatisierter Fahrsysteme“, Dissertation, Technische Universität Braunschweig, Braunschweig, eingereicht.

[13] M. Scholtes, L. Westhofen, L. R. Turner, K. Lotto, M. Schuldes, H. Weber, N. Wagener, C. Neurohr, M. H. Bollmann, F. Kortke, J. Hiller, M. Hoss, J. Bock und L. Eckstein (2021), „6-layer model for a structured description and categorization of urban traffic and environment," IEEE Access, Bd 9, S. 59131–59147, , doi: 10.1109/ACCESS.2021.3072739

[14] T. Kerbl et al. (2025), “TUM Teleoperation: Open Source Software for Remote Driving and Assistance of Automated Vehicles," 2025 IEEE Intelligent Vehicles Symposium (IV), Cluj-Napoca, Romania, pp. 2593-2600 , doi: 10.1109/IV64158.2025.11097531

[15] G. Kaljavesi, T. Kerbl, T. Betz, K. Mitkovskii und F. Diermeyer (2024), "CARLA-Autoware-Bridge: Facilitating Autonomous Driving Research with a Unified Framework for Simulation and Module Development," 2024 IEEE Intelligent Vehicles Symposium (IV), Jeju Island, Korea, Republic of, S. 224-229 , doi: 10.1109/IV55156.2024.10588623.

[16] N. Merkel, S. Gary, C. Maag und A. Neukum (2025), Human Factors in der Teleoperation – Potenziale des Simulators als Untersuchungs- und Trainingswerkzeug, Workshopbeitrag, safe.tech Tagung des TÜV Süd, München, 20.-21.05.2025.

[17] D. Brecht et al (2024)., "Evaluation of Teleoperation Concepts to Solve Automated Vehicle Disengagements," in IEEE Open Journal of Intelligent Transportation Systems, Bd. 5, S. 629-641, , doi: 10.1109/OJITS.2024.3468021.

[18] C. Maag, S. Gary, N. Merkel und A. Neukum (2025), “Studying Effects of Up- and Downlink Latency on Remote Driving Using Teledriving Simulation", 2025 IEEE Intelligent Vehicles Symposium (IV), Cluj-Napoca, Romania, S. 1321-1326 , doi: 10.1109/IV64158.2025.11097757.