Engineering und Software-Entwicklung

ÖV-LeitmotiF-KI

Funktionales Sicherheitskonzept (FSK)

Gültigkeitsbereich (Projekt)	ÖV-LeitmotiF-KI **Förderkennzeichen: 45AVF3004B**
Erzeugnis (Work Product)	Functional Safety Concept ISO-26262-03:2018 Clause 7.5.1 → 7.4.1 to 7.4.3
Dokumentenklassifikation	öffentlich (Förderprojekt)
Autor	Michael Oettelt Projektleiter Mobile: +49 (151) 1207 1278 michael.oettelt@ese.de
Reviewer	Mandy Steinberg Integration & Validation Business Unit Safety & Security mandy.steinberg@ese.de
Freigeber	Prof. Dr.-Ing. habil. Lars Schnieder Chief Executive Officer (CEO) Telefon: +49 531 23880-30 lars.schnieder@ese.de Paul Bethge Digital unterschrieben von Paul Bethge Datum: 2024.07.05 11:49:00 +02'00'

Dokumentenversion und Status:

Aktuelle Fassung	Version 1.0	27.06.2024 21:43	freigegeben

Dokumentenhistorie:

Version	Datum	Status	Änderung (Kapitel + Bearbeiter)
0.1	27.11.2023	Entwurf	Initiale Fassung unvollständig. Ausleitung für Konsortialtreffen 28/29.11.2023 Michael Oettelt
0.2	04.02.2024	Entwurf	Vervollständigung der initialen Fassung. Verantwortungshandshake BHMS zu ÖV-Leitstelle (innerhalb versus außerhalb) des Betriebshofes ergänzt. Erhöhung des Detaillierungsgrades mit Ergänzung einer Kurzbeschreibung der Verantwortung/Zuständigkeit pro Organisationseinheit mit der zugehörigen Sicherheitsrelevanz in einer Matrix (Kapitel 3.2) Michael Oettelt
0.3	20.02.2024	im Review	Einarbeitung Review Befunde ESE Michael Oettelt
0.4	27.06.2024	Reviewed	Einarbeitung Review Befunde / Wünsche aus dem Konsortium Michael Oettelt
1.0		Freigabe	Freigabe durch GF

Inhaltsverzeichnis

1 Einleitung 4
1.1 Gültigkeitsbereich 4
1.2 Zielsetzung 4
1.3 Mitgeltende Dokumente 6
1.4 Begriffe 7
2 Methodik 8
2.1 Anforderungsmanagement 8
2.1.1 Juristische Anforderungen 10
2.1.1.1 Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV) 10
2.1.1.2 Anforderungen aus der Verordnung über den Bau und Betrieb der Straßenbahnen (BOStrab) 21
2.1.1.3 Anforderungen aus der Eisenbahn-Bau- und Betriebsordnung (EBO) 22
2.1.1.4 Produkthaftung 22
2.1.1.5 Betreiberhaftung 22
2.1.2 Anforderungen aus Normen und Standards 23
2.1.2.1 Anforderungen an Sicherheitsanforderungen gemäß ISO-26262:2018 23
2.1.2.2 Anforderungen an Sicherheitsanforderungen gemäß ISO-21448 25
2.2 Metriken 28
2.2.1 Bewertung per Risikograph (VDV-Schrift-161) 28
2.2.2 Freigabelevel 29
2.3 Schutz vor dem unberechtigten Zugriff Dritter (Security) 30
2.3.1 Anforderungen der Datensicherheit 31
2.3.2 Datensicherheit durch Schutzmechanismen 32
2.3.3 Sicherheitszonen 34
3 Ableitung der funktonalen Sicherheitsrelevanz 36
3.1 Analyseobjekt (Referenzmodell) 36
3.2 Use Cases 37
3.2.1 UC-01 Fahrzeug aufrüsten 38
3.2.2 UC-02 Umlaufanmeldung/-zuweisung 44
3.2.3 UC-03 Leerfahrt 48
3.2.4 UC-04 Fahrgastfahrt 55
3.2.5 UC-05 Regelhalt 62
3.2.6 UC-06 Türkontrolle 66
3.2.7 UC-07 Fahrzeug abrüsten 71
3.2.8 UC-08 Datenaktualisierung 77
3.2.9 UC-09 Datenentsorgung 82
3.2.10 UC-10 Fahrgastzählung 85
3.2.11 UC-11 Stauerkennung 87
3.2.12 UC-12 Systemüberwachung und ggf. Störmeldung 89

3.2.13 UC-13 Fahrtänderung 99
3.2.14 UC-14 Umlaufänderung 104
3.2.15 UC-15 Neuen Umlauf hinzufügen 109
3.2.16 UC-16 Neue Fahrplandaten aufgrund dispositiver Maßnahmen verteilen 113
3.2.17 UC-17 Anschlußbeziehungen aktualisieren und darstellen 118
3.2.18 UC-18 Zielbeschilderung außen und innen ändern 120
3.2.19 UC-19 Liniennummer ändern 122
3.2.20 UC-20 Fahrgäste akustisch informieren 124
3.2.21 UC-21 Fahrgäste textuell informieren (Tickertext) 126
3.2.22 UC-22 Problem mit Fahrgast (störendes Verhalten) 128
3.2.23 UC-23 Kommunikation mit Fahrgästen bei außergewöhnlichen Ereignissen 135
3.2.24 UC-24 Fundsachen und Sauberkeit im Fahrzeug 143
3.2.25 UC-25 Waschvorgang 147
3.2.26 UC-26 Lademanagement 151
3.2.27 UC-27 Ersatzfahrzeug bereitstellen 154
3.2.28 UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA) 157
3.2.29 UC-29 Temporäre Sensorbeeinträchtigung 163
3.2.30 UC-30 Fehler in der Selbstpositionierung 166
3.2.31 UC-31 Entscheidungshilfe (Fahrtfortsetzung) 171
3.2.32 UC-32 Detektion von Trajektorien Abweichung 176
3.2.33 UC-33 Interpretation des fahrzeuginternen Systemzustandes 181
3.2.34 UC-34 Interpretation des Gesamtsystemzustandes zwischen Infrastruktur/Leitstelle und Fahrzeug 186
3.2.35 UC-35 Detektion von Abweichungen in Sensordaten zwischen Fahrzeug und Infrastruktur 189
3.2.36 UC-36 Detektion und Rückmeldung übertreten der Operativen Design Domain (Kartierung, Wetter, Geschwindigkeit) 191
3.2.37 UC-37 Bereitstellen von Verhaltensinformationen an AD-Leitstelle zum späteren System Lernen 194
3.2.38 UC-38 Lernen von Verhalten im Störfall aus früheren Fahrsituationen, die von der AD-Leitstelle begleitet wurden 197
3.2.39 UC-39 Ausgestaltung der AD-Leitstelle für die Technische Aufsicht (TA) 201
3.2.40 UC-40 Nothalt 205
3.2.41 UC-41 Fahrzeug dauerhaft unerreichbar 217
3.2.42 UC-42 Parameter für LSA Beeinflussung setzen 222
3.2.43 UC-43 Parken 224
3.2.44 UC-44 Fahrt im Depot 226
3.2.45 UC-45 MissionCtrl 234
3.3 Anforderungen zur Absicherung der operativen Situationen (Use Cases) 236
3.3.1 Zuordnung der Verantwortlichkeit mit Sicherheitsrelevanz (Matrix) 236
3.3.2 Das Autonomous Drivable Object (ADO) 256
3.3.2.1 Systembild 256
3.3.2.2 Regelkreis der Systems Theoretic Process Analysis (STPA) 256
3.3.3 Sicherheitsziele / Safety Goals (SG) 257
3.3.4 Sicherheitsmaßnahmen 257
3.3.4.1 Kategorien der Sicherheitsmaßnahmen 257
3.3.4.1.1 Sicherheitsmaßnahme Funktional (SiMF) 257
3.3.4.1.2 Sicherheitsmaßnahme Technik (SiMT) 258
3.3.4.1.3 Sicherheitsmaßnahme Qualitätssicherung (SiMQ) 258
3.3.4.1.4 Sicherheitsmaßnahme Herstellung (SiMH) 258
3.3.4.1.5 Sicherheitsmaßnahme Wartung (SiMW) 259
3.3.4.1.6 Sicherheitsmaßnahme Sicherheitsfahrer (SiMSiF) 259

Abbildungsverzeichnis

Abbildung 1 Das ÖV-LeitmotiF-KI Konsortium mit der Verteilung der Arbeitspakete gemäß GVB 4
Abbildung 2 Hierarchisch strukturierte Sicherheitsanforderungen eigene Darstellung angelehnt an ISO-26262-03:2018 Figure 2 23
Abbildung 3 Bewertung per Risikograph (Metrik) 28
Abbildung 4 Systembild von einem automatisierten / autonomen Fahrzeug 32
Abbildung 5 Referenzarchitektur, aktualisiert durch die Schnittstelle 20, basierend auf Referenzmodell. 36
Abbildung 6 Kammscher Kreis 102
Abbildung 7 Ablauf vor dem Ausrücken 226
Abbildung 8 Autonomous Drivable Object (ADO) mit optionalen Tuning-Kits 256
Abbildung 9 Regelkreis von einem autonomen Fahrzeug (ADO) mittels Systems Theoretic Process Analysis (STPA) 256

1 Einleitung

Der Einsatz autonomer Fahrzeuge im Öffentlichen Verkehr (ÖV) erfordert ihre organisatorische und technisch standardisierte Integration in die betrieblichen Prozesse des Verkehrswesens um einen diskriminierungsfreien Marktzugang für alle Anbieter, sowohl in ländlichen Regionen als auch in Ballungsräumen, flexibel für die Fahrgäste zu gestalten.

Präambel

Aus Gründen der besseren Verständlichkeit wird auf die multigeschlechtliche Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Bezeichnungen gelten gleichermaßen für jede Geschlechtsform.

Hinweis:
Der Motor / Die Motoren / Das Motörchen.

1.1 Gültigkeitsbereich

Dieses funktionale Sicherheitskonzept (FSK) betrachtet die Operationen (UseCases) und das Zusammenspiel der der ÖV-Leitstelle (Öffentlicher Verkehr), sowie der AD-Leitstelle (engl. Autonomous Driving ≙ **A**utonome **D**urchtriebfunktionsüberwachung) mit dem Fahrzeug auf Basis des Referenzmodells des Projektes ÖV-LeitmotiF-KI im autonomen Betrieb.

Hinweis: Das Referenzmodell ist abgebildet im Kapitel Analyseobjekt.

Das Konsortium besteht aus Partnern der Forschung, Industrie und Verkehrsunternehmen stellt sich vor unter https://bmdv.bund.de/SharedDocs/DE/Artikel/DG/AVF-projekte/oev-leitmotif-ki.html oder https://www.vdv.de/leitmotif-ki.aspx.

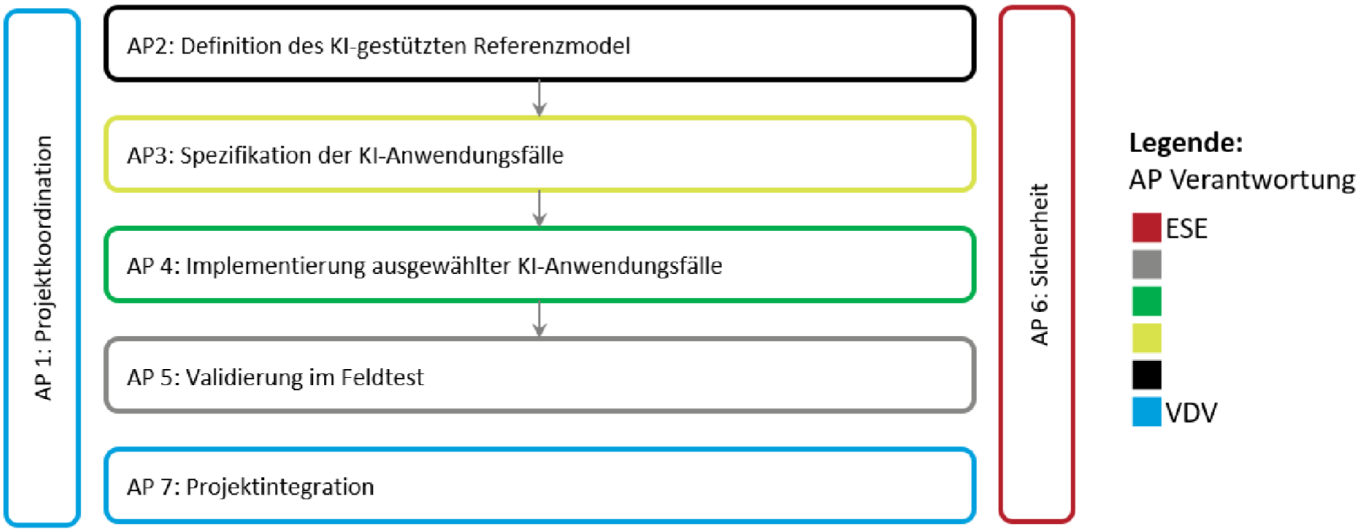


Abbildung 6: Abhängigkeiten und Verantwortlichkeiten in den Arbeitspaketen

Abbildung 1 Das ÖV-LeitmotiF-KI Konsortium mit der Verteilung der Arbeitspakete gemäß GVB

1.2 Zielsetzung

Im Rahmen des Projektes ÖV-LeitmotiF-KI soll ein funktionales Sicherheitskonzept zur Erreichung der Gesamtsystemsicherheit unter Einbindung von KI in die betrieblichen Prozesse definiert werden.

Hierbei wird von einem sicheren und den gesetzlichen Vorgaben erfüllenden Fahrzeug (OEM) ausgegangen. Gleiches gilt für die eingesetzten Komponenten / Elemente (ÖV-Bordrechner / AD-Bordsystem) inklusive der zugehörigen Peripherie (z.B. Kamera, Mikrophone, Datenaufzeichnung oder auch Linienanzeiger), welche eigenständig vom Produkt-Inverkehrbringer (Hersteller), eigenverantwortlich über ein zugehörigen Sicherheitsnachweis in den Markt gebracht werden.

Insofern gibt es im Rahmen des Projektes keine Produktherstellung und damit keine Freigabelevel aus dem Produktentstehungsprozeß (PEP).

Die Anforderungen an die Technische Aufsicht (TA) der AD Leitstelle werden aus Sicht des Halters (ÖPNV) betrachtet. Da diese Geschäfts-Prozesse jedoch diskriminierungsfrei der direkten Verantwortung des ÖPNV-Unternehmens obliegen, muß das Unternehmen auch frei sein bei der Auswahl der Strategie zur Erstellung des Sicherheitsnachweises.

Das Funktionale Sicherheitskonzept (FSK) benennt (referenziert) Methoden, welche zur Erstellung von Sicherheitsnachweisen angewendet werden können und bildet über die Strategie heraus, welche Methodik zu welchem Freigabelevel, als geeignet ausgewählt wurde.

Gefahren resultieren aus der (bewußten) Nutzung von Objekten sowie von vorhandenen Elementen der Umgebung. Die Gefährdung resultiert aus den Energien ($W_{kinetisch}$, $W_{Potential}$, …) der Objekte.

Gefährdungen sind durch geeignete (Gegen-)Maßnahmen zu vermeiden, oder sofern dieses nicht realistisch möglich sein sollte, angemessen abzumildern.

Die Absicherung folgt den typischen Sicherheitsanforderungen, welche in der ISO-26262-03:2018 Clause 7.4.2.3 ff vorgegeben sind. Der Ablauf, der im Projekt spezifizierten Use Cases, erfolgt in atomarer Schreibweise im Block „Aktionen“ des jeweiligen Use Cases im Kapitel 3.2 Use Cases.

Neben den Anforderungen der Sicherheit (Safety) gibt es auch noch Anforderungen vom Betriebsschutz (Security), auf welche im Kapitel 2.3 Schutz vor dem unberechtigten Zugriff Dritter (Security) eingegangen wird.

1.3 Mitgeltende Dokumente

- Automotive SPICE®
  https://www.automotivespice.com
- Bundesdatenschutzgesetz (BDSG)
  https://www.gesetze-im-internet.de/bdsg_2018
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen
  Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2023-01.
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=6
- Bundesministerium für Digitales und Verkehr (BMDV)
  Bericht der Ethik-Kommission – Automatisiertes und Vernetztes Fahren
  https://www.bundesregierung.de/breg-de/service/publikationen/bericht-der-ethik-kommission-729110
- DIN EN ISO-7010:2011
  Graphical Symbols – Safety Colours and Safety Signs – Registered Safety Signs (Rettungszeichen)
  https://www.iso.org/standard/54432.html
  https://commons.wikimedia.org/wiki/Category:ISO_7010_safe_condition_signs?uselang=de
- DIN EN IEC 62443-3-3 (VDE 0802-3-3) System Security Requirements and Security Levels
  https://www.vde-verlag.de/normen/0800628/din-en-iec-62443-3-3-vde-0802-3-3-2020-01.html
- DIN 72552 Klemmenbezeichnungen
  https://de.wikipedia.org/wiki/Klemmenbezeichnung
- ISO/SAE 21434:2021 Road Vehicles – Cybersecurity Engineering
  https://www.iso.org/standard/70918.html
- ISO-21448:2022 Road vehicles – Safety of the intended functionality (SOTIF)
  https://www.iso.org/standard/77490.html
- ISO-26262-04:2018 Road Vehicles – Functional Safety
  https://www.iso.org/standard/43464.html
- ISO-22900 = Road Vehicles – Modular vehicle communication interface (MVCI)
  https://www.iso.org/standard/41275.html
- Minimum Risk Manoeuvre (MRM)
  https://wiki.unece.org/download/attachments/27459841/ACSF-04-07_(D) - ACSF-MRM.pdf?api=v2
- Personenbeförderungsgesetz (PBefG)
  https://www.gesetze-im-internet.de/pbefg/BJNR002410961.html
- Straßenverkehrs-Ordnung (StVO)
  https://www.gesetze-im-internet.de/stvo_2013/BJNR036710013.html
- Straßenverkehrs-Zulassungs-Ordnung (StVZO)
  https://www.gesetze-im-internet.de/stvzo_2012/BJNR067910012.html
- United Nations Regulation R155e
  (Cyber Security And Cyber Security Management System)
  https://unece.org/sites/default/files/2021-03/R155e.pdf
- Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO)
  Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten
  https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679
- Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen (Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung - AFGBV)
  https://www.gesetze-im-internet.de/afgbv/AFGBV.pdf
- Verordnung über den Betrieb von Kraftfahrunternehmen im Personenverkehr (BOKraft)
  https://www.gesetze-im-internet.de/bokraft_1975/BOKraft.pdf.

Die Auflistung erhebt keinen Anspruch auf Vollständigkeit.

1.4 Begriffe

- Allgemeine Begriffe aus der Technik
  - ADO Autonomous Drivable Object (ADO)
    SAE ≥4, es gibt keinen Sicherheitsfahrer im Fahrzeug, die Verantwortung (Haftung) obliegt dem Fahrzeughersteller (OEM).
    Hinweis:
    SAE-J3016™ Surface Vehicle recommended practice Kapitel 7.1.1 (%)
    - *Some driving automation systems may indeed be autonomous if they perform all of their functions independently and self-sufficiently,*
    - *but if they depend on communication and/or cooperation with outside entities, they should be considered cooperative rather than autonomous → automation.*
  - ADS Autonomous Driving System (ADS)
  - ASIL Automotive Safety Integrity Level (ASIL)
  - RDS Remote Driving System (RDS)
    Hinweis:
    Nicht Radio Broadcast Data System (RBDS) USA → Radio Data System (RDS) Europa ≙ UKW.
  - SECU sichere elektronische Steuereinheit (SECU)
    Safe Electronic Control Unit (SECU)
  - VMC Vehicle Motion Controller
  - VRU Vulnerable Road User (VRU) ≙ verwundbarer Verkehrsteilnehmer
- Cybersecurity
  - BSI Bundesamt für Sicherheit in der Informationstechnik (BSI)
    https://www.bsi.bund.de/DE/Home/home_node.html
  - CERT Computer Emergency Response Team (CERT)
  - CSIRT Cyber Security Incident Response Team (CSIRT)
  - CVE® Common Vulnerabilities and Exposures (CVE®)
  - NIST National Institute of Standards and Technology (NIST)
    http://csrc.nist.gov
  - NVD National Vulnerability Database (NVD)
    https://nvd.nist.gov
  - SVM Software Vulnerability Management (SVM)
- Fahrzeugkommunikation
  - C2C Kommunikation Fahrzeug (Car) zu Fahrzeug (Car) = Fahrzeugverbund / Platoon
  - C2I Kommunikation Fahrzeug (Car) zu Infrastruktur
  - C2X Kommunikation Fahrzeug (Car) zu Allen
- Sonstiges
  - 🗎 Kennzeichen Dokument / Dokumentenreferenz, kennzeichnet eine Quellenangabe
  - % prozentual → anteilig (Auszugsweise ggf. paraphrasiert)
  - AD (engl. Autonomous Driving) ≙ Autonome Durchtriebfunktion
  - BMJ Bundesministerium der Justiz
  - OEM Original Equipment Manufacturer (OEM) ≙ Original- / Initial- / Erstausrüster
  - ÖV Öffentlicher Verkehr
  - ÖPNV Öffentlicher Personennahverkehr
- Verantwortung (Rollen) → siehe auch 20230330_Deliverable_MS2_Referenzmodell.docx Tabelle 3.
  - Betriebshof Management System (BHMS)
    Das BH-Personal ist der menschliche Operator = Bestandteil vom Betriebshofmanagementsystem, welches dem Menschen die Aufgaben zuweist. → BHMS-Mission ≡ BH-Mission, BHMS-Mitarbeiter ≡ BH-Mitarbeiter, BHMS-Umlauf ≡ BH-Umlauf.
  - Fahrgastinformation (FGI)
  - Fahrgast-Notfallmanagement (FG-NFM)
  - Technische Aufsicht (TA) *gemäß AFGBV*
  - Technische Aufsichtsbehörde (TAB) *gemäß BOStrab*

Die Auflistung erhebt keinen Anspruch auf Vollständigkeit.

Legende der Schriftfarben:	
Blau	Referenz / Link innerhalb des Dokumentes
Hellblau	Hervorhebung für das Querlesen (wesentliche Begrifflichkeit)
Rot	Hervorhebung Verneinung / Vermeidung ODER Einschränkung / Randbedingung
Orange	Projektmanagementrelevanz (Randbedingung der Entscheidungsfindung / Abgrenzung)
Violett	Zusatzinformation 1st-Level
Grau	Zusatzinformation 2nd-Level

Zusatzinformationen / Hinweise werden historisch bedingt kursiv dargestellt für schwarz/weiß-Ausleitungen.

2 Methodik

2.1 Anforderungsmanagement

Das Funktionale Sicherheitskonzept (FSK) ist eine Spezifikation, welche gemäß dem Prozeß Anforderungsmanagement erstellt wird. Die Spezifikationen werden über die Ebenen des V-Models von oben nach unten verfeinert und gemäß ihren Abhängigkeiten verlinkt. Die Umsetzung erfolgt typisch über Datenbanken (Tools, wie z.B. DOORS, Codebeamer, Polarion), worüber eine verifizierbare Traceability sichergestellt werden kann.

Dazu werden Anforderungen zerschnitten (in kleine Teilstücke zerlegt) gemäß dem Abholenden (Ausführender / Umsetzender), dadurch können unvollständige oder auch sinngemäß ergänzte Texte vorkommen. Die Zielsetzung hierbei ist es eine effizient, nachvollziehbare Verlinkbarkeit zu erhalten.

Dabei findet auch eine Attribuierung statt, d.h. die Texte werden nach Ihren Eigenschaften strukturiert.
Es gibt (typisch):

- Überschriften
- Informationen, *z.B. Zielsetzung oder Hinweise, sowie Referenzen*.
- Definitionen
- Funktionale Anforderungen
- Quantitative Anforderungen
- Randbedingungen
- Designempfehlungen
- Entwurfsentscheidungen
- Funktionale Architekturbeschreibungen
- Quantitative Architekturbeschreibungen

Anforderungen haben einen Identifier (Datenbank-ID, typisch mit einem Präfix des Ursprungs, wodurch die Gültigkeit erkannt werden kann), weshalb dieser stets am Anfang platziert ist. Diese ID fungiert als Referenzanker.

Im Projekt ÖV-LeitmotiF-KI existieren solche Tools nicht, stattdessen werden Dokumente mit Office erstellt, weshalb diese Inhalte (Texte) händisch multiple Male zu kopieren sind, welches sonst über die toolgestützte Verlinkung (Referenzen) mittels einer Datenbank umgesetzt (systematische angezeigter Text in Form von verlinktem Inhalt) wird.

Das Kopieren hat den Zweck der Informationsweitergabe, damit es bei den verschiedenen zu erstellenden Arbeitspaketen Anwendung findet, sowie um gleichzeitig ein gemeinsames, konsistentes Wissen zu etablieren, welches sich in der Implementierung wiederfindet.

Jede Anforderung wird von verschiedenen Reviewteilnehmerkreisen verifiziert und validiert. Dazu zählen Entwickler der Funktion, der System- und Bauteilebene, ebenso wie die Ingenieure der Funktionalen Sicherheit, der FMEA-Analyse, die Tester der einzelnen Testebenen insbesondere Testobjektverantwortliche (TOV), verantwortlich auf der systemübergreifenden Bauteilebene, und der Systemtestmanager (STM), bauteilübergreifend verantwortlich für ein System / Fahrzeug.

Folglich gibt es eine hohe Anzahl von Mitwirkenden, häufig >100 bei einer einzelnen Funktion, wie z.B. der Querdynamik (Lenkung), welche sich über das Anforderungsmanagementsystem (Applikation/Datenbank/Tool) zeitversetzt arbeitend austauschen und sich abstimmen. Dabei ist es irrelevant, wer, wann, was beigetragen hat. Die Spezifikation gehört dem auftraggebenden Unternehmen, welche das exklusive Nutzungsrecht hat.

Es ist absolut irrelevant welcher Mitarbeiter, ob intern oder extern, welchen Beitrag geleistet hat. Auch die Namen der Auftragausführenden Unternehmen wird nicht explizit dokumentiert. Es gibt keine Autoren oder Co-Autoren-Liste.

Spezifikationen sind kein Buch, wo Referenzen an der Stelle der Anwendung zitiert werden, stattdessen gibt es weitere Anforderungsdokumente, welche diese Quellen über den Identifier, die Präfix-ID, abbilden, d.h. z.B.

3.19

identifier

language-independent data string or pointer that establishes the identity of its association, alone or in combination with other elements

Note 1 to entry: This is a generalized definition of ISO 5127:2017, 3.1.12.19.

- Referenz auf eine Norm:
  ISO-26262-03:2018 Clause 7.5.1 Functional Safety Concept (FSC) → 7.4.1 to 7.4.3,
  [Inhalt, ggf. zerlegt (teilweise / Auszug), paraphrasiert (umformuliert, jedoch inhaltlich identisch), sofern erforderlich inhaltlich erweitert, fokussiert oder vereinfacht, sowie ggf. in andere Sprachen übersetzt]

  Bedeutung:
  Dokument / Dokumentenreferenz *bezogen auf die nachfolgend benannte Quelle*
  ISO-26262-03:2018 Clause 7.5.1
  → ISO-26262 *ist eine Norm*,
  → -03 *ist der Band aus der zuvor genannten Norm (eine Norm kann mehrere Bände beinhalten)*,
  → :2018 *ist die Version des zuvor genannten Bandes der Norm*,
  Clause → der Absatz / Satz oder auch Abschnitt / Kapitel, ggf. mit Ziffer bzw. Aufzählungspunkt
  7.5.1 → ist das Kapitel mit dem Namen „Functional Safety Concept“ *paraphrasiert und erweitert um die Abkürzung „(FSC)“*,
  welches durch das Symbol „→“ weiterleitet (referenziert) auf die Kapitel 7.4.1 to 7.4.3, *in dem gleichen Band der zuvor genannten Norm*.

  Beispiel:
  Die Anforderungen aus der 7.4.x lauten und werden umgesetzt,
  (in diesem Dokument) siehe Anforderungen an Sicherheitsanforderungen gemäß ISO-26262:2018.

  Beispiel:
  Die Anforderungen werden aus dem Englischen übersetzt und inhaltlich adaptiert *(fokussiert und vereinfacht)*.

  - Sofern die Verletzung eines Sicherheitszieles vermieden werden kann, durch den Übergang / Wechsel in einen anderen Betriebs- oder Wartungszustand, dann muß diese Spezifikation angewendet werden.
    ISO-26262-03:2018 Clause 7.4.2.5
    If a safety goal violation can be prevented by transitioning to, or by maintaining, one or more safe states, then the corresponding safe state(s) shall be specified.

  Für den ungeübten Leser mag dieses wie ein Übersetzungsfehler aussehen, ist es aber nicht.
  Die Vorgabe ist, daß ein entsprechender / dazu gehöriger / dazu passender (corresponding) sicherer Zustand zu spezifizieren ist, welches in der zugehörigen Spezifikation umzusetzen ist. Diese Spezifikation ist auf der funktionalen Ebene das Funktionale Sicherheitskonzept (FSK) = dieses Dokument.

- Referenz auf eine juristische / vertragliche Anforderung:
  Die Quellen von Textelementen werden über den Präfix (Attribut) gekennzeichnet, die klassische Zitierung ist hierbei als eine Anforderung vom Typ Information in der Spezifikation (im Tool, z.B. DOORS) eingebunden.

AFGBV-[Nummer] Identifier	Information Typ (Attribut)	Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen (Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung - AFGBV) https://www.gesetze-im-internet.de/afgbv/AFGBV.pdf Ausfertigungsdatum: 24.06.2022 [Das Dokument (pdf) wird hier als embedded Element oder im Dokumenten Management System (DMS) abgelegt und hier verlinkt], deshalb keine Angabe im Format: [zuletzt aufgerufen am dd.mm.jjjj um hh:mm:ss] *Deshalb auch keine Angabe zum Autor, ISBN oder …* *das steht unverändert im Dokument (embedded / im DMS).* *Hinweis:* *Das Tool / die Applikation speichert das Erstelldatum mit Uhrzeit automatisch bei der Erstellung, außerdem wird jegliche Änderung dokumentiert.*

Schreibweise von Anforderungen (Beispiel)

Anforderung:
- AFGBV Anlage 1 Teil 1 Abschnitt 5.1 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur dynamischen Ausübung der Fahraufgabe gilt:
  a) Zur dauerhaften Überwachung der technischen Ausrüstung werden nicht personenbezogene technische Daten im Kraftfahrzeug erhoben und gespeichert.
  b) Eine Beeinträchtigung der technischen Ausrüstung ist der Technischen Aufsicht unverzüglich anzuzeigen.

Original (Quelle):

5. Dauerhafte Selbstüberwachung
Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muss vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, dass eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.

5.1 Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur dynamischen Ausübung der Fahraufgabe gilt:

a) Zur dauerhaften Überwachung der technischen Ausrüstung werden nicht personenbezogene technische Daten im Kraftfahrzeug erhoben und gespeichert.

b) Eine Beeinträchtigung der technischen Ausrüstung ist der Technischen Aufsicht unverzüglich anzuzeigen.

Fazit:
Klassische Zitierungsregeln sind im Anforderungsmanagement nicht brauchbar, weil die Texte zerschnitten / zerlegt werden, damit diese von der bzw. den Absicherungen (durch Test, Verifikation und Validierung) abgeholt werden können, wobei häufig keine vollständigen Sätze verbleiben, dafür werden diese gerne verständlich für die Zielgruppe umformuliert, welches sich auf jeder Ebene der abholenden Spezifikation wiederholt. Gleichzeitig können die Texte (Anforderungen) in verschiedenen Sprachen verfaßt sein, was insbesondere dann auftritt, wenn eine Absicherung (Test) für mehrere Spezifikationen (Lastenhefte) angewendet wird, welche in verschiedenen Sprachen verfaßt sind, oder wenn der Abholende (Umsetzende) in einem anderen Land beheimatet ist und somit eine andere Sprache benötigen könnte um die Anforderung zu verstehen. Die hohe Anzahl der Autoren und Co-Autoren bzw. ein Autorenverzeichnis würde die Lesbarkeit der teilweise unvollständigen, dafür mehrsprachigen, verschachtelten Texte noch weiter verkomplizieren, so daß für die Verständlichkeit zu wenig bis nichts übrigbleiben würde.

Die Eingangsdokumente zu einem Arbeitserzeugnis (Work Product) werden im Dokument referenziert, in diesem Dokument im Kapitel Analyseobjekt (Referenzmodell), wo auch die projektspezifischen Besonderheiten beschrieben sind.

2.1.1 Juristische Anforderungen

2.1.1.1 Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV)

- AFGBV §1 Absatz 1
  Diese Verordnung ist anzuwenden auf den Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion im Sinne der §§ 1d bis 1h und mit automatisierter oder autonomer Fahrfunktion im Sinne des § 1h des Straßenverkehrsgesetzes.
- AFGBV §3 Absatz 1
  Der Hersteller hat die Betriebserlaubnis für Kraftfahrzeuge mit autonomer Fahrfunktion beim Kraftfahrt-Bundesamt zu beantragen.
- AFGBV §5 Absatz 5
  Die Hersteller und die Halter von Kraftfahrzeugen mit autonomer Fahrfunktion sind verpflichtet
  ► das Kraftfahrt-Bundesamt bei der Durchführung der Marktüberwachungstätigkeiten zu unterstützen und
  ► dem Kraftfahrt-Bundesamt auf Verlangen die für die Marktüberwachung erforderlichen Unterlagen und Informationen sowie andere technische Spezifikationen unentgeltlich bereitzustellen, wobei die Hersteller auf Verlangen auch einen Zugang zu Software und Algorithmen ermöglichen müssen.
- AFGBV §7 Absatz 1
  Kraftfahrzeuge mit autonomer Fahrfunktion dürfen im öffentlichen Straßenraum nur in einem nach Absatz 2 festgelegten und genehmigten Betriebsbereich im Sinne des §1d Absatz 2 des Straßenverkehrsgesetzes betrieben werden.
- AFGBV §7 Absatz 2
  Die Festlegung eines Betriebsbereichs für ein Kraftfahrzeug mit autonomer Fahrfunktion erfolgt durch den Halter des Kraftfahrzeugs. Der nach Satz 1 festgelegte Betriebsbereich bedarf der Genehmigung durch die zuständige Behörde.
- AFGBV §7 Absatz 3
  Die Genehmigung des festgelegten Betriebsbereichs kann gemeinsam für mehrere baugleiche Fahrzeuge erteilt werden, sofern jeweils eine entsprechende Betriebserlaubnis für Kraftfahrzeuge mit autonomer Fahrfunktion nach den vorstehenden Vorschriften vorliegt.
- AFGBV §8 Absatz 1 Punkt 1
  Der Antrag auf Genehmigung eines festgelegten Betriebsbereichs muß enthalten eine Darstellung des als Betriebsbereich festgelegten Streckennetzes für den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion mit Darstellung eines kartographisch umgrenzten Bereichs in geeigneter digitaler Form nach Vorgabe der zuständigen Behörde sowie eine konkrete Beschreibung des Betriebszwecks und der damit verbundenen Betriebsbedingungen.
- AFGBV §8 Absatz 1 Punkt 2
  Der Antrag auf Genehmigung eines festgelegten Betriebsbereichs muß enthalten den Nachweis des Halters, daß die Deaktivierbarkeit der autonomen Fahrfunktion des Kraftfahrzeugs mit autonomer Fahrfunktion im Sinne des § 1e Absatz 2 Nummer 4 bis 9 des Straßenverkehrsgesetzes und die Möglichkeit der Freigabe von Fahrmanövern im Sinne des § 1e Absatz 3 des Straßenverkehrsgesetzes in diesem Betriebsbereich zu jeder Zeit gewährleistet sind.
- AFGBV §8 Absatz 1 Punkt 3
  Der Antrag auf Genehmigung eines festgelegten Betriebsbereichs muß enthalten die Erklärung des Halters, daß die personellen und sachlichen Voraussetzungen nach den §§ 13 und 14 vorliegen.
- AFGBV §8 Absatz 2 Punkt 1
  Der Halter hat mit dem Antrag außerdem vorzulegen die Betriebserlaubnis für ein Kraftfahrzeug mit autonomer Fahrfunktion nach § 4 Absatz 1 sowie in den Fällen des § 4 Absatz 1 in Verbindung mit Absatz 3

ergänzend einen Nachweis über die Feststellung der Gleichwertigkeit der ausländischen Betriebserlaubnis durch das Kraftfahrt-Bundesamt, wobei auch in diesen Fällen § 23 des Verwaltungsverfahrensgesetzes unberührt bleibt.

- AFGBV §8 Absatz 2 Punkt 2
  Der Halter hat mit dem Antrag außerdem vorzulegen jeweils vom Halter oder von den vom Halter nach § 13 Absatz 2 Satz 2 eingesetzten Personen und der Technischen Aufsicht
  a) ein Führungszeugnis zur Vorlage bei einer Behörde und
  b) eine Auskunft aus dem Fahrerlaubnisregister, *und*
- AFGBV §8 Absatz 2 Punkt 3
  Der Halter hat mit dem Antrag außerdem vorzulegen von der Technischen Aufsicht zusätzlich eine Auskunft über Eintragungen aus dem Fahreignungsregister.
- AFGBV §8 Absatz 3
  Die zuständige Behörde kann darüber hinaus weitere Angaben vom Halter verlangen, sofern dies für das Verfahren zur Genehmigung eines festgelegten Betriebsbereichs erforderlich ist.
- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §12 Anforderungen an den Hersteller Absatz 1
  Der Hersteller eines Kraftfahrzeugs mit autonomer Fahrfunktion hat Reparatur- und Wartungsinformationen für das Kraftfahrzeug nach Anlage 3 Nummer 2.3 und 2.6 dieser Verordnung zu erstellen.
- AFGBV §12 Anforderungen an den Hersteller Absatz 1 Punkt 2
  Der Hersteller eines Kraftfahrzeugs mit autonomer Fahrfunktion hat
  ein Sicherheitskonzept zur funktionalen Sicherheit nach Anlage I Nummer 7.2 zu erstellen, und dabei
  a) auf Basis dieses Sicherheitskonzeptes eine Gefährdungsanalyse nach Anlage I Ziffer 7.2.1 durchzuführen,
  b) das Sicherheitskonzept nach Anlage III Ziffer 3 zu dokumentieren,
  c) die Sicherheit der autonomen Fahrfunktion entsprechend dieses Sicherheitskonzepts zu überprüfen und die Sicherheit gegenüber dem Kraftfahrt-Bundesamt nach den Anforderungen nach Anlage I Ziffer 10 nachzuweisen.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 1
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen die Fahrzeugsysteme für die aktive und passive Sicherheit des Kraftfahrzeugs mit autonomer Fahrfunktion regelmäßig überprüft werden.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 2
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß täglich vor Betriebsbeginn eine erweiterte Abfahrkontrolle nach Absatz 7 durchgeführt wird.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 3
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen ab dem Tag der Zulassung zum Straßenverkehr alle 90 Tage eine Gesamtprüfung nach den Vorgaben des Betriebshandbuchs für das Kraftfahrzeug mit autonomer Fahrfunktion durchgeführt wird.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 4
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß die Ergebnisse der Gesamtprüfungen nach Nummer 3 einschließlich einer Beschreibung aller festgestellten Mängel und durchgeführter Instandsetzungen in einem Bericht dokumentiert und dem Kraftfahrt-Bundesamt sowie der zuständigen Behörde auf Verlangen unverzüglich übermittelt werden, sofern dies erforderlich ist.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.

- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 2
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen haben.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 3
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihnen anvertrauten Aufgaben zuverlässig sind; zur Beurteilung ihrer Zuverlässigkeit sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde sowie, bei Einsatz für die Durchführung von Fahrten im manuellen Betrieb, eine Auskunft aus dem Fahrerlaubnisregister vorzulegen; § 8 Absatz 3 gilt entsprechend.
- AFGBV §13 Anforderungen an den Halter Absatz 3
  Der Halter muß sicherstellen, daß Anweisungen zur ordnungsgemäßen Durchführung der Wartungsarbeiten, der Gesamtprüfungen, weiterer Untersuchungen und Fahrten im manuellen Fahrbetrieb vorliegen und daß diese Anweisungen befolgt werden. Die Anweisungen sind zu dokumentieren.
- AFGBV §13 Anforderungen an den Halter Absatz 4
  Berichte über die Durchführung von Wartungsarbeiten, von Gesamtprüfungen und von weiteren Untersuchungen müssen durch den Halter oder die verantwortliche Person unverzüglich schriftlich oder elektronisch erstellt werden. Die Berichte sind zu unterzeichnen. Die Berichte sind zu dokumentieren und vom Halter oder von der für die Technische Aufsicht verantwortlichen Person sechs Monate lang aufzubewahren und nach Ablauf dieser Frist unverzüglich, bei elektronischer Speicherung automatisiert, zu löschen.
- AFGBV §13 Anforderungen an den Halter Absatz 5
  Die Anforderungen zur Dokumentenverwaltung für die Anweisungen nach Absatz 3 und der Berichte nach Absatz 4 müssen dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik wird vermutet, wenn die Vorgaben der ISO 9001:2015 Qualitätsmanagementsysteme – Grundlagen und Begriffe erfüllt werden. Darüber hinaus muß die Dokumentenverwaltung den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 genügen.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.
- AFGBV §13 Anforderungen an den Halter Absatz 7
  Die erweiterte Abfahrkontrolle im Sinne des Absatzes 1 Nummer 2 beginnt mit einer Probefahrt, um die Systeme zu aktivieren. Im Anschluß an die Probefahrt werden folgende Bereiche überprüft:
  - Bremsanlage,
  - Lenkanlage,
  - Lichtanlage,
  - Reifen/Räder,
  - Fahrwerk,
  - sicherheitsrelevante elektronisch geregelte Fahrzeugsysteme sowie die Sensorik zur Erfassung externer und interner Parameter und
  - mechanische Fahrzeugsysteme für die aktive und passive Sicherheit.
- AFGBV §13 Anforderungen an den Halter Absatz 8
  Der Halter hat für das Kraftfahrzeug mit autonomer Fahrfunktion eine Hauptuntersuchung nach Maßgabe der Anlage VIII in Verbindung mit Anlage VIIIa der Straßenverkehrs-Zulassungs-Ordnung zu veranlassen. Die Frist für die Hauptuntersuchung nach § 29 der Straßenverkehrs-Zulassungs-Ordnung beträgt sechs Monate ab dem Zeitpunkt der Zulassung des Kraftfahrzeugs mit autonomer Fahrfunktion.
- AFGBV §13 Anforderungen an den Halter Absatz 9
  Der Halter darf ohne eine Genehmigung nach § 4 Absatz 6 die nachträgliche Aktivierung von automatisierten oder autonomen Fahrfunktionen nicht vornehmen.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach §1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie in der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik, Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik über einen Abschluß verfügt als
  - Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert),
  - Bachelor, Master oder
  - staatlich geprüfter Techniker.

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 2
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie eine entsprechende Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen hat.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 3
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muß, und
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 4
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihr anvertrauten Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes zuverlässig ist.
  Zur Beurteilung der Zuverlässigkeit im Sinne des Satzes 2 Nummer 4 sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde, eine Auskunft aus dem Fahrerlaubnisregister sowie eine Auskunft über Eintragungen aus dem Fahreignungsregister vorzulegen. Sofern in dem Fahrerlaubnisregister mehr als drei Punkte eingetragen sind, ist die Zuverlässigkeit nicht gegeben. § 8 Absatz 3 gilt bezüglich Satz 3 entsprechend.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 2
  Die als Technische Aufsicht eingesetzte natürliche Person darf sich mit Zustimmung des Halters zur Erfüllung ihrer Pflichten weiterer geeigneter natürlicher Personen bedienen, die über mindestens drei Jahre Berufserfahrung im Bereich des Verkehrs- oder Kraftfahrzeugwesens verfügen. Die eingesetzten natürlichen Personen müssen wiederkehrend, mindestens jedoch jährlich beim Hersteller in Bezug auf den Umgang mit dem Kraftfahrzeug sowie wesentliche Veränderungen am Kraftfahrzeug oder der autonomen Fahrfunktion geschult werden. Die Schulung ist mit einer praktischen Prüfung einschließlich der Bewältigung simulierter Betriebsstörungen abzuschließen. Der erfolgreiche Abschluß der Schulung von eingesetzten natürlichen Personen ist von der Technischen Aufsicht zu dokumentieren. Sollen die eingesetzten natürlichen Personen Fahrten im manuellen Fahrbetrieb übernehmen oder Fahrmanöver freigeben, müssen diese Personen eine gültige Fahrerlaubnis besitzen. Die Klasse der Fahrerlaubnis muß der des Fahrzeugs mit autonomer Fahrfunktion entsprechen.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 3
  Befindet sich das Kraftfahrzeug mit autonomer Fahrfunktion im risikominimalen Zustand im Sinne des § 1d Absatz 4 des Straßenverkehrsgesetzes, hat die als Technische Aufsicht eingesetzte natürliche Person eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durchzuführen, bevor sie dessen Beendigung veranlassen darf. Das Ergebnis der Untersuchung ist zu dokumentieren. Wurde der risikominimale Zustand durch einen Defekt am Kraftfahrzeug ausgelöst, muß nach Erreichen des risikominimalen Zustands die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage 1 Nummer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
  Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist ungeachtet der Sätze 1 und 3 das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen. In diesen Fällen erfolgt die Untersuchung der Technischen Aufsicht gemäß Satz 1 im Nachgang des Abtransports auf Grundlage der gespeicherten Fahrdaten.
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV §15 Datenspeicherung Absatz 2
  Die gespeicherten Daten dürfen nur durch das Kraftfahrt-Bundesamt und die zuständige Behörde und nur zum Zweck der Nachprüfung der Erfüllung der Voraussetzungen der Genehmigung und der mit der Genehmigung verbundenen Überwachungspflichten erhoben, gespeichert und verwendet werden.
- AFGBV Anlage 1 Teil 1 Funktionale Anforderungen an Kraftfahrzeuge mit autonomer Fahrfunktion
  Kraftfahrzeuge mit autonomer Fahrfunktion müssen die im Folgenden dargestellten funktionalen Anforderungen erfüllen. Die geforderten Funktionen können vom Hersteller oder vom Halter oder von beiden in einer möglichen, so genannten Testphase des Kraftfahrzeugs mit autonomer Fahrfunktion ohne Fahrgäste im festgelegten Betriebsbereich nachgewiesen werden.
  Hinweis:
  AFGBV Anlage 3 Dokumentationspflichten des Herstellers spezifiziert die Anforderungen zu
  1. Funktionale Beschreibung
  2. Betriebshandbuch
  3. Sicherheitskonzept
  4. Sicherheit im Bereich der Informationstechnologie
  Hinweis:

Im Rahmen des Projektes ÖV-LeitmotiF-KI wird von einem sicheren und den gesetzlichen Vorgaben erfüllenden Fahrzeug (OEM) ausgegangen. Die Anforderungen an die Technische Aufsicht (TA) der AD-Leitstelle werden aus Sicht des Halters (ÖPNV) betrachtet.

- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
  Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
  Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.1 Generelle Kollisionsvermeidung
  Kollisionen mit anderen Verkehrsteilnehmenden und unbeteiligten Dritten müssen vermieden werden, sofern dies durch
  1. Notbremseingriffe oder
  2. andere Teilnehmende des umgebenden Verkehrs, andere unbeteiligte Dritte oder die Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nicht gefährdende Ausweichmanöver möglich ist. Kann eine Kollision zur Abwendung einer Gefährdung des Lebens der Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nur durch eine Gefährdung des Lebens anderer Teilnehmender des umgebenden Verkehrs oder unbeteiligter Dritter vermieden werden (unvermeidbare alternative Gefährdung von Menschenleben), darf der Schutz der anderen Teilnehmenden des umgebenden Verkehrs und der unbeteiligten Dritten nicht nachrangig gegenüber dem Schutz der Insassen des autonom fahrenden Kraftfahrzeugs erfolgen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.2 Interaktion mit anderen Verkehrsteilnehmenden
  a) Vorausfahrende Verkehrsteilnehmende auf der Fahrbahn werden erkannt. Es wird jederzeit in jedem Geschwindigkeitsbereich und in jeder möglichen Fahrsituation ein angemessener Sicherheitsabstand eingehalten. Der einzuhaltende Sicherheitsabstand bestimmt sich nach § 4 der Straßenverkehrs-Ordnung.
  b) Der Fahrstreifenwechsel vorausfahrender oder nachfolgender Fahrzeuge, der von einem benachbarten Fahrstreifen in den eigenen Fahrstreifen oder aus dem eigenen Fahrstreifen heraus in einen benachbarten Fahrstreifen erfolgt, wird erkannt und bei der Fahraufgabe entsprechend berücksichtigt.
  c) Situationen, welche einen Fahrstreifenwechsel bedingen (beispielsweise anhaltende oder langsame Fahrzeuge auf der Fahrbahn, Ende eines Fahrstreifens), werden erkannt und geeignete Manöver zum Fahrstreifenwechsel werden sicher durchgeführt.
  d) Einsatzfahrzeuge werden erkannt und geeignete Fahrmanöver sicher durchgeführt.

- AFGBV Anlage 1 Teil 1 Abschnitt 1.3 Planung der Fahrpfade und Geschwindigkeiten
  Bei Geschwindigkeitsanpassungen kommt es zu keiner vermeidbaren Beeinträchtigung von Insassen, anderen Verkehrsteilnehmenden und unbeteiligten Dritten. Es gelten folgende Anforderungen:
  a) Geschwindigkeitsbeschränkungen und Änderungen der Geschwindigkeitsbeschränkung werden erkannt und die Geschwindigkeit wird entsprechend angepaßt.
  b) Besondere Anforderungen an die Geschwindigkeit werden erkannt und im Geschwindigkeits- und Fahrtverlauf befolgt (beispielsweise in Bereichen vor Schulen und an Arbeitsstellen an Straßen, an Bushaltestellen, Bahnübergängen, in engen Kurvenradien oder bei Gefällen, in Engstellen, in denen der eigene Fahrstreifen vom Gegenverkehr mitbenutzt werden muß).
  c) Zeichen und Weisungen der Polizeibeamten gemäß § 36 der Straßenverkehrs-Ordnung, Wechsellichtzeichen gemäß § 37 der Straßenverkehrs-Ordnung, sonstige Zeichen gemäß der §§ 39 bis 42 der Straßenverkehrs-Ordnung sowie Verkehrseinrichtungen gemäß § 43 der Straßenverkehrs-Ordnung werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  d) Situationen, in denen die Vorfahrt anderen gewährt werden muß (beispielsweise vor Fußgängerüberwegen, in Kreuzungsbereichen oder Einmündungen), werden erkannt und ohne Gefährdung oder Behinderung der Vorfahrtberechtigten bewältigt. Es ist eine berechnete Zeit bis zum Aufprall von mehr als drei Sekunden bezüglich des Vorfahrtberechtigen einzuhalten. Wird von diesen Werten abgewichen, muß dies ausreichend begründet und auf Basis von systematischen Sicherheitsbewertungen nach dem Stand der Technik dokumentiert werden. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO-26262:2018-12 Straßenfahrzeuge – Funktionale Sicherheit erfüllt werden.
  e) Bauliche Straßengestaltungen mit Auswirkung auf das Verhaltensrecht (beispielsweise bis zu 5 Meter vom Fahrbahnrand einer vorfahrtberechtigten Straße abgesetzte Radwege nach § 9 Absatz 3 der Straßenverkehrs-Ordnung oder abgesenkte Bordsteine nach § 10 der Straßenverkehrs-Ordnung) werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  f) Arbeitsstellen an Straßen, temporär veränderte Fahrbahnverläufe oder Fahrbahnmarkierungen werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  g) Defizite am Zubehör, insbesondere der Verkehrseinrichtungen (zum Beispiel verschlissene, beschädigte, fehlende oder defekte temporäre oder dauerhafte Fahrbahnmarkierungen und Verkehrszeichen, Phantommarkierungen) und der Straßenausstattung, insbesondere solcher nach vorstehenden Buchstaben a bis f werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Dies gilt insbesondere nach Sturm- und sonstigen Witterungsereignissen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.4 Reaktion auf Umweltbedingungen
  Wetter-, Umwelt- und Straßeninfrastrukturbedingungen (beispielsweise Regen, Sichtbehinderung durch Rauch, Schlaglöcher) werden im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Fahrpfad und Geschwindigkeit sind – bis hin zum Stillstand des Fahrzeugs – so zu wählen, daß die in den Nummern 1.1 bis 1.3 gestellten Anforderungen auch bei geänderten Umweltbedingungen erfüllt werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 2 Risikominimaler Zustand
  Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur Ausübung der Fahraufgabe gilt: Das Kraftfahrzeug kann nur auf Veranlassung der Technischen Aufsicht den risikominimalen Zustand verlassen.
- AFGBV Anlage 1 Teil 1 Abschnitt 3 Notfahrfunktion
  Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit einer Notfahrfunktion ausgestattet sein. Muß sich das Kraftfahrzeug im Falle eines Defekts am Kraftfahrzeug in den risikominimalen Zustand versetzen, muß dies mit der Notfahrfunktion erfolgen. Fahrten mit der Notfahrfunktion dürfen nur bei Schrittgeschwindigkeit und aktivierter Warnblinkanlage erfolgen. Der Übergang der autonomen Fahrfunktion aus der normalen Fahrt in die Fahrt mit der Notfahrfunktion ist von dieser Geschwindigkeitsbegrenzung ausgenommen, sofern ein Abbremsen erforderlich ist.
- AFGBV Anlage 1 Teil 1 Abschnitt 4 Manueller Fahrbetrieb
  Im manuellen Fahrbetrieb erfüllt eine fahrzeugführende Person die Fahraufgabe. Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit Vorrichtungen ausgestattet sein, die es einer fahrzeugführenden Person ermöglichen, die Fahraufgabe wahrzunehmen. Ist die Steuerung im manuellen Fahrbetrieb auf Geschwindigkeiten nicht höher als Schrittgeschwindigkeit begrenzt, ist es nicht erforderlich, daß die fahrzeugführende Person sich innerhalb des Kraftfahrzeugs mit autonomer Fahrfunktion aufhält. Die Steuerung kann in diesem Fall über eine im Nahfeld des Kraftfahrzeugs befindliche Fernsteuerung ausgeführt werden. Die maximale Distanz, über die eine Fernsteuerung möglich ist, beträgt 6 Meter, gemessen in gerader Verbindung. Die Einhaltung der maximalen Distanz ist vom Hersteller durch geeignete technische Mittel sicher zu stellen. Soll das Kraftfahrzeug mit autonomer Fahrfunktion im manuellen Fahrbetrieb mit Geschwindigkeiten höher als Schrittgeschwindigkeit gesteuert werden, muß es mit einem Sitzplatz für die fahrzeugführende Person ausgestattet sein. Der Sitzplatz ist entsprechend der geltenden Vorschriften zu gestalten.

- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.1 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur dynamischen Ausübung der Fahraufgabe gilt:
  a) Zur dauerhaften Überwachung der technischen Ausrüstung werden nicht personenbezogene technische Daten im Kraftfahrzeug erhoben und gespeichert.
  b) Eine Beeinträchtigung der technischen Ausrüstung ist der Technischen Aufsicht unverzüglich anzuzeigen.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.2 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und mit konventionellen Vorrichtungen zur Ausübung der Fahraufgabe gilt:
  Die autonome Fahrfunktion darf nicht erneut aktivierbar sein, solange eine Beeinträchtigung der technischen Ausrüstung besteht.
- AFGBV Anlage 1 Teil 1 Abschnitt 6 Übertragung von Daten an das Kraftfahrzeug
  Die zur selbstständigen Bewältigung der Fahraufgabe im autonomen Betrieb notwendigen Daten und Informationen von externen technischen Einheiten (beispielsweise Backends oder Server eines Anbieters, externe Sensoren, Smartphone) müssen vom Kraftfahrzeug sicher empfangen und verwendet werden können. Daten externer Einheiten können im Kraftfahrzeug zur Ausführung der autonomen Fahrfunktionen verwendet werden. Daten und Informationen können beispielsweise bei bestimmten Anwendungsfällen über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) von einer externen technischen Einheit an das Kraftfahrzeug und vom Kraftfahrzeug an eine technische Einheit übertragen werden. Die Übertragung solcher Daten muß insbesondere den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und nach dem aktuellen Stand der Technik abgesichert sein. Das Absicherungskonzept muß die in einer Bedrohungsanalyse identifizierten Risiken mit wirksamen Maßnahmen adressieren und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten. Zur Datenübertragung sollte eine zentrale sichere elektronische Steuereinheit (SECU) genutzt werden. Die SECU dient als Informationsgateway im Kraftfahrzeug. Die SECU kommuniziert intern an die Kommunikationsbusse des Kraftfahrzeugs und an den physischen On-Board-Diagnose II-Anschluß (OBD II) oder an eine proprietäre Schnittstelle eines Herstellers. Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung sind Teil 5 zu entnehmen. Die Integrität, Authentizität und Verfügbarkeit der Datenübertragung sind sicherzustellen. Die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen oder mit Infrastrukturkomponenten ist zulässig. Sie muß auf der Basis einer Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 insbesondere den Anforderungen an die Informationstechnik nach Teil 5 und damit den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen. Während des Betriebs in einer optionalen Testphase ist die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen und Infrastrukturkomponenten zu testen und gegebenenfalls anzupassen.
- AFGBV Anlage 1 Teil 1 Abschnitt 7.1 Betriebshandbuch
  Zweck des Betriebshandbuchs ist es, mittels detaillierter Vorgaben den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten und der Technischen Aufsicht die richtige Reaktion auf Fehlerfälle zu ermöglichen.
  Hinweis:
  AFGBV Anlage 3 Dokumentationspflichten des Herstellers Kapitel 2 spezifiziert die Anforderungen.
  Hinweis:
  Es sollte stets von Ereignissen / Störmeldungen statt Fehlerfällen gesprochen werden,
  um die Interpretation / Unterstellung von vorsätzlich implementierten Fehlern zu vermeiden.
- AFGBV Anlage 1 Teil 1 Abschnitt 7.2 Sicherheitskonzept
  In dem Sicherheitskonzept ist die Sicherheit der Fahrfunktion zu bewerten. Mit einem systematischen Vorgehen müssen die für die Operational Design Domain (ODD) relevanten gefährlichen Szenarien und Ereignisse identifiziert und in einer Risikoanalyse bewertet werden. Um Gefährdungen zu verhindern oder deren Risiko auf ein akzeptables Maß zu mindern, muß ausgehend von erkannten Risiken für die entsprechenden Szenarien und Ereignisse ein Systemverhalten definiert oder müssen Systemverbesserungen umgesetzt werden. Die Systematik muß dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO/PAS 21448:2019-01 Straßenfahrzeuge – Sicherheit der beabsichtigten Funktion erfüllt werden. Die ausreichende Vollständigkeit der Szenarien wird auf Basis von Validierungsfahrten oder anderen Datenaufzeichnungen im Fahrbetrieb durch statistische Analysen belegt.
  Hinweis:
  ISO-21448:2022 Road vehicles – Safety of the intended functionality (SOTIF)
  Hinweis:
  AFGBV Anlage 3 Dokumentationspflichten des Herstellers Kapitel 3 spezifiziert die Anforderungen.
  Hinweis:
  Im Rahmen des Projektes ÖV-LeitmotiF-KI wird von einem sicheren und den gesetzlichen Vorgaben erfüllenden Fahrzeug (OEM) ausgegangen.

- AFGBV Anlage 1 Teil 1 Funktionale Anforderungen an Kraftfahrzeuge mit autonomer Fahrfunktion
  Abschnitt 7.3 Periodisch technische Fahrzeugüberwachung
  Durch eine geeignete funktionelle und konstruktive Gestaltung des Kraftfahrzeugs ist die Durchführbarkeit der periodischen technischen Fahrzeugüberwachung sicherzustellen (beispielsweise manueller Fahrbetrieb, Zugänglichkeit von Bremsen). Insbesondere die Befahrbarkeit von Bremsprüfständen, Lichteinstellplätzen, Hebebühnen oder Gruben und die Durchführung aller vorgeschriebenen Prüfungen müssen möglich sein.
- AFGBV Anlage 1 Teil 1 Abschnitt 8 Sensorik
  Zur technischen Umsetzung der autonomen Fahrfunktion muß eine Sensorik verwendet werden, die alle für die sichere Erfüllung der Fahraufgabe erforderlichen Gegenstände, Daten oder Personen im Umfeld des Kraftfahrzeugs erfaßt und hinsichtlich der Verarbeitung personenbezogener Daten die Vorgaben der Verordnung (EU) 2016/679, des Bundesdatenschutzgesetzes und spezialgesetzlicher datenschutzrechtlicher Vorschriften beachtet. Zur Erfüllung des in Satz 1 genannten Zwecks und unter Einhaltung der genannten Vorgaben kann die Sensorik durch externe Systeme unterstützt werden. Beeinflussen Wetter-, Umwelt- und Infrastrukturbedingungen die Leistungsfähigkeit der Sensorik, werden von der technischen Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion Maßnahmen eingeleitet, um die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken auszugleichen. Die Sensorik ist in das Sicherheitskonzept des Kraftfahrzeugs mit autonomer Fahrfunktion nach Nummer 7.2 und in die permanente Systemüberwachung nach Nummer 5 einzubinden.
- AFGBV Anlage 1 Teil 1 Abschnitt 9 Alterung und Abnutzung des Systems
  Das Kraftfahrzeug muß die funktionalen Anforderungen auch bei Alterung und Abnutzung der relevanten Systemkomponenten erfüllen. Beeinflussen Alterungserscheinungen die Leistungsfähigkeit, beispielsweise der Sensorik, gleicht die technische Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken durch geeignete Maßnahmen aus.
- AFGBV Anlage 1 Teil 2 Test- und Validierungsmethoden für Fahrzeuge mit autonomer Fahrfunktion (Abschnitt 10 bis 12) → *Definiert Test- und Validierungsmethoden, welche bei der Implementierung und Validierung anzuwenden sind. Diese juristischen Anforderungen gehören zur rechten Seite des V-Modells und damit nicht zum FSK*.
  Hinweis:
  V-Modell gemäß ISO-26262-02:2018 Kapitel 5.2.2.2d.
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse
  - ► 1) <u>Keine</u> Datenspeicherung bei autonomer Fahrt im festgelegten Betriebsbereich

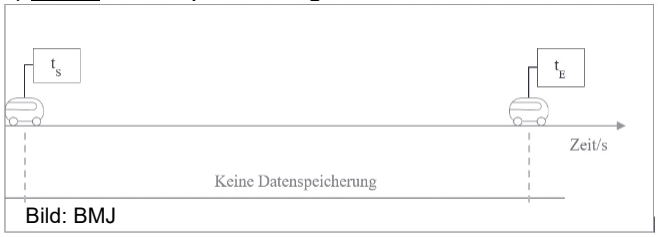


Bild: BMJ

  - ► 2) Datenspeicherung bei autonomer Fahrt im festgelegten Betriebsbereich mit Ereignis (bspw. Unfall)

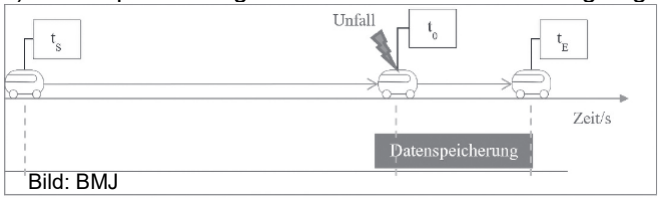


Bild: BMJ

- 3) Datenspeicherung bei autonomer Fahrt im festgelegten Betriebsbereich mit Ereignis und anschließender Überführung des Kraftfahrzeuges in den risikominimalen Zustand

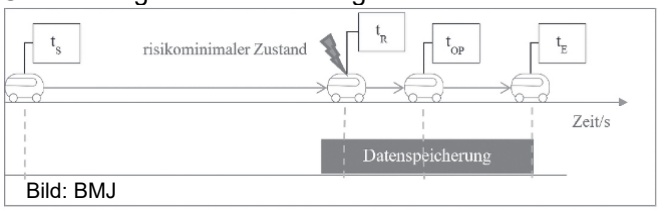


Bild: BMJ

- Legende:
  t_S Zeitpunkt – Beginn der Fahrt (Starten des Kraftfahrzeuges)
  t_R Zeitpunkt – Auslösung des risikominimalen Zustands
  t_0 Zeitpunkt – Unfallereignis
  t_{0P} Zeitpunkt – Anforderung oder Eingabe der Technischen Aufsicht
  t_E Zeitpunkt – Ende der Fahrt

- AFGBV Anlage 1 Teil 3 Abschnitt 13.2 Technische Vorgaben für das Speichern, Auslesen und Übertragen von Daten
  Das System der Datenspeicherung darf nicht flüchtig sein. Die gespeicherten Daten müssen im stromlosen Zustand erhalten bleiben.
  Ergänzende technische Anforderungen für den Datenspeicher
  - a) Der Zugang zu den im Kraftfahrzeug mit autonomer Fahrfunktion gespeicherten Daten erfolgt über die normierte 16-polige On-Board-Diagnose-Schnittstelle (16-polige OBD-Schnittstelle) über ein Kommunikationsmodul nach ISO 22900-1:2008-03 Straßenfahrzeuge – Modulare Kommunikationsschnittstelle im Fahrzeug (MVCI) – Teil 1: Hardwaredesign Anforderungen unter Verwendung der proprietären Software des Herstellers oder über die proprietäre Schnittstelle. Ergänzend dazu müssen in bestimmten Situationen oder nach bestimmten Ereignissen die Daten direkt über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) an die zuständige staatliche Stelle gesendet werden.
  - b) Der Zugang und das Herunterladen der gespeicherten Daten über die normierte 16-polige OBD-Schnittstelle oder über die proprietäre Schnittstelle darf nur durch das Kraftfahrt-Bundesamt und die zuständige Behörde erfolgen, sofern dies für deren jeweilige Aufgabenerfüllung nach dieser Verordnung erforderlich ist.
  - c) Im Reparaturfall erfolgt der Zugang zum Datenspeicher im Kraftfahrzeug mit autonomer Fahrfunktion über die normierte 16-polige OBD-Schnittstelle über ein Kommunikationsmodul nach ISO 22900 nur unter Verwendung der proprietären Software des Herstellers oder über die proprietäre Schnittstelle.
  - d) Die Datenspeicherung und die Datenübermittlung an das Kraftfahrt-Bundesamt und die zuständige Behörde haben den Anforderungen an die Sicherheit im Bereich der Informationstechnologie (Teil 5) zu genügen. Insbesondere müssen die Daten dem Stand der Technik gemäß unter Beachtung der Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 vor Manipulation und mißbräuchlicher Verwendung geschützt werden.

- AFGBV Anlage 1 Teil 4 Anforderungen an Mensch-Maschine-Schnittstellen Abschnitt 14 Interaktion
  Ein Kraftfahrzeug mit autonomer Fahrfunktion, das autonom innerhalb eines festgelegten Betriebsbereichs betrieben wird, erfordert nur in Ausnahmesituationen eine Interaktion mit der Technischen Aufsicht. Insbesondere ist die Mensch-Maschine-Schnittstelle unter Berücksichtigung der folgenden zwei Ausnahmesituationen zu gestalten.

- AFGBV Anlage 1 Teil 4 Abschnitt 14.1 Die Technische Aufsicht erteilt eine Fahrmanöverfreigabe an das Kraftfahrzeug mit autonomer Fahrfunktion
  Die technische Ausrüstung versetzt das Kraftfahrzeug in den risikominimalen Zustand, da die Fortsetzung der Fahrt aufgrund einer Verkehrssituation nicht fortgesetzt werden kann. Das Verlassen des risikominimalen Zustands erfolgt mit Unterstützung der Technischen Aufsicht. Folgendes ist hierbei zu beachten:
  a) Die autonome Fahrfunktion kann initial der Technischen Aufsicht mögliche Fahrmanöver zur Fortsetzung der Fahrt vorschlagen und ausreichend Daten zur Beurteilung der Situation liefern.
  b) Wird durch die Technische Aufsicht ein Fahrmanöver vorgegeben, so muß dieses durch die autonome Fahrfunktion validiert werden.
  Unabhängig von den Buchstaben a und b darf das Fahrmanöver nicht ausgeführt werden, wenn daraus eine Gefährdung der am Verkehr Teilnehmenden und unbeteiligter Dritter resultieren würde.
  Die sichere Ausführung oder Nichtausführung solcher Fahrmanöver obliegt weiterhin der autonomen Fahrfunktion mit systemseitiger Auswertung der aktuellen Verkehrssituation vor Ort.
  Hinweis:
  Der aktuelle Gesetzestext ist auf den ersten Blick korrekt, aber fatal beim zweiten Blick. Der menschliche Operator muß, insbesondere nach dem Überschreiten der Leistungsfähigkeitsgrenze eines Fahrzeugsystems in der Lage sein das Fahrzeug zu steuern, ohne daß dieses durch das vorab bereits versagte System verhindert werden kann. Sonst hätte man einen Dead-Lock.
  Autonome, automatisierte oder KI-Anwendungen können menschliche Verantwortung nicht ersetzen.
  (Ethische Regeln haben Bestand).
  Hinweis:
  Der menschliche Operator mit der zugehörigen Kompetenz (es kann eine Begrenzung auf erfahrene Operator geben) muß in der Lage

sein auch gegen einen Gegenstand, z.B. einen Stein auf der Straße bewußt zu fahren, z.B. nach einem Steinschlag, wo herabfallende Steine jetzt die Fahrbahn teilweise versperren, um das Fahrzeug aus der Gefahrenzone von weiteren herabfallenden Steinen zu bewegen, welche durch die Fahrzeugsicherheitssysteme nicht verhindert werden darf.

- AFGBV Anlage 1 Teil 4 Abschnitt 14.2 Übernahme der Fahraufgabe durch manuelle Steuerung außerhalb des festgelegten Betriebsbereichs.
  Erreicht die autonome Fahrt die Grenzen des festgelegten Betriebsbereichs, muß das Kraftfahrzeug durch die autonome Funktion in den risikominimalen Zustand versetzt werden. Wird die Fahrt außerhalb der Grenzen des festgelegten Betriebsbereichs durch eine fahrzeugführende Person fortgesetzt, ist die fahrzeugführende Person mittels eines geeigneten Interaktionskonzepts zur Aktivität aufzufordern. Sofern das Stehenbleiben des Kraftfahrzeugs mit autonomer Fahrfunktion den umlaufenden Verkehr oder Dritte behindern würde, ist die Aufforderung durch einen entsprechenden Hinweis zu ergänzen. Die Aufforderung ist in ihrer Intensität fortlaufend zu steigern. Die Aufforderung kann beispielsweise durch Signaltöne in zunehmender Lautstärke oder durch Vibrationen mit zunehmender Intensität erfolgen.
- AFGBV Anlage 1 Teil 5 Anforderungen an die Sicherheit im Bereich der Informationstechnologie
- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.
- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).

- AFGBV Anlage 2 Datenspeicherung
  Während des Betriebs sind bei den in § 1g Absatz 2 des Straßenverkehrsgesetzes genannten Anlässen im Kraftfahrzeug mit autonomer Fahrfunktion folgende Daten zu erfassen.

Fahrzeugidentifizierungsnummer	Alphanummerische Zeichen [A-Z; 0-9] Beispiel: AAAAAA654398GFRDE
Positionsdaten	Breiten- und Längengrad [±ddd.ddddd, Angabe in ± Graden (°) und Dezimalgraden, 5 Nachkommastellen] Höhenangaben in Meter Ausgabe im Globalen Positionsbestimmungssystem – Austauschformat als Abfolge von Punkten, in denen eine Änderung der Fortbewegungsrichtung erfolgt; Angabe des (Karten-)Bezugssystems.
Anzahl und Zeiten der Nutzung sowie der Aktivierung/Deaktivierung der autonomen Funktion	Datum (Jahr:Monat:Tag), Zeit (Stunde:Minute:Sekunde), Beispiel: 2019-07-16, 05:25:12
Anzahl und Zeit der Freigabe von alternativen Fahrmanöver.	Anzahl, Einzelzeiten (Stunde:Minute:Sekunde)
Systemüberwachungsdaten (Beginn/Ende) samt Softwarestand	Alphanummerische Zeichen [A-Z; 0-9] samt Erklärung Beispiel: P0601 Motorsteuergerät – Speicher Prüfsummenfehler
Umwelt- und Wetterbedingungen	Temperatur/°C, Helligkeit/Beleuchtungsstärke/lux, Stellung des Scheibenwischers an/aus.
Vernetzung	Vernetzungsparameter wie beispielsweise Übertragungslatenz und verfügbare Bandbreite
Name der aktivierten/deaktivierten passiven und aktiven Sicherheitssysteme, Zustand, auslösende Instanz (System oder extern)	Name des Systems, Zustand, Instanz Beispiel: Notbremssystem, aktiv, Systemfunktionsfähigkeit
Fahrzeugbeschleunigung in Längs- und Querrichtung	Nummerische Werte in Meter pro Sekunde zum Quadrat
Geschwindigkeit	Nummerischer Wert in Meter pro Sekunde
Status der lichttechnischen Einrichtungen	Beispiel: Blinken an/aus, Tagfahrlicht an/aus
Spannungsversorgung des autonomen Kraftfahrzeugs	Nummerischer Wert in Volt
Von extern an das Fahrzeug gesendete Befehle und Informationen	Gesendetes Format der Befehle sowie Metadaten zu Informationen: Dateigröße, Dateiformat, Quelle, Ziel, Übertragungszeit.

- AFGBV Anlage 3 Dokumentationspflichten des Herstellers
  … sind vom Fahrzeughersteller (OEM) eigenständig umzusetzen und somit nicht Bestandteil des Projektes ÖV-LeitmotiF-KI.

2.1.1.2 Anforderungen aus der Verordnung über den Bau und Betrieb der Straßenbahnen (BOStrab)

Im Rahmen des Projektauftrages ÖV-LeitmotiF-KI – Gesamtvorhabenbeschreibung (GVB), Kapitel 5 liegt der Arbeitsschwerpunkt der ESE im Bereich

- der Sicherheit im Sinne von Safety und
- der Sicherheit im Sinne von Security als Schutz gegen den unberechtigten Zugriff Dritter.

Hierbei bringt die ESE ihre Erfahrung aus der Begutachtung hochautomatisierter Systeme des Schienenverkehrs mit ein und überträgt diese auf den Gegenstandsbereich straßengebundener Verkehrssysteme.

Hinweis:
Die BOStrab hat für die Betrachtung innerhalb der Projektgrenze keinerlei Relevanz, da sie juristisch nicht bindend vorgeschrieben ist, jedoch kann sie als Vergleichsobjekt betrachtet werden, welche ähnliche Anforderungen der Sicherheit abbildet, die bei autonom fahrenden Fahrzeugen ihre Gültigkeit behalten. Gleichzeitig kann dieses das Verständnis bei erfahrenen Mitarbeitern des ÖPNV aus dem Bereich der Straßenbahn erleichtern, z.B. BOStrab §54 Absatz 3 versus AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.
- BOStrab §3 Absatz 2
  Einrichtungen in Betriebsanlagen und Fahrzeugen, die für die Benutzung oder Betätigung durch Fahrgäste bestimmt sind, müssen gut erkennbar und leicht erreichbar sein. Ihre Handhabung muß sich sinnfällig erkennen lassen; Fehlbedienungen dürfen zu keiner Betriebsgefährdung führen.
  Hinweis:
  Einrichtungen (welche für die Nutzung durch Fahrgäste vorgesehen sind) müssen
  gut erkennbar, (d.h. der Verwendungszweck muß eindeutig und leicht verständlich / logisch)
  und leicht erreichbar (behindertengerecht und für Kinder geeignet) sein.
- BOStrab §4 Absatz 2
  Betriebsanlagen und Fahrzeuge sind instandzuhalten. Treten an ihnen während des Betriebes Mängel auf, die die Betriebssicherheit beeinträchtigen können, sind sie ganz oder teilweise außer Betrieb zu nehmen und erforderlichenfalls abzusichern.
- BOStrab §4 Absatz 4
  Durch betriebliche Vorkehrungen ist dafür zu sorgen, daß Betriebsstörungen zügig beseitigt werden, bei Unfällen und gefährlichen Ereignissen unverzüglich Hilfe geleistet wird und insbesondere bei Brandfällen die Möglichkeit zur Selbst- oder Fremdrettung von Personen oder eine Kombination von beidem in Abhängigkeit von den lokalen Verhältnissen besteht.
- BOStrab §7 Absatz 2
  Der Unternehmer ist verpflichtet, bei der Auswahl, Aus- und Fortbildung, Verwendung und Beaufsichtigung der Betriebsbediensteten die Sorgfalt anzuwenden, die eine sichere und ordnungsgemäße Beförderung von Personen erfordert.
- BOStrab §7 Absatz 3
  Der Unternehmer hat zur Wahrnehmung der ihm nach dieser Verordnung obliegenden Aufgaben unbeschadet seiner eigenen Verantwortlichkeit einen Betriebsleiter zu bestellen. Bei mehreren Betriebsarten kann je ein Betriebsleiter bestellt werden. Für jeden Betriebsleiter ist mindestens ein Stellvertreter zu bestellen.
- BOStrab §7 Absatz 4
  Die Bestellung des Betriebsleiters und seiner Stellvertreter bedarf der Bestätigung durch die Technische Aufsichtsbehörde.
- BOStrab §23 Absatz 1
  Für die Verständigung von Betriebsbediensteten mit Betriebsstellen müssen im betriebsnotwendigen Umfang nachrichtentechnische Anlagen vorhanden sein. Besonders wichtige Meldungen an zentrale Betriebsstellen sollen vorrangig übermittelt werden können.
- BOStrab §23 Absatz 3
  Bei Fahrbetrieb ohne Fahrzeugführer müssen nachrichtentechnische Anlagen vorhanden sein, die eine vorrangige Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle ermöglichen.
- BOStrab §43 Absatz 3
  Türen müssen Schutzeinrichtungen haben, die verhindern, daß Fahrgäste durch Einklemmen verletzt werden.
- BOStrab §43 Absatz 5 Punkt 3
  bei Fahrbetrieb ohne Fahrzeugführer sicherstellen, daß Züge nur bei geschlossenen Türen anfahren können.
- BOStrab §43 Absatz 6
  Türen müssen in geschlossener Stellung festgehalten sein. Sie müssen jedoch von Fahrgästen im Notfall geöffnet werden können.
- BOStrab §46 Absatz 4
  Fahrzeuge müssen Einrichtungen für eine Sprechverbindung zwischen Fahrzeugführer und einer Betriebsstelle haben. Notfall-Informationen müssen vorrangig durchgegeben werden können.

- BOStrab §46 Absatz 5
  Personenfahrzeuge eines Zuges, die nicht mit Betriebsbediensteten besetzt sind, müssen ständig verfügbare Einrichtungen für eine Notfall-Sprechverbindung zwischen Fahrgästen und dem Fahrzeugführer haben.
  Hinweis:
  Die Technische Aufsicht (TA) der AD-Leitstelle ist der Fahrzeugführer im automatisierten (Remote-Sicherheitsfahrer bei ≤ SAE 3) / autonomen (≥ SAE4) Betrieb.
  Hinweis:
  Im konventionellen Betrieb befindet sich der Sicherheitsfahrer im Fahrzeug.
- BOStrab §46 Absatz 6
  Bei Fahrbetrieb ohne Fahrzeugführer müssen Personenfahrzeuge Einrichtungen für eine Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle haben. Absatz 4 Satz 2 gilt entsprechend.
- BOStrab §52 Absatz 3
  Betriebsanlagen oder Fahrzeuge, die ganz oder teilweise selbsttätig arbeiten oder fernbedient werden, müssen im Rahmen der betrieblichen Erfordernisse von Betriebsbediensteten auf einwandfreie Funktion überwacht werden.
- BOStrab §54 Absatz 3
  Personenzüge dürfen nur so beschleunigt und nur so gebremst werden, daß Fahrgäste nicht mehr als unvermeidbar gefährdet werden.

2.1.1.3 Anforderungen aus der Eisenbahn-Bau- und Betriebsordnung (EBO)

Im Rahmen des Projektauftrages ÖV-LeitmotiF-KI – Gesamtvorhabenbeschreibung (GVB), Kapitel 5 liegt der Arbeitsschwerpunkt der ESE im Bereich

- der Sicherheit im Sinne von Safety und
- der Sicherheit im Sinne von Security als Schutz gegen den unberechtigten Zugriff Dritter.

Hierbei bringt die ESE ihre Erfahrung aus der Begutachtung hochautomatisierter Systeme des Schienenverkehrs mit ein und überträgt diese auf den Gegenstandsbereich straßengebundener Verkehrssysteme.

Hinweis:
Die Eisenbahn-Bau- und Betriebsordnung (EBO) hat für die Betrachtung innerhalb der Projektgrenze keinerlei Relevanz, (weil diese für Eisenbahnen gilt und somit keinerlei Anwendung im Straßenverkehrswesen hat), jedoch kann sie als Vergleichsobjekt betrachtet werden, welche ähnliche Anforderungen der Sicherheit abbildet.

- EBO §28 Absatz 4
  Fernbetätigte oder automatisch schließende Türen müssen so beschaffen sein, daß bei ihrer Betätigung Personen nicht gefährdet werden.
- EBO §45 Absatz 7
  Reisezüge sind mit mindestens einem Zugbegleiter zu besetzen, sofern dessen betriebliche Aufgaben nicht von einem anderen Betriebsbeamten oder von technischen Einrichtungen übernommen werden. Sie dürfen ohne Zugbegleiter verkehren, wenn das Schließen der Wagentüren auf den Fahrgastwechsel abgestimmt und das Geschlossensein der Wagentüren vor Abfahrt dem Triebfahrzeugführer angezeigt oder bei einfachen Verhältnissen von ihm festgestellt wird.

Die juristischen Anforderungen der Eisenbahn sind weit entfernt von denen der Automotive, deshalb hier stark gekürzt, d.h. die obige Aufzählung ist bewußt weit entfernt von einer Vollständigkeit.

2.1.1.4 Produkthaftung

Der Fahrzeughersteller (OEM) hat neben den Anforderungen aus der AFGBV insbesondere die Anforderungen aus dem Produkthaftungsgesetz (ProdHaftG) und dem Produktsicherheitsgesetz (ProdSG) zu gewährleisten.

2.1.1.5 Betreiberhaftung

Neben der Produkthaftung gibt es auch die Betreiberhaftung, wobei als Betreiber jede juristische Person gilt, welche eine Anlage betreibt oder besitzt bzw. der die ausschlaggebende wirtschaftliche Verfügungsmacht obliegt.

Die Betreiberhaftung ist nicht als eigenständiges Gesetz spezifiziert, sondern wird in verschiedenen Gesetzen und Verordnungen abhängig vom Typ der Anlage spezifiziert, z.B.

- AFGBV §13ff Anforderungen an den Halter
- BOStrab §2 Grundregeln und §3 Allgemeine Anforderungen an den Bau der Betriebsanlagen und Fahrzeuge, sowie §4 Allgemeine Anforderungen an den Betrieb.
- Personenbeförderungsgesetz (PBefG)
- Verordnung über den Betrieb von Kraftfahrunternehmen im Personenverkehr (BOKraft)

2.1.2 Anforderungen aus Normen und Standards

2.1.2.1 Anforderungen an Sicherheitsanforderungen gemäß ISO-26262:2018

ISO-26262-03:2018 Clause 7.5.1 Functional Safety Concept (FSC) → 7.4.1 to 7.4.3

- Die funktionalen Sicherheitsanforderungen sollen abgeleitet werden aus den Sicherheitszielen unter Beachtung der Systemarchitektur
  ISO-26262-03:2018 Clause 7.4.2.1 → Sicherheitsziele / Safety Goals (SG).
- Mindestens eine Sicherheitsanforderung soll für jedes Sicherheitsziel etabliert werden, jedoch darf eine identische Sicherheitsanforderung zur Absicherung mehrerer Sicherheitsziele angewendet werden.
  ISO-26262-03:2018 Clause 7.4.2.2 → Sicherheitsziele / Safety Goals (SG).
  ➔ *Sicherheitsanforderungen müssen hierarchisch strukturiert sein.*

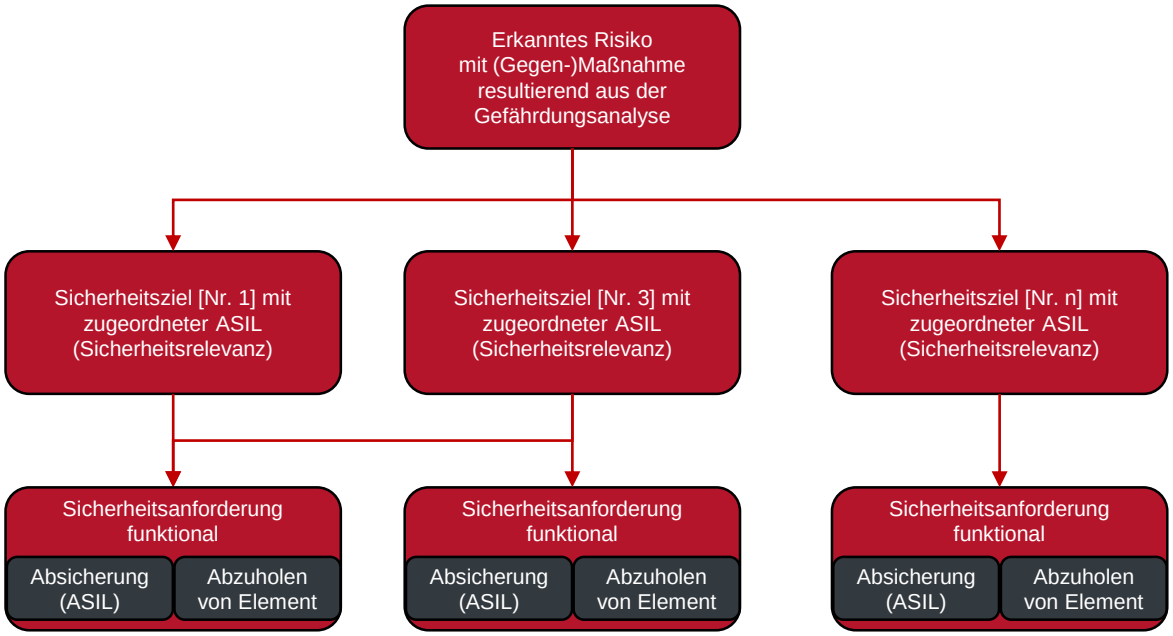


Abbildung 2 Hierarchisch strukturierte Sicherheitsanforderungen eigene Darstellung angelehnt an ISO-26262-03:2018 Figure 2

- Die funktionalen Sicherheitsanforderungen sollen spezifizieren, sofern notwendig, Strategien für …
  ISO-26262-03:2018 Clause 7.4.2.3 → Dämpfung- plus Unterstützungsleistung (Robustheit), s.ggf. UC-12.
  - Fehlervermeidung → Gegenmaßnahmen
    ISO-26262-03:2018 Clause 7.4.2.3a
  - Fehlererkennung und Steuerung der resultierenden Fehlfunktionsverhalten
    ISO-26262-03:2018 Clause 7.4.2.3b
  - Überführung in den sicheren Zustand, ggf. ausgehend von einem sicheren Zustand
    ISO-26262-03:2018 Clause 7.4.2.3c
  - Fehlertoleranz
    ISO-26262-03:2018 Clause 7.4.2.3d
  - die Verminderung / Verschlechterung der Funktionalität, im Fehlerfall bzgl. der Auswirkung auf f bzw. g
    ISO-26262-03:2018 Clause 7.4.2.3e
  - Warnmeldungen für den Fahrer *(bzw. der technischen Aufsicht in der AD-Leitstelle)*, welche das erkannte Risiko, durch aufzeigen / anzeigen (für einen angemessenen Zeitraum) der Warnmeldung, reduzieren.
    → Priorisierung von Warnmeldungen in der Benutzeroberfläche / Graphical User Interface (GUI)
    ISO-26262-03:2018 Clause 7.4.2.3f
    → UC-12 Systemüberwachung und ggf. Störmeldung.
  - Fahrerwarnmeldungen sollen die Kontrollierbarkeit des Fahrzeuges durch den Fahrer erhöhen
    ISO-26262-03:2018 Clause 7.4.2.3g
    → UC-12 Systemüberwachung und ggf. Störmeldung.
  - Die Berücksichtigung von zeitlichen Anforderungen (Latenzzeiten) an die funktionalen Sicherheitsanforderungen auf dem Fahrzeuglevel → gehört **nicht** zum Umfang des Projektes.
    Dieses obliegt dem Inverkehrbringer / OEM eigenverantwortlich ← diskriminierungsfreier Marktzugang für den Fahrzeughersteller (OEM).
    Hinweis:
    Das funktionale Zusammenspiel von Fahrzeug und Leitstand wird betrachtet, jedoch sind die Hersteller von Fahrzeugen und Leitständen frei in der Wahl ihrer Hardware plus der zugehörigen Software und der daraus resultierenden Parametrierung bzgl. des Zeitmanagements des Hardware-Software-Interfaces (HSI).
    ISO-26262-03:2018 Clause 7.4.2.3h

- Vermeidung oder Verminderung der Auswirkungen von gefährdenden Ereignissen aufgrund von unangemessenen Verfahren / Prozeduren von verschiedenen Steuerungsanforderungen bei simultanen / gleichzeitigen Anforderungen von verschiedenen Funktionen. → Handhabung von Wechselwirkungen.
  ISO-26262-03:2018 Clause 7.4.2.3i

Hinweis: Die Punkte c, e, f und g können Teil einer Warnung- und Abstufungsstrategie → Priorisierung sein

- Alle funktionalen Sicherheitsanforderungen sollen spezifiziert werden mit Berücksichtigung von
  a) den Betriebszuständen / Anwendungsfällen
  b) dem Fehlertoleranzzeitintervall
  c) den sicheren Zuständen
  d) dem Notfalloperationzeitintervall
  e) funktionalen Redundanzen (z.B. Fehlertoleranz)
  ISO-26262-03:2018 Clause 7.4.2.4
- Sofern die Verletzung eines Sicherheitszieles vermieden werden kann, durch den Übergang / Wechsel in einen anderen Betriebs- oder Wartungszustand, dann muß diese Spezifikation angewendet werden.
  ISO-26262-03:2018 Clause 7.4.2.5
- Für den Fall, daß der Wechsel in den sicheren Zustand nicht in einer akzeptablen Zeit erreicht werden kann, dann muß eine Notfalloperation spezifiziert werden. → *UC-12 ungenügende Maßnahme → MRM*.
  ISO-26262-03:2018 Clause 7.4.2.6
- Sofern Annahmen über das notwendige Verhalten des Fahrers oder einer anderen Person getroffen werden, um eine Verletzung eines Sicherheitszieles zu vermeiden, dann soll folgendes beachtet werden.
  ISO-26262-03:2018 Clause 7.4.2.7
  - Diese Handlungen müssen im funktionalen Sicherheitskonzept (FSK) beschrieben sein.
  - Angemessenes Handeln durch den Fahrer bedeutet, daß diese erwartbaren Handlungen die typischen Fähigkeiten eines Fahrers nicht übersteigen bzw. den Fahrer überfordern dürfen.
- Die funktionalen Sicherheitsanforderungen müssen den Elementen der Systemarchitektur zugewiesen werden.
  ISO-26262-03:2018 Clause 7.4.2.8
  - Während der Zuordnung von Anforderungen muß der ASIL passend zu den Parametern aus 7.4.2.4 (Betriebszustände, Fehlertoleranzen, sichere Zustände, Notfalloperationen und Redundanzen) plus deren zugehörenden Sicherheitszielen abgeleitet (vererbt) werden. Wenn die ASIL-Zerlegung angewendet wird, gelten auch die Anforderungen von ISO 26262-9:2018, Abschnitt 5.
  - Sofern Unabhängigkeit (Ungebundenheit) zwischen den Elementen und den implementierten Sicherheitsanforderungen gemäß ISO-26262-9:2018, Clause 6 **nicht** bestehen sollte, dann ist die höchste ASIL-Bewertung maßgeblich.
  - Sofern ein Item aus mehreren Elementen (E/E-Systemen) bestehen sollte, müssen die Sicherheitsanforderungen des Elementes mit den Schnittstellen unter Berücksichtigung der Architektur spezifiziert werden.
  - Sofern ein Item aus mehreren Elementen (E/E-Systemen) bestehen sollte, können die Zielwerte der Metriken gemäß ISO 26262-5:2018, Clauses 8 and 9, für jedes Element individuell festgelegt werden, im Einklang mit ISO 26262-4:2018, 6.4.5.2 .
  - Sofern ASIL Dekomposition (Zerlegung) angewendet wird, muß dieses im Einklang mit ISO-26262-9:2018, Clause 5 erfolgen.
- Sofern das Funktionale Sicherheitskonzept (FSK) Elemente anderer Technologien verwenden sollte:
  ISO-26262-03:2018 Clause 7.4.2.9
  - müssen die funktionalen Sicherheitsanforderungen von anderen Elementen / Technologien abgeleitet werden aus der zugehörigen Architektur.
  - müssen die funktionalen Sicherheitsanforderungen der Schnittstellen von anderen Elementen / Technologien spezifiziert werden.
  - müssen die funktionalen Sicherheitsanforderungen von anderen Elementen / Technologien abgesichert werden durch spezifische Maßnahmen, welche nicht der Zielsetzung der ISO-26262 folgen.
  - soll kein ASIL den Sicherheitsanforderungen der Elemente anderer Technologien zugewiesen werden.
- Sofern das Funktionale Sicherheitskonzept (FSK) von externen Maßnahmen abhängt, muß folgendes erfüllt werden:
  ISO-26262-03:2018 Clause 7.4.2.10
  - Die funktionalen Sicherheitsanforderungen, welche über externe Maßnahmen implementiert wurden, müssen abgeleitet und dokumentiert werden.
  - Die funktionalen Sicherheitsanforderungen von Schnittstellen mit externen Maßnahmen müssen spezifiziert sein.
  - Sofern externe Maßnahmen von einem oder mehreren Elementen (E/E-Systemen) implementiert wurden, müssen die funktionalen Sicherheitsanforderungen den Vorgaben der ISO-26262 folgen.

- Die Akzeptanz der Kriterien der Sicherheitsvalidierung auf der Item-Ebene muß die Spezifikation der Sicherheitsanforderungen und der Sicherheitsziele beinhalten.
  ISO-26262-03:2018 Clause 7.4.3.1
  ➔ *Sicherheitsanforderungen müssen dem Automotive Safety Integrity Level (ASIL) der Funktion und dem zugehörigen Sicherheitsziel entsprechen. Des Weiteren müssen Sicherheitsanforderungen nachvollziehbar (begründet) und rückverfolgbar sein.*

ISO-26262-08:2018 Clause 6 Specification and Management of Safety Requirements

Die ISO-26262 stellt Prozeßanforderungen an die Methodik und Verfahrensweise zum Spezifizieren von Sicherheitsanforderungen, insbesondere an die Attribuierung und die Charakteristika, welche für den Nachweis der Traceability von entscheidender Bedeutung sind.

Die Methodik und Verfahrensweise für die Erstellung der Anforderungen und der zugehörigen Verifikation (Review) hängen von der Sicherheitsrelevanz der Funktion (Anwendung) ab, s. ggf. ISO-26262-08:2018 Tabelle 1.

Hinweis:
Es gibt keine eigenständigen zu erstellenden Arbeitsergebnisse (Work Products) gemäß ISO-26262-08:2018 Clause 6.5.

Die Traceability muß die Anforderungen des AutomotiveSPICE® – Process Reference Model (PRM) erfüllen, insbesondere

- Automotive SPICE® – Process Assessment Model (PAM) – v3.1 Figure D.4
  Bidirectional Traceability and Consistency
  Hinweis:
  Die Quelle ist im Internet nicht mehr verfügbar, da diese zwischenzeitlich durch Version 4.0 ersetzt wurde
  DMS: AutomotiveSPICE®-ProcessAssessmentModel(PAM)-v3.1-01112017.pdf.
- Automotive SPICE® – Process Assessment Model (PAM) – v4,0 Figure
  Quelle: https://vda-qmc.de/wp-content/uploads/2023/12/Automotive-SPICE-PAM-v40.pdf
  DMS: AutomotiveSPICE®-ProcessAssessmentModel.(PAM)-v40-29112023.pdf.
- Automotive SPICE® – Model for Cybersecurity Engineering – v1.0 Figure 5 C.2 bis C.4
  Bidirectional Traceability and Consistency,
  Quelle: https://www.automotivespice.com/fileadmin/software-download/AutomotiveSPICE_for_Cybersecurity_PAM_1st_edition_2021.pdf
  DMS: AutomotiveSPICE®-ModelForCybersecurityEngineering-v1.0-06072021.pdf.

mit Erfüllung des Reifegrades von Capability Level 2 (CL2).

Ein Nachweis der Einhaltung der Nachverfolgbarkeit ist bei der Verifikation und Validierung der Produktentwicklung zu erbringen. Die Sicherheitsziele der Funktionalen Sicherheit auf der obersten Ebene sind beschrieben in 3.3.3 Sicherheitsziele / Safety Goals (SG). Die Sicherheitsziele der Cybersecurity werden beschrieben in WP 17-51 Cybersecurity Goals, welches nicht Bestandteil des Projektes ÖV-LeitmotiF-KI ist, weil diese Cybersecurity Sicherheitsziele wesentlich von den spezifischen Betriebsprozessen des jeweiligen ÖPNV-Unternehmens und der verwendeten Software der Leitstellen, sowie dem Fahrzeug selbst inklusive der spezifischen Software der ÖV- und AD-Tuning-Kits abhängig sind, wobei Software von dem Fahrzeughersteller (OEM) und deren Bauteilzulieferern enthalten sind, welche gegebenenfalls 3rd-Party-Softwareanteile enthalten. Nichtsdestotrotz werden Elemente, welche Einfluß auf den Schutz von Wirtschaftsgütern ausüben im Kapitel 2.3 Schutz vor dem unberechtigten Zugriff Dritter (Security) und den Unterkapiteln beschrieben.

2.1.2.2 Anforderungen an Sicherheitsanforderungen gemäß ISO-21448

ISO-21448:2022 Road Vehicles – Safety of the intended Functionality (SOTIF)

Die Safety of the intended Functionality (SOTIF) ≙ Sicherheit der Sollfunktion, hat zum Ziel die Sollfunktion so zu spezifizieren, daß diese als (hinreichend) sicher nachgewiesen werden kann. Somit sind unsichere (und insbesondere unbekannte) Ereignisse oder Werte auszuschließen.

Unsichere und unbekannte Ereignisse können durch geeignete Gegenmaßnahmen vermieden werden. Dazu zählt insbesondere der Qualitätsaspekt „Robustheit“, welcher vorgibt, daß Werte sich in einem Wertebereich, (ggf. mit Toleranzbereich) befinden müssen. Sollte der Wertebereich und/oder das erwartete Zeitverhalten der Aktualisierung nicht eingehalten werden, sind sichere Ersatzwerte (Amplitudenersatzwert oder Zeitersatzwert) zur Stabilisierung und Aufrechterhaltung der funktionalen und technischen Sicherheit anzuwenden. Zum Bauteilschutz und um abrupte Bewegungen zu vermeiden, sind Dämpfungsmaßnahmen bei Wertebereichsüberschreitung und Unterstützungsleistung bei Wertebereichsunterschreitung zu implementieren.

Neben den funktionalen Anforderungen gibt es sogenannte „*nicht-funktionale-Anforderungen*“, ein Begriff der immer wieder in Unterlagen, von verschiedenen Projekten und unterschiedlichen Unternehmen, als Anforderung ohne Funktion verstanden werden kann, weshalb man diese nicht zu testen oder zu überwachen braucht, welches ein häufig zu findender Fehler ist, der in Assessments erkannt / aufgedeckt wird oder im realen Leben bei der Erprobung zu lebensbedrohlichen Situationen führen kann.

Deshalb soll stattdessen der Begriff „Randbedingung“ (engl. boundary condition) im Anforderungsmanagement angewendet werden, welcher sich bereits etabliert hat.
Hinweis:
Das gilt auch, wenn der Begriff „nicht-funktionale-Anforderungen“ in einer Norm verwendet wird !

Hinweis:
In solchen Fällen kann die Abweichung im Projektmanagementhandbuch (PMH) dokumentiert werden.

Definition Randbedingung:
Beschreibt Prozeßanforderungen plus
nicht funktionale Größen z.B. Budgetierung (Speicherplatz), Temperatur, Luftfeuchtigkeit und Einschränkungen durch Schnittstellen oder die Herstellung (Fertigungsparameter, Kalibrierungsdaten).

Folglich beschreiben Randbedingungen Umfeldparameter (Umweltparameter), welche im Automotive Bereich zu finden sind bei der Umfelderkennung. Diese können z.B. durch LIDAR-Systeme gewonnen werden, welche erkannte Objekte als rechteckige Quader (bounding box ≙ Hüllkörper) abbilden. Diese Hüllkörper können sowohl Objekte aus der Umgebung, z.B. parkendes Auto, Wartehaus der Haltestellen oder auch Personen / Tiere sein.

Dementsprechend existieren feststehende und bewegliche Objekte. Feststehende Objekte können im Gegensatz zu beweglichen Elementen keine Gefahrensituation herbeiführen.

Hinweis:
Ein feststehendes Objekt kann nicht aktiv in den Fahrweg des Fahrzeuges eindringen, das bewegliche Fahrzeug kann ein feststehendes Objekt treffen (Unfall). Somit ist das verursachende und damit zu kontrollierende (zu steuernde) Objekt das Fahrzeug.

Daher ist es von entscheidender Bedeutung das feststehende von beweglichen Objekten unterscheidbar sein müssen, hierbei ist das Problem, daß ein bewegliches Objekt zwischenzeitlich auch den Zustand „Stillstand“ annehmen kann und somit für die Sensorik nicht unterscheidbar ist.

Ein weiteres Problem ist, daß ein Objekt seine Bewegung (Geschwindigkeit) ändern kann, diese kann z.B. der Übergang von „Gehen“ zu „Laufen“ sein (z.B. um noch rechtzeitig zur Haltestelle zu kommen bevor das gewünschte Transportmittel abfährt).

Eine Gefahrenänderung von gehender zu laufender Person ist kalkulierbar, da die Geschwindigkeiten von gehenden Menschen, in der Regel v ≤6km/h (Bundeswehrmarschgeschwindigkeit) zu laufenden Menschen, typisch 5 bis 15km/h *(Kurzstrecke 100m Lauf ist schneller als Marathon)*, einen bekannten Wertebereich haben.

Problematisch sind die Sonderfälle, wie Skatebordfahrer, Inline-Skater, … welche als langsam erkannt werden, dann aber ihre erwartete Geschwindigkeit deutlich, um Faktoren erhöhen können.

Die potentielle Gefahr, kann bewertet werden durch
- das Schadenspotential (Classes of Severity),
- die Beherrschbarkeit (Classes of Controllability) und
- die Auftretenswahrscheinlichkeit (Classes of probability of Exposure regarding operational situations),

welche als Sicherheitsrelevanz unter Automotive Safety Integrity Level (ASIL), definiert in der ISO-26262 etabliert angewendet wird.

Das Schadenspotential wird bestimmt durch die physikalische Größe der Energien ($W_{kinetisch}$, $W_{Potential}$, …) der Objekte.

Die Beherrschbarkeit hängt von den Fähigkeiten ab, dieses gilt sowohl für Menschen, automatisierte und auch autonome Systeme mit oder ohne KI.

Die Auftretenswahrscheinlichkeit kann aus der Statistik (Historie) ermittelt werden.

Safety of the intended Functionality (SOTIF) ≙ Sicherheit der Sollfunktion, hat (auch) zum Ziel aus der Felderfahrung zu lernen, insbesondere Spezifikationslücken zu erkennen. Dazu wird über die Lebenszykluskurve von Produkten ein Gefährdungslogbuch geführt, welches kontinuierlich (über den Zeitpunkt des Inverkehrbringens hinaus) gepflegt wird um dadurch iterativ das Produkt zu verbessern.

Hierbei ist die entscheidende Frage was man kontrollieren und damit steuern kann.

- Das Schadenspotential (S)
  hängt von den Energien ab, man kann jedoch nur seine eigenen Energien kontrollieren,
  aber nicht die Energien, welche andere Objekte, auf einen ausüben.
  Solange Energien anderer Objekte die eigenen Energien nicht beeinflussen ist die Kontrollierbarkeit der Situation gegeben.
- Die Auftretenswahrscheinlichkeit (E)
  wird ermittelt aus dem Gefährdungslogbuch des eigenen Produktes sowie ggf. vergleichbarer Gefährdungen, welche in einer Statistik zusammengeführt werden können.
- Die Beherrschbarkeit (C)
  ist die Größe in der ASIL-Metrik und damit in der Entwicklung, welche sich wesentlich beeinflussen läßt.
  - Der Mensch kann seine Fähigkeiten verbessern durch Ausbildung z.B. Sicherheitstraining
  - Der Mensch kann von Fahrerassistenzsystemen wesentlich unterstützt und entlastet werden. Fahrerassistenzsysteme haben zudem den Vorteil, daß diese sich im Gegensatz zum Menschen nicht erschrecken können. Dafür haben Fahrerassistenzsysteme jedoch den Nachteil, daß diese komplexe Situationen im Gegensatz zum Menschen nicht so leicht, hinreichend mit allen Wechselwirkungen und Potentialen / Möglichkeiten erkennen können.

Fahrerassistenzsysteme können durch den Einsatz von KI-Methoden trainiert (angelernt) werden. Dazu werden automatisiert Situationen aus dem Gefährdungslogbuch analysiert und mit den in der Vergangenheit getroffenen Maßnahmen verglichen. Die getroffenen Maßnahmen werden mit angemessen (richtig), nicht angemessen (falsch) sowie ggf. auch mit Zwischenwerten, z.B. unzureichend (tendenziell richtig aber nicht hinreichend) bewertet, welches dann für zukünftige automatisierte Maßnahmen als Entscheidungshilfe (mathematisch gewichtet) angewendet werden kann.

Hinweis:
Dieses ist ein Beispiel für eine KI-Lernmethode, es gibt noch weitere.

2.2 Metriken

2.2.1 Bewertung per Risikograph (VDV-Schrift-161)

Die Methodik der Bewertung von Gefahren mittels Risikograph wird definiert in der VDV-Schrift-161, *welche auf die „DIN EN 61508-5, Anhang D, Bild D.2 und Tabelle D.1“* verweist.
Es werden die Risikostufen *(vernachlässigbar, tolerabel, unerwünscht und intolerabel)* mittels der Eingangsparameter ermittelt. Dazu wird die folgende Metrik angewendet, welche besteht aus den Parametern:

- Auswirkung *(unbedeutend bis katastrophal)* des gefährlichen Vorfalls C *gemäß DIN EN 61508-5 (VDE 0803-5):2011-02*
  ⚠ Consequence Risk Parameter IEC-61508-5:2010.
  - C1 Geringe Verletzung
  - C2 schwere irreversible Verletzung einer oder mehrerer Personen inkl. Tod einer einzigen Person
  - C3 Tod mehrerer Personen
  - C4 Tod vieler Personen *(es gibt keine quantitative Angabe von „viele“ versus „mehrere“)*
- Frequenz (F) = Häufigkeit *(so gut wie nie bis häufig)* und Zeit des Aufenthalts (Dauer) im Gefahrenbereich
  - F1 seltener bis öfterer Aufenthalt im gefährlichen Bereich
  - F2 häufiger bis dauernder Aufenthalt im gefährlichen Bereich
- Potential (P) = Möglichkeit, den gefährlichen Vorfall zu vermeiden → (Gegen-)Maßnahme
  - P1 möglich unter bestimmten Bedingungen
  - P2 beinahe unmöglich
- Wahrscheinlichkeit (W)
  - W1 Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich.
  - W2 Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich
  - W3 Eine relativ hohe Auftretenswahrscheinlichkeit und häufige unerwünschte Ereignisse sind wahrscheinlich.

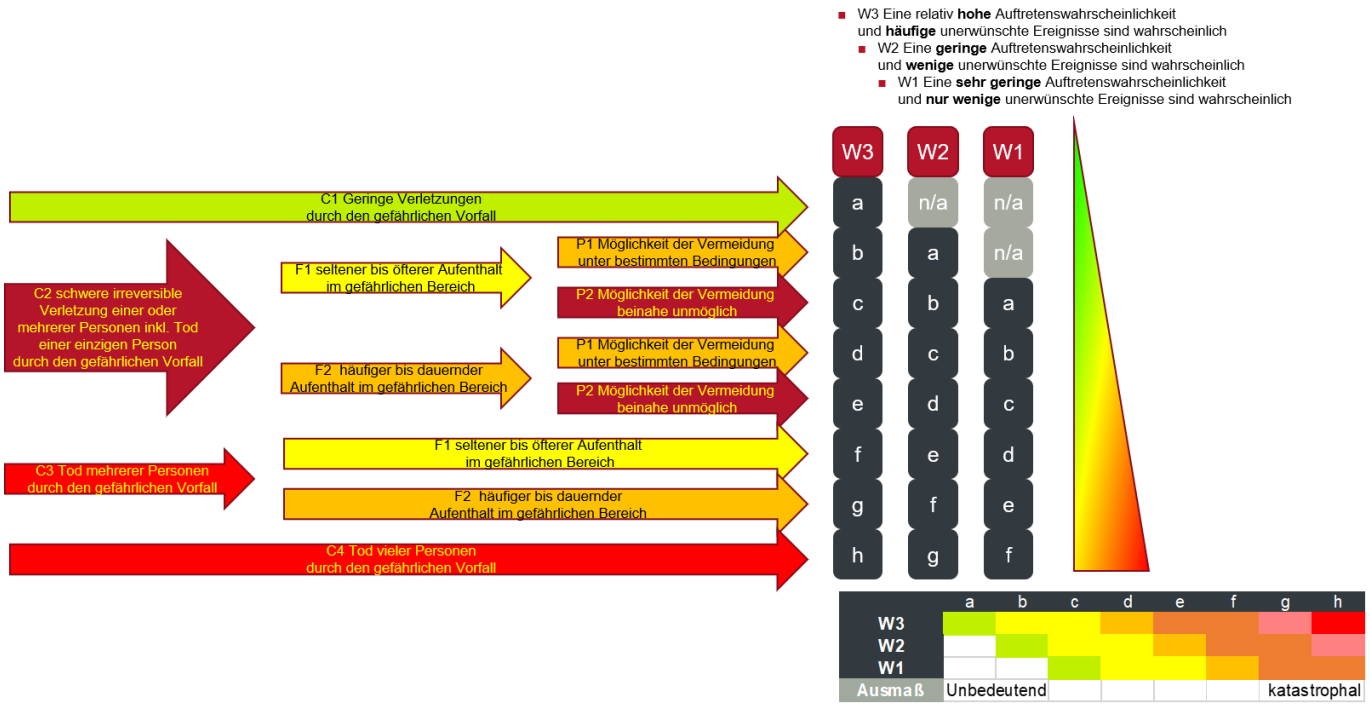


Abbildung 3 Bewertung per Risikograph (Metrik)

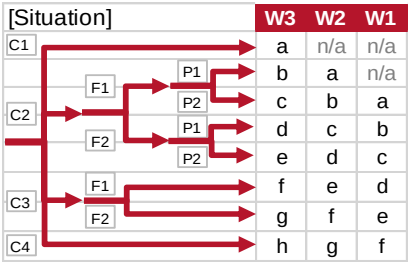
Hinweis:
Die VDV-Schrift-161 referenziert auf die DIN EN 61508-5 (VDE 0803 Teil 5), welche wiederum auf die ISO-14121-2 und ISO-13849-1, Anhang A als Quelle verweist.

Zuordnung der 8 Stufen (a bis h) des Risikographen zu den SIL / ASIL-Stufen:

Notwendige minimale Risikominderung (Kategorie)	Sicherheits-Integritätslevel (SIL)	Automotive Safety Integrity Level (ASIL)
n/a	Keine Sicherheitsanforderungen	QM
a	Keine speziellen Sicherheitsanforderungen	
b	1	ASIL A
c		
d	2	ASIL B
e	3	ASIL C
f		
g	4	ASIL D
h	ein einziges sicherheitsbezogenes E/E/PE-System ist nicht ausreichend	

Hinweis:
elektrisch/elektronisch/programmierbar elektronisch (E/E/PE)
gemäß DIN-EN-61508-4.(VDE-0803-4)-2011-02 (Begriffe und Abkürzungen) – Kapitel 3.2.13.

Risikograph:



2.2.2 Freigabelevel

Definition der typischen Freigabelevel über die Entwicklungsphasen im Produktentstehungsprozeß (PEP) zur Absicherung der Produktreife bis hin zur Baumustergenehmigung (BMG).

Freigabelevel:

L0 = keine Inbetriebnahme

L1 = Prüfstandversuche und Fahrversuche ausschließlich auf dem Prüfgelände durch eingewiesenes Fachpersonal der Fachabteilung.

L2 = Prüfstandversuche und Fahrversuche ausschließlich auf dem Prüfgelände durch eingewiesenes Fachpersonal der technischen Entwicklung.

L3 = Prüfstandversuche und Fahrversuche auf öffentlichem Gelände durch eingewiesene Mitarbeiter inkl. Partnerfirmen.

L4 = Fahrten durch Endkunden auf öffentlichen Straßen.

Hinweis:
Die Freigabelevel haben Relevanz bei Updates/Upgrades, welche die Zulassung / Genehmigung des festgelegten Betriebsbereichs betreffen oder zu einer relevanten Abweichung führen, so daß keine baugleichen Fahrzeuge nach der Modifikation mehr vorliegen, wodurch eine Erneuerung der Betriebserlaubnis durch den Halter einzuholen ist.

Hinweis:
Der Fahrzeughersteller (OEM) kann nicht für die Zulassung verantwortlich gemacht werden, weil einerseits das originale Fahrzeug (OEM) durch das AD-Kit modifiziert wird, (wobei die spezifischen Eigenschaften des ÖPNV-Unternehmens, insbesondere die spezifischen Verfahren und Überwachungsprozesse durch die Streckennetzabhängigkeit in der Software der Leitstände adaptiv implementiert ist), weshalb die Betriebserlaubnis durch die Modifikation (nicht mehr baugleiches Fahrzeug) zu erneuern ist, sowie zum Anderen entlang der Streckenführung (Umlauf), die Straßeninfrastruktur, die technischen Anforderungen der modifizierten Fahrzeuge in Kombination zu der Implementierung der Leitstände passen müssen, welches durch den Halter nachzuweisen ist.

Ein ÖPNV-Unternehmen hat die Möglichkeit, die Zulassung / Genehmigung eigenständig umzusetzen oder diese bei einer (Tuning-)Werkstatt oder ggf. dem Hersteller zu beauftragen. Sofern es eigenständig umgesetzt werden soll, gehört dieses in den Aufgabenbereich des Betriebshofes, wo die Fahrzeuge instandgehalten werden.

2.3 Schutz vor dem unberechtigten Zugriff Dritter (Security)

Anwendungen sind gemäß ihrer Bestimmung zu Nutzen.
Dieses bedeutet gleichermaßen, daß Anwendungen gegen nicht bestimmungsmäßige und/oder unbefugte Nutzung zu schützen sind.

Die bestimmungsmäßige Nutzung kann von dem Fachwissen bzw. der Ausbildung und den Aufgaben des Anwenders abhängig sein, weshalb unterschiedliche Zugriffsrechte für unterschiedliche Nutzergruppen (Anwender) gemäß ihren Aufgaben (gemäß Rollenbeschreibung) notwendig sind.

Im Projekt ÖV-LeitmotiF-KI werden die Sicherheitszonen im Referenzmodell abgebildet.
Es gibt Verantwortlichkeiten:

- AD-Leitstelle bzw. Rolle Technische Aufsicht (TA)
  Verantwortlich für die Überwachung und Gewährleistung der sicheren autonomen Fahrt.
- Betriebshof bzw. Rolle Betriebshof Management System (BHMS)
  Verantwortlich für die Sicherstellung der Einsatzbereitschaft / Betriebsbereitschaft der Fahrzeuge inklusive Nachweis der Gewährleistung der Einhaltung der Reparatur- und Wartungsinformationen der Fahrzeugsysteme gemäß den Vorgaben des Herstellers.
- ÖV-Leitstelle bzw. Rolle Disponent
  Verantwortlich für die Disposition der Fahrpläne inkl. Pünktlichkeit, Kapazitäts- und Einsatzplanung und Informationsversorgung der potentiellen und realen Fahrgäste. Dazu gehört auch die Überwachung des Fahrweges des Fahrzeuges / Platoon gemäß den Fahrplandaten, sofern notwendig / sinnvoll, das Ergreifen von Maßnahmen um die Pünktlichkeit wiederherzustellen sowie die mitreisenden und potentiellen Fahrgäste über Einhaltung / Abweichung der Pünktlichkeit zu informieren, als auch die Unterstützung bei der Sicherstellung des zeitgerechten Erreichens bei Anschlüssen der Fahrt.

und Zuständigkeiten:

- AD-Bordsystem
  Regelsystem mit Möglichkeit der menschlichen Fernsteuerungsübernahme durch die Technische Aufsicht (TA) im Fahrzeug.
- ÖV-Bordrechner
  Informationssystem mit Möglichkeit der Kommunikation zum Fahrgast im Fahrzeug.

Für den Schutz vor dem unberechtigten Zugriff Dritter (Security) sind geeignete technische, organisatorische und physische Zugriffsschutz-Maßnahmen anzuwenden.

Etablierte Maßnahmen, sowie Vorschriften sind beschrieben in den folgenden Dokumenten / Schriften:

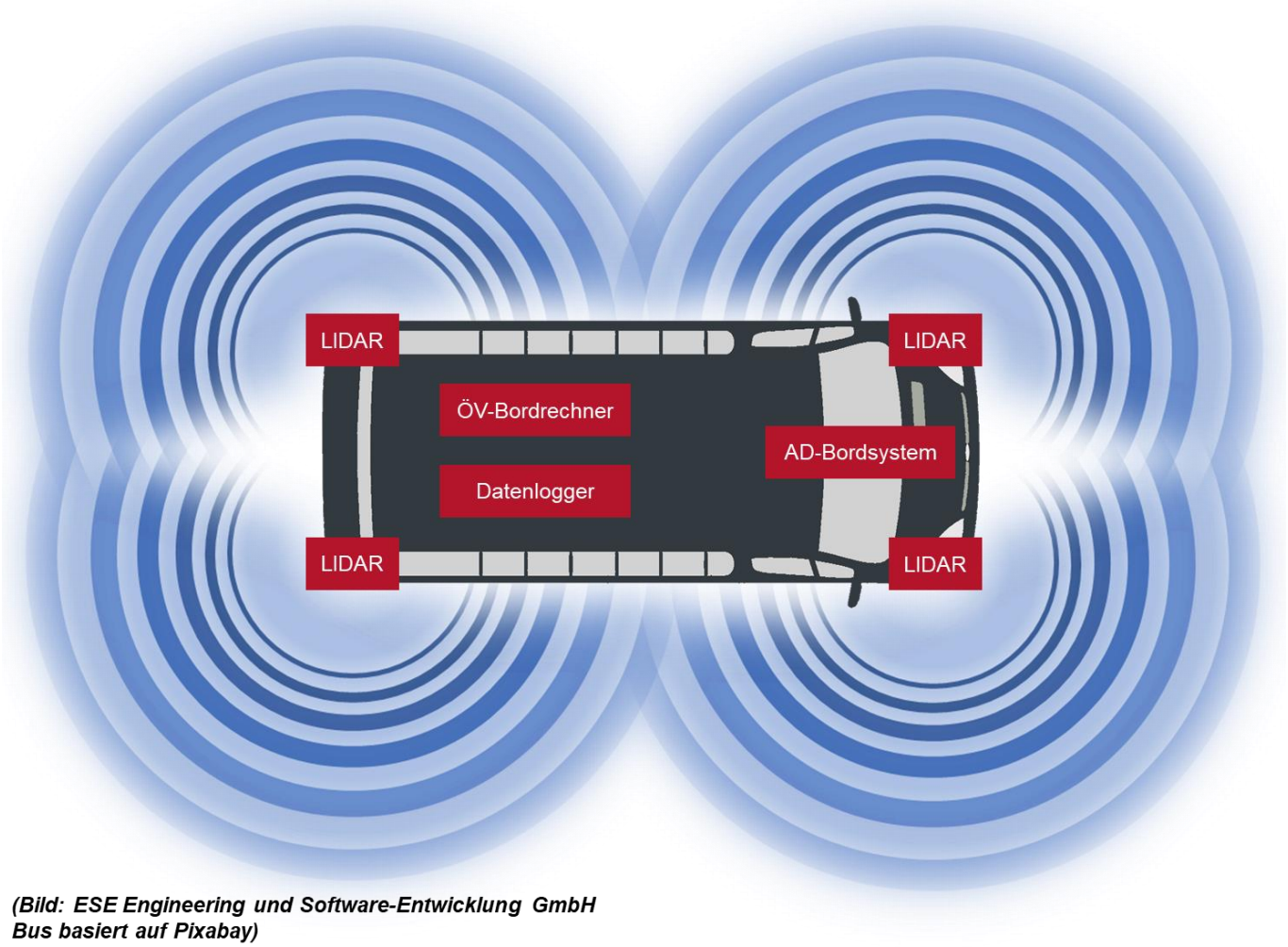
- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)
- CENELEC CLC/TS 50701:2023 Railway Applications – Cybersecurity
- DIN EN IEC 62443-3-3 (VDE 0802-3-3) System security requirements and security levels ≙ Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme – Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level.
- DIN EN IEC 62443-3-2 Security risk assessment and system design,
  welche beim Fahrzeuglevel zusätzlich mit einzubeziehen ist.
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection
  → Information Security Management Systems (ISMS)
- Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2023-01.
- VDV-Schrift-440 Branchenanforderungen an die IT-Sicherheit, Version 2023-02.
  - VDV-Schrift-4400 Maßnahmenkatalog zur VDV-Schrift 440:2023-02, Version 2023-02.
  - VDV-Mitteilung 4401, Version 2023-02.

2.3.1 Anforderungen der Datensicherheit

Zur Absicherung von Sicherheitsanforderungen hat sich die folgende Schutzziele-Klassifizierung etabliert.

- Vertraulichkeit (Confidentiality)
  - Schutz vor unbefugten Zugriffen auf vertraulichen Daten
  - Zugriffskontrolle, Verschlüsselung
- Integrität (Integrity)
  - Unverfälschtheit von Daten (Datenintegrität)
  - Schutz bei der Übertragung von Daten und ruhenden Daten
- Authentizität (Authenticity)
  - Sicherstellung der Identität von Benutzern und Systemen
  - Identität des Ursprungs der Daten
- Verfügbarkeit (Availability)
  - Funktionalität
  - Korrekte Verarbeitung
  - Nichtabstreitbarkeit (Non-Repudiation)
    Hinweis:
    Verbindlichkeit (digitale Unterschrift bei Angeboten und Verträgen)
  - Nachweisbarkeit durchgeführter Handlungen
    Hinweis:
    Nachweis der Erfüllung / Umsetzung einer Verbindlichkeit (Lieferung von vertraglich definierten Gütern oder Dienstleistungen)
  - Zurechenbarkeit (Accountability)
    Hinweis:
    Ordnungsgemäße Abrechnung (ggf. per Sachkonten) über erbrachte Leistung und plus der dafür verbrauchten Ressourcen.
  - Durchgeführte Handlungen können eindeutig zugeordnet werden
    Hinweis:
    Dokumentation der Handlungserbringung (Wer, Wann und Wo ggf. Wie, ggf. Womit).

2.3.2 Datensicherheit durch Schutzmechanismen



(Bild: ESE Engineering und Software-Entwicklung GmbH
Bus basiert auf Pixabay)

Abbildung 4 Systembild von einem automatisierten / autonomen Fahrzeug

Die Datensicherheit (Security) basiert auf Zugangszonen, in der obigen Abbildung sind dieses die Zonen

- Fahrgastraum (im Fahrzeuginneren)
  - Zone für Fahrgäste, z.B. Sitzplätze und die Fahrgast-HMIs ÖV + AD
  - Schutzzonen zu den Systemen, zu welchen Fahrgäste keinen Zugang erlangen dürfen
- Außenumwelt
  - Öffentlicher Bereich, wo sich andere Verkehrsteilnehmer aufhalten können

Die Sicherheit (Safety) von verwundbaren Verkehrsteilnehmern wird durch deren sichere Erkennung über die Fahrzeugsensoren (LIDAR, RADAR, Ultraschall) gewährleistet.

Somit ist es von Bedeutung, daß die realen Daten nicht von Dritten verändert / bewußt verfälscht oder manipuliert werden können, welches mittels einer geeigneten, sicheren Verschlüsselung der Daten zum Schutz gegen unautorisierten Zugriff realisiert werden kann.

Für die Verschlüsselung stehen verschiedene Methoden / Standards zur Verfügung, die Authentifizierung / Autorisation (digitale Unterschrift) kann mittels Zertifikaten erfolgen, außerdem können mehrfach Authentifizierung / (2FA/MFA) Anwendung finden, zusätzlich zur Verschlüsselung der sicheren Netzwerkübertragung nach TLS1.3.

Hinweis:
Die Zweifaktorauthentifizierung (2FA) beziehungsweise Multifaktorauthentifizierung (MFA) wird bei einem Login-Vorgang verwendet, wo neben den Nutzernamen und dem Kennwort noch weitere Daten anzugeben sind.

Verschlüsselung:

- Asymmetrische Verschlüsselung
  Es gibt zwei sich zu einem Schlüsselpaar ergänzende Schlüssel, den sogenannten Public Key und den Private Key.
- Symmetrische Verschlüsselung
  Die symmetrische Chiffre ist bereits aus der Antike bekannt, durch Julius Caesar, welcher jeden Buchstaben im Alphabet um drei versetzt hat.
  ABC…XYZ ↓ von oben nach unten = Symmetrische Verschlüsselung
  ↓ ↓
  DEF…ABC ↑ von unten nach oben = Symmetrische Entschlüsselung

In der gesicherten eMail-Kommunikation können beide Verfahren kombiniert angewendet werden

- ► eMails werden mit X.509-Zertifikaten / PGP asymmetrisch verschlüsselt

Sofern eine 2FA gefordert / zweckmäßig ist, können

- ► eMail-Anhänge mit einer per Paßwort gesicherten, verschlüsselten zip-Datei, zusätzlich zur eMail Verschlüsselung (PGP / X.509) verwendet werden,
  wobei ein systematisches Projektpaßwort je berechtigter Nutzergruppe Anwendung finden kann.

Bei Login-Prozessen kann eine 2FA oder auch MFA mittels HW und /oder SW-Token (Seed, Bit, Zeitserver) angewendet werden.

Bei den Netzwerken (WPA2 bei WLAN bzw. SSH oder IPSec bei VPN) hat sich

- Advanced Encryption Standard (AES)
  Symmetrische Verschlüsselung mit Blockchiffre mit Schlüssellänge 128 / 192 / 256bit
- Data Encryption Standard (DES)
  Symmetrische Verschlüsselung mit Blockchiffre mit Schlüssellänge 56bit.
  Double DES = 2DES / DDES hat eine Schlüssellänge von 112bit
  Triple DES = 3DES / TDES hat eine Schlüssellänge von 168bit

etabliert, d.h. heute wird AES so ziemlich überall im WLAN verwendet, sofern die Performance der Systeme gegeben ist, da die symmetrische AES-Verschlüsselung rechenintensiv ist. Dafür ist es nicht quantensicher.

Normen:
siehe Kapitel Schutz vor dem unberechtigten Zugriff Dritter (Security).

BSI:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/Arten-der-Verschluesselung/arten-der-verschluesselung.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.html

2.3.3 Sicherheitszonen

Es gibt verschiedene Sicherheitszonen, welche von der Struktur / Organisation des ÖPNV selbst abhängen, weshalb diese Thematik hier nur systematisch kurz beschrieben wird. Zu den Sicherheitszonen können Rollen (siehe „20230330_Deliverable_MS1_UseCases_Deliverable.docx / pdf, Version 1, Letzte Aktualisierung 30.03.2023“, sowie nachfolgende Versionen / Varianten) zugeordnet werden.

- Leitstelle
  Es gibt 3 verschiedene Typen von „Leitstellen“ (verantwortliche Organisationseinheit).
  Alle 3 Typen der Leitstelle können zusammen in einem Raum sitzen oder auch auf mehrere Räume, Gebäude oder Unternehmen verteilt sein.
  - Betriebshof (inklusive der Zugänge zum BHMS)
    Der Betriebshof kümmert sich um die Aufrechterhaltung der Kapazität des ÖPNV-Betriebes, damit für die Kernaufgabe der Fahrgastbeförderung, die dafür notwendigen Mittel / Ressourcen verfügbar sind.
    Dazu gehört die Wartung und Instandhaltung. Es können mehrere Betriebshöfe parallel betrieben werden, diese können vom ÖPNV-Unternehmen frei strukturiert werden, z.B. können Betriebshöfe einen
    - regionalen Bezug haben (Gebietszuständigkeit, z.B. Nordstadt, Südweststadt, östliche Gemeinden, …)
    - funktionalen Bezug, z.B.
      - Service und Wartung für Fahrzeuge von Hersteller A
        jedoch unabhängig der Fahrzeugklasse (Shuttle, PKW, VAN, Bus).
      - Service und Wartung abhängig der Fahrzeugklasse
        jedoch unabhängig vom Hersteller.
      - Reinigung außen durch eigene Mitarbeiter oder Dienstleister
        jedoch unabhängig vom Ort (kann auf dem BH / Zulieferer z.B. Waschstraße der Tankstelle erfolgen).
      - Reinigung innen
        unabhängig vom Ort (wird jedoch in der Regel auf dem eigenen Betriebsgelände durch eigene Mitarbeiter / Dienstleister umgesetzt).
  - ÖV-Leitstelle
    Die ÖV-Leitstelle kümmert sich um die Betriebssteuerung und die Fahrgastinformation / -kommunikation.
    Es können mehrere ÖV-Leitstellen parallel, auch unabhängig voneinander operieren, jedoch sind die Verantwortlichkeiten und Zuständigkeiten verständlich, eindeutig und widerspruchsfrei zu beschreiben.
    Hinweis:
    Im Rahmen des Projektes ÖV-LeitmotiF-KI wird definiert, daß die ÖV-Leitstelle für alles außerhalb des BH zuständig ist.
  - AD-Leitstelle
    Die AD-Leitstelle wird zukünftig als Remote-Sicherheitsfahrer im Bedarfsfall fungieren. Eine Person der Technischen Aufsicht (TA) kann mehrere Fahrzeuge parallel / per Multitasking überwachen / begleiten, (ähnlich dem Fluglotsen), jedoch mit der Möglichkeit die Steuerung des Fahrzeuges im Bedarfsfall zu übernehmen. Es können mehrere AD-Leitstellen parallel, auch unabhängig voneinander operieren, jedoch sind die Verantwortlichkeiten und Zuständigkeiten verständlich, eindeutig und widerspruchsfrei zu beschreiben.
- Fahrzeug
  - Bedienelemente bestimmt zur Benutzung durch den Fahrgast außerhalb des Fahrzeuges
    Emergency & Nottüröffnung
  - Bedienelemente bestimmt zur Benutzung durch den Fahrgast innerhalb des Fahrzeuges
    Nothalt, Notruf, Kommunikation
  - Regelsysteme mit Überwachung im Fahrzeug geschützt vor dem Zugriff durch den Fahrgast innerhalb des Fahrzeuges.
    - Fahrzeugsystem des Herstellers z.B. Motor
    - AD-Bordsystem
    - ÖV-Bordrechner
  - Bedienelemente bestimmt zur Nutzung durch das ÖPNV-Personal zur Erfüllung ihrer Aufgaben gemäß Rechtekonzept für die Rolle und ggf. Firmenzugehörigkeit, sofern Fremdmitarbeiter im ÖPNV-Betrieb eingesetzt werden.

Die Beschreibung erhebt keinen Anspruch auf Vollständigkeit, listet jedoch die typischen Elemente auf.
Dem ÖPNV-Unternehmen steht es frei dieses gemäß ihren Bedürfnissen und der Unternehmensstruktur anzupassen.

Es besteht auch die Möglichkeit, daß eine Person verschiedene Rollen in Personalunion (PU) wahrnimmt, aber hier ist auf die Zweckmäßigkeit zu achten, d.h.

- Es macht Sinn, wenn der Werkstattmeister im Rahmen der technischen Wartung in der Rolle der Technischen Aufsicht (TA) eine Probefahrt nach der Reparatur / Instandsetzung des Fahrzeuges auf dem Gelände des Betriebshofes ausführt.
- Es macht wenig Sinn, wenn Mitarbeiter, welche handwerkliche Tätigkeiten bevorzugen, für bürokratische, administrative Aufgaben der Verwaltung eingesetzt werden und umgekehrt.
  Hinweis:
  Insbesondere bei kleinen ÖPNV-Unternehmen kann der ÖV-Disponent auch mit den Aufgaben der logistischen Planung, dem Service und der technischen Wartung der Fahrzeuge in Personalunion verantwortlich sein.

3 Ableitung der funktonalen Sicherheitsrelevanz

3.1 Analyseobjekt (Referenzmodell)

Das Analyse Objekt basiert auf den Use Cases, welche spezifiziert wurden im Dokument „Use Cases für die Integration automatisierter Fahrzeuge in den ÖV“ mit dem Dateinamen „20230330_Deliverable_MS1_UseCases_Deliverable.docx / pdf, Version 1, Letzte Aktualisierung 30.03.2023“ plus dem Komponentendiagram der Referenzarchitektur (Abbildung 6) welches spezifiziert wurde im Dokument „Referenzmodell“ mit dem Dateinamen „20230330_Deliverable_MS2_Referenzmodell_Deliverable.docx / pdf, Version 1, Letzte Aktualisierung 30.03.2023“.

Es wird nach dem initialen Projekteende, zu welchem die ESE aus dem Projekt ausscheidet, neue Versionen der beiden obigen Dokumente geben, weil aufgrund der laufenden, agilen Bearbeitung bekannte, notwendige Änderungen erst zum Ende des Projektes statt bis zum ursprünglich geplanten Termin, dem Meilenstein M3, von den Konsortialpartnern eingearbeitet werden. Die vorab bekanntgewordenen, abgestimmten und schriftlich freigegebenen Veränderungen, welche vor dem Zeitpunkt der Erstellung dieses Dokumentes liegen, wurden soweit möglich, bereits eingearbeitet, jedoch können sich Inkonsistenzen durch spätere Änderungen ergeben, welche nach der Bereitstellung zum Review in den beiden Nachfolgeversionen der oben genannten Eingangsdokumente beschrieben wurden und somit hier nicht eingeflossen sind.

Die Unterschiede können durch die Beschreibung der Aktionen gegenüber den Swimlanediagrammen nachvollzogen werden.

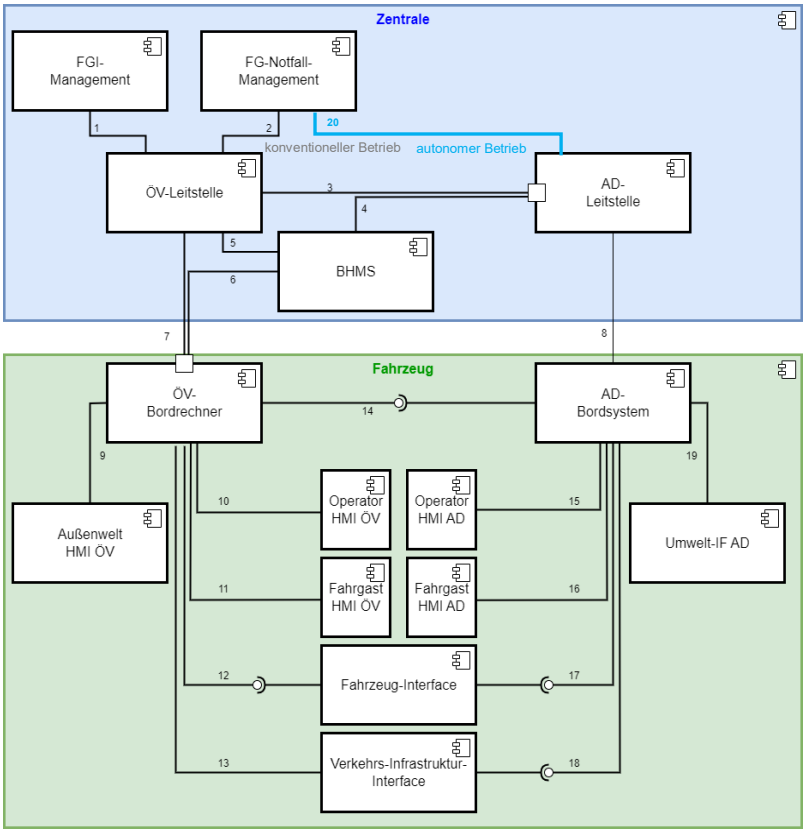


Abbildung 5 Referenzarchitektur, aktualisiert durch die Schnittstelle 20, basierend auf Referenzmodell.

Die Auflistung der Use Cases erfolgt in atomarer Schreibweise im Schema:
Hinweis: Atomare Schreibweise bedeutet, daß die funktionalen Operationen (Use Cases) unabhängig voneinander gelesen werden können.

Überschrift mit „UC-[Use Case Nummer, zweistellig] [Use Case Name]“ gemäß obiger, dokumentierter Spezifikation, plus paraphrasierter textueller Beschreibung daraus, welche durch weitere Kommentare und Hinweise ergänzt worden sein kann, gefolgt von

- einer Kurzdarstellung der Verantwortlichkeit und der Aktivität.
  Hinweis: Verantwortung können nur Personen haben, Geräte haben Zuständigkeit.
- dem Betriebsschutz
- dem zeitlichen Ablauf des UseCases (Situation und Aktionen)
- Juristischen Anforderungen als spezifische Ergänzung zu Mitgeltende Dokumente.
- dem Punkt „**Gefahren nach HAZOP**“ (Gefährdungsanalyse), welcher beispielhaft Erkenntnisse zum Verständnis und der Nachvollziehbarkeit der Bewertung liefert, welche in der einheitlichen Form Bewertung per Risikograph (VDV-Schrift-161) angewendet wurde.

Hinweis:
Das Arbeitserzeugnis (Work Product) Gefährdungs- und Risikoanalyse (GuR)
Hazard Analysis and Risk Assessment Report (HARA) gemäß ISO-26262-03:2018 Kapitel 6.5.1 ist ein eigenständiges Dokument, welches als Eingangsgröße zum Funktionalen Sicherheitskonzept (FSK) fungiert, welches von der Definition der Items abhängt, welche nicht Bestandteil des Projektauftrages ist, weshalb diese von keinem Konsortialpartner erstellt wurde. Somit wurde der Punkt Gefahren nach HAZOP bei den Use Case aufgenommen.

Hinweis:
Die erkannte Gefahr (Hazard) führt zu einem Sicherheitsziel (Safety Goal). Dieses wird abgeholt von der Analyse der Systemarchitektur, welche den Fehlerort (HW/SW/HSI) ermittelt, wo dann die (Gegen-)Maßnahmen der Vermeidung bzw. Risikominimierung implementiert werden.

3.2 Use Cases

Das FSK basiert auf dem vom ÖPNV-Unternehmen kontrollierten, geschlossenen Regelkreislauf, d.h. die ÖV-Leitstelle sendet eine FZ-Mission an die AD-Leitstelle, welche diese an das AD-Bordsystem weiterleitet, wo eine Prüfung der Umsetzbarkeit der geplanten Mission gegenüber der hochauflösenden Karte durchgeführt wird. Die Rückmeldung erfolgt einerseits zur AD-Leitstelle, sowie informativ an den ÖV-Bordrechner, welcher das Ergebnis seiner eigenen Prüfung des Fahrauftrages (wo die Missionen enthalten sind) mit dem Ergebnis der Missionsprüfung vom AD-Bordsystem an die ÖV-Leitstelle rückgemeldet, somit triggert der ÖV-Bordrechner die Übertragung der Mission, wodurch ausgeschlossen wird, daß das autonome Fahrzeug auf einer Mission unterwegs ist, welche nicht der im ÖV-Bordrechner eingestellten Fahrt entspricht.

Im Projektmonat 27/30 gab es eine eigenständige Designänderung durch Konsortialpartner, welche das oben beschriebene Routing abändert. Durch diese Änderung erfolgt die Rückmeldung der Missionsprüfung von der AD-Leitstelle (als Weiterleitung von der Meldung vom AD-Bordsystem) zur ÖV-Leitstelle. Eine Rückmeldung vom ÖV-Bordrechner erfolgt nicht mehr.

Als Konsequenz daraus, beschreibt das FSK eine abweichende Rückmeldung mit Routing (über 8 // 14 + 7) in den Use Cases, welches zukünftig im Feldtest durch ein Routing (über 8 + 3) umgesetzt werden soll.
Hinweis:
Die Schreibweise (über [Ziffer], …) referenziert auf die betroffenen Schnittstellen vom Routing gemäß dem Referenzmodell, abgebildet im Analyseobjekt (Referenzmodell).

Die agil beschriebenen Use Cases in 20230330_Deliverable_MS1_UseCases_v3.docx mit dem agilen 20230330_Deliverable_MS2_Referenzmodell.docx und den beiden oben referenzierten, freigegebenen Vorgängerversionen dieser beiden Dokumente, bilden die Eingangsdokumente aus welchen dieses FSK seinen Inhalt abzuleiten hat. Da unter der Leitung vom für AP2 verantwortlichen Projektpartner die Beschreibung der Use Cases auf die Konsortialpartner gemäß Mapping_UC_Verantwortliche_r_letzte_Aktulisierung.xlsx verteilt wurde, kommt es bei den Use Cases, welche die ESE im Dokument vom für AP2 verantwortlichen Projektpartner zu spezifizieren hat, zu Zirkelbezügen zwischen diesem FSK und seinem Eingangsdokument, weil die Spezifikationen im Rahmen des FSK entstanden sind und dann vom FSK Rückübertragen wurden in das Dokument vom für AP2 verantwortlichen Projektpartner.

3.2.1 UC-01 Fahrzeug aufrüsten

Bevor das Fahrzeug in Betrieb genommen wird, müssen die Fahrzeugsysteme gestartet und das Fahrzeug geprüft werden. Das Betriebshofpersonal rüstet das Fahrzeug auf dem Betriebshof gemäß den Vorgaben (Fahrzeug-ID, Terminvorgabe und vorgesehene Konfiguration) des Betriebshofmanagementsystems (BHMS) auf.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Erstellung der Fahrpläne und Zuordnung zu den vorhandenen Fahrzeugen per Einsatzplanung.	Fahrpläne (Umläufe) Kapazitätsplanung Einsatzplanung
BHMS	Prüfung der Einsatzbereitschaft. (Verifikation der Umsetzung der Maßnahmen von Wartung und Pflege) vor dem Aufrüsten plus Absolvieren der (erweiterten) Abfahrkontrolle.	Fahrzeugzustand (Einsatzbereitschaft, dazu zählen Wartung und Pflege der Fahrzeuge insbesondere zeitnahe Umsetzung der Inspektionen plus TÜV und AU-Termine, sowie angemessene, der Jahreszeit entsprechende, Bereifung.
AD-Leitstelle	Fahrzeuganmeldung entgegennehmen und Fahrzeugstatus erfassen. *Die Fahrzeugnummer wird auf aktiv gesetzt, damit erscheint das Fahrzeug mit den zuletzt bekannten Mängeln und den angeforderten Maßnahmen der Instandsetzung auf dem Schirm der technischen Aufsicht.* *Mit dieser Information wird der Testumfang des Selbsttests spezifisch für diese bekannten Mängel per Parametrierung erweitert.* *Das AD-System meldet den kumulierten Fahrzeugselbsttest (inklusive der spezifischen Tests) zur Prüfung, ob angeforderte Maßnahmen der Mängelbehebung, welche durch das BHMS organisiert wurde, beseitigt wurden, an den ÖV-Bordrechner.*	Verifikation der Beseitigung bekannter Mängel der Fahrsicherheit.

Hinweis:
Das Betriebshofmanagementsystem (BHMS) umfaßt das Planungs- und Steuerungssystem für alle Vorgänge auf dem Betriebshof, z.B. Abstellen, Rangieren, Kuppeln, Waschen, Tanken / Laden, etc. von Bussen und Shuttles.

Hinweis:
Es gibt in Deutschland keine gesetzliche Pflicht, die explizit die Nutzung von Winterreifen vorschreibt, aber StVO §2 Absatz 3a besagt: „Der Führer eines Kraftfahrzeuges darf dies bei Glatteis, Schneeglätte, Schneematsch, Eisglätte oder Reifglätte nur fahren, wenn alle Räder mit Reifen ausgerüstet sind, die unbeschadet der allgemeinen Anforderungen an die Bereifung den Anforderungen des § 36 Absatz 4 der Straßenverkehrs-Zulassungs-Ordnung genügen.“

Hinweis: StZVO §36 Absatz 4:
Reifen für winterliche Wetterverhältnisse sind Luftreifen im Sinne des Absatzes 2
1. durch deren Laufflächenprofil, Laufflächenmischung oder Bauart vor allem die Fahreigenschaften bei Schnee gegenüber normalen Reifen hinsichtlich ihrer Eigenschaft beim Anfahren, bei der Stabilisierung der Fahrzeugbewegung und beim Abbremsen des Fahrzeugs verbessert werden, und
2. die mit dem Alpine-Symbol (Bergpiktogramm mit Schneeflocke) nach der Regelung Nr. 117 der Wirtschaftskommission der Vereinten Nationen für Europa (UNECE) – Einheitliche Bedingungen für die Genehmigung der Reifen hinsichtlich der Rollgeräuschemissionen und der Haftung auf nassen Oberflächen und/oder des Rollwiderstandes (ABl. L 218 vom 12.8.2016, S. 1) gekennzeichnet sind.

Betriebsschutz:
Zugang zum Betriebshof (Sicherheitszone) haben nur ausgebildete und (sicherheitstechnisch) geschulte Mitarbeiter, Fahrgäste haben keinen Zugang.

Hinweis:
Es gibt bewußt keine direkte Schnittstelle vom BHMS zum AD-Bordsystem (Betriebsschutz vor Manipulation, Sicherstellung der Rückwirkungsfreiheit).

Situation:
Fahrzeug verfügbar machen (Regelbetrieb).

Aktionen:

- Der Mitarbeiter des BHMS bereitet das Fahrzeug mit der Fahrzeugnummer gemäß ÖV-Einsatzplanung vor. Dazu identifiziert er das Fahrzeug (ggf. über das Kennzeichen) und startet die Systeme (KL15 = ein).
- Das Fahrzeug startet (über 6 und 4 → 8) die Systeme und führt einen Selbsttest *(Fehlererkennung)* durch.
  - ▶ Der ÖV-Bordrechner prüft (über 9, 10, 11, 13 bzw. 12) die ÖV-Systeme gemäß Referenzmodel.

- Das AD-Bordsystem prüft (über 15, 16, 19 bzw. 17 und 18) die AD-Systeme gemäß Referenzmodel mit dem parametrierbaren Testumfang der technischen Aufsicht der AD-Leitstelle, damit die Behebung bekannter Fehler automatisiert verifiziert werden kann.
  Hinweis:
  Es gibt bewußt keine direkte Schnittstelle vom BHMS zum AD-Bordsystem (Betriebsschutz vor Manipulation).
  Hinweis:
  Das Fahrzeuginterface und das Verkehrs-Infrastruktur-Interface werden bereits vom ÖV-Bordrechner geprüft.
- Der BH-Mitarbeiter führt gemäß Prozeßvorgabe (Arbeitsvorschrift) eine Sichtkontrolle durch und startet die automatische Prüfung, z.B. optische Überprüfung der Bremsscheibendicke per Kameras auf dem Betriebshof. Die Ergebnisse werden nachverfolgbar dokumentiert und im System, dem ÖV-Bordrechner hinterlegt.

- Der ÖV-Bordrechner sammelt die einzelnen Selbsttestergebnisse von seinem eigenen Systemtest, dem kumulierten AD-Systemtest (über 14) und der Prüfung (Freigabe) des BH-Mitarbeiters (über 6) und sendet
  - eine Störmeldung (über 6) an das BHMS, falls das Fahrzeug nicht einsatzbereit sein sollte.
    Dann startet dieser UC-01 von vorne, sofern ein Ersatzfahrzeug gemäß ÖV-Einsatzplanung vorgehalten und noch verfügbar ist. Sollte kein Ersatzfahrzeug verfügbar sein, so erfolgt eine Störmeldung (über 5) an den Disponenten der ÖV-Leitstelle.
  - eine Einsatzbereitschaftsmeldung (über 6) mit Fahrzeugnummer (Fahrzeugnummer) an das BHMS, welches das Fahrzeug automatisiert (über 4) bei der AD-Leitstelle anmeldet plus den BH-Mitarbeiter informiert, daß er mit UC-02 (Umlauf Abfahrkontrolle) fortfahren kann.
- Das Fahrzeug absolviert (UC-01 → UC-02 → UC-44 → UC-01) die erweiterte Abfahrkontrolle (Probefahrt) unter der Systemüberwachung der Technischen Aufsicht (TA) der AD-Leitstelle und kehrt dann zum BHMS zurück, um die in AFGBV §13 Anforderungen an den Halter Absatz 7 definierten Bereiche zu überprüfen. Die Prüfung ist zu dokumentieren.
  Hinweis:
  UC-01 startet die Systeme,
  UC-02 aktiviert den Umlauf (BHMS) erweiterte Abfahrkontrolle (Probefahrt).
  UC-44 setzt die Probefahrt der erweiterten Abfahrkontrolle um
  UC-01 prüft die definierten (AFGBV §13 Anforderungen an den Halter Absatz 7) Bereiche
- Sobald der BH-Mitarbeiter die Dokumentation der Prüfung abgeschlossen hat und sofern die Prüfung Mängelfrei ist, wird mit dem Umlauf Betriebsaufnahme gemäß Umlauf (Fahrplan) des ÖV-Disponenten inklusive des Ausrückens (über UC-02) fortgefahren.

Juristische Anforderungen:

- AFGBV §12 Anforderungen an den Hersteller Absatz 1
  Der Hersteller eines Kraftfahrzeugs mit autonomer Fahrfunktion hat Reparatur- und Wartungsinformationen für das Kraftfahrzeug nach Anlage 3 Nummer 2.3 und 2.6 dieser Verordnung zu erstellen.
  → Welche hier anzuwenden sind.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 1
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen die Fahrzeugsysteme für die aktive und passive Sicherheit des Kraftfahrzeugs mit autonomer Fahrfunktion regelmäßig überprüft werden.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 2
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß täglich vor Betriebsbeginn eine erweiterte Abfahrkontrolle nach Absatz 7 durchgeführt wird.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 3
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen ab dem Tag der Zulassung zum Straßenverkehr alle 90 Tage eine Gesamtprüfung nach den Vorgaben des Betriebshandbuchs für das Kraftfahrzeug mit autonomer Fahrfunktion durchgeführt wird.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 4
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß die Ergebnisse der Gesamtprüfungen nach Nummer 3 einschließlich einer Beschreibung aller festgestellten Mängel und durchgeführter Instandsetzungen in einem Bericht dokumentiert und dem Kraftfahrt-Bundesamt sowie der zuständigen Behörde auf Verlangen unverzüglich übermittelt werden, sofern dies erforderlich ist.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im

Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.

- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 2
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen haben.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 3
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihnen anvertrauten Aufgaben zuverlässig sind; zur Beurteilung ihrer Zuverlässigkeit sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde sowie, bei Einsatz für die Durchführung von Fahrten im manuellen Betrieb, eine Auskunft aus dem Fahrerlaubnisregister vorzulegen; § 8 Absatz 3 gilt entsprechend.
- AFGBV §13 Anforderungen an den Halter Absatz 3
  Der Halter muß sicherstellen, daß Anweisungen zur ordnungsgemäßen Durchführung der Wartungsarbeiten, der Gesamtprüfungen, weiterer Untersuchungen und Fahrten im manuellen Fahrbetrieb vorliegen und daß diese Anweisungen befolgt werden. Die Anweisungen sind zu dokumentieren.
- AFGBV §13 Anforderungen an den Halter Absatz 4
  Berichte über die Durchführung von Wartungsarbeiten, von Gesamtprüfungen und von weiteren Untersuchungen müssen durch den Halter oder die verantwortliche Person unverzüglich schriftlich oder elektronisch erstellt werden. Die Berichte sind zu unterzeichnen. Die Berichte sind zu dokumentieren und vom Halter oder von der für die Technische Aufsicht verantwortlichen Person sechs Monate lang aufzubewahren und nach Ablauf dieser Frist unverzüglich, bei elektronischer Speicherung automatisiert, zu löschen.
- AFGBV §13 Anforderungen an den Halter Absatz 5
  Die Anforderungen zur Dokumentenverwaltung für die Anweisungen nach Absatz 3 und der Berichte nach Absatz 4 müssen dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik wird vermutet, wenn die Vorgaben der ISO 9001:2015 Qualitätsmanagementsysteme – Grundlagen und Begriffe erfüllt werden. Darüber hinaus muß die Dokumentenverwaltung den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 genügen.
- AFGBV §13 Anforderungen an den Halter Absatz 7
  Die erweiterte Abfahrkontrolle im Sinne des Absatzes 1 Nummer 2 beginnt mit einer Probefahrt, um die Systeme zu aktivieren. Im Anschluß an die Probefahrt werden folgende Bereiche überprüft:
  - Bremsanlage,
  - Lenkanlage,
  - Lichtanlage,
  - Reifen/Räder,
  - Fahrwerk,
  - sicherheitsrelevante elektronisch geregelte Fahrzeugsysteme sowie die Sensorik zur Erfassung externer und interner Parameter und
  - mechanische Fahrzeugsysteme für die aktive und passive Sicherheit.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie in der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik, Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik über einen Abschluß verfügt als
  - Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert),
  - Bachelor, Master oder
  - staatlich geprüfter Techniker.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 3
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muß, und

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 4
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihr anvertrauten Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes zuverlässig ist.
  Zur Beurteilung der Zuverlässigkeit im Sinne des Satzes 2 Nummer 4 sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde, eine Auskunft aus dem Fahrerlaubnisregister sowie eine Auskunft über Eintragungen aus dem Fahreignungsregister vorzulegen. Sofern in dem Fahrerlaubnisregister mehr als drei Punkte eingetragen sind, ist die Zuverlässigkeit nicht gegeben. § 8 Absatz 3 gilt bezüglich Satz 3 entsprechend.
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.2 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und mit konventionellen Vorrichtungen zur Ausübung der Fahraufgabe gilt:
  Die autonome Fahrfunktion darf nicht erneut aktivierbar sein, solange eine Beeinträchtigung der technischen Ausrüstung besteht.
- AFGBV Anlage 1 Teil 1 Abschnitt 6 Übertragung von Daten an das Kraftfahrzeug
  Die zur selbstständigen Bewältigung der Fahraufgabe im autonomen Betrieb notwendigen Daten und Informationen von externen technischen Einheiten (beispielsweise Backends oder Server eines Anbieters, externe Sensoren, Smartphone) müssen vom Kraftfahrzeug sicher empfangen und verwendet werden können. Daten externer Einheiten können im Kraftfahrzeug zur Ausführung der autonomen Fahrfunktionen verwendet werden. Daten und Informationen können beispielsweise bei bestimmten Anwendungsfällen über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) von einer externen technischen Einheit an das Kraftfahrzeug und vom Kraftfahrzeug an eine technische Einheit übertragen werden. Die Übertragung solcher Daten muß insbesondere den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und nach dem aktuellen Stand der Technik abgesichert sein. Das Absicherungskonzept muß die in einer Bedrohungsanalyse identifizierten Risiken mit wirksamen Maßnahmen adressieren und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten. Zur Datenübertragung sollte eine zentrale sichere elektronische Steuereinheit (SECU) genutzt werden. Die SECU dient als Informationsgateway im Kraftfahrzeug. Die SECU kommuniziert intern an die Kommunikationsbusse des Kraftfahrzeugs und an den physischen On-Board-Diagnose II-Anschluß (OBD II) oder an eine proprietäre Schnittstelle eines Herstellers. Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung sind Teil 5 zu entnehmen. Die Integrität, Authentizität und Verfügbarkeit der Datenübertragung sind sicherzustellen. Die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen oder mit Infrastrukturkomponenten ist zulässig. Sie muß auf der Basis einer Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 insbesondere den Anforderungen an die Informationstechnik nach Teil 5 und damit den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen. Während des Betriebs in einer optionalen Testphase ist die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen und Infrastrukturkomponenten zu testen und gegebenenfalls anzupassen.
- AFGBV Anlage 1 Teil 1 Abschnitt 8 Sensorik
  Zur technischen Umsetzung der autonomen Fahrfunktion muß eine Sensorik verwendet werden, die alle für die sichere Erfüllung der Fahraufgabe erforderlichen Gegenstände, Daten oder Personen im Umfeld des Kraftfahrzeugs erfaßt und hinsichtlich der Verarbeitung personenbezogener Daten die Vorgaben der Verordnung (EU) 2016/679, des Bundesdatenschutzgesetzes und spezialgesetzlicher datenschutzrechtlicher Vorschriften beachtet. Zur Erfüllung des in Satz 1 genannten Zwecks und unter Einhaltung der genannten Vorgaben kann die Sensorik durch externe Systeme unterstützt werden. Beeinflussen Wetter-, Umwelt- und Infrastrukturbedingungen die Leistungsfähigkeit der Sensorik, werden von der technischen Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion Maßnahmen eingeleitet, um die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken auszugleichen. Die Sensorik ist in das Sicherheitskonzept des Kraftfahrzeugs mit autonomer Fahrfunktion nach Nummer 7.2 und in die permanente Systemüberwachung nach Nummer 5 einzubinden.
- AFGBV Anlage 1 Teil 1 Abschnitt 9 Alterung und Abnutzung des Systems
  Das Kraftfahrzeug muß die funktionalen Anforderungen auch bei Alterung und Abnutzung der relevanten Systemkomponenten erfüllen. Beeinflussen Alterungserscheinungen die Leistungsfähigkeit, beispielsweise der Sensorik, gleicht die technische Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken durch geeignete Maßnahmen aus.

- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt. → *siehe AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse*.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.2
  a) Der Zugang zu den im Kraftfahrzeug mit autonomer Fahrfunktion gespeicherten Daten erfolgt über die normierte 16-polige On-Board-Diagnose-Schnittstelle (16-polige OBD-Schnittstelle) über ein Kommunikationsmodul nach ISO 22900-1:2008-03 Straßenfahrzeuge – Modulare Kommunikationsschnittstelle im Fahrzeug (MVCI) – Teil 1: Hardwaredesign Anforderungen unter Verwendung der proprietären Software des Herstellers oder über die proprietäre Schnittstelle. Ergänzend dazu müssen in bestimmten Situationen oder nach bestimmten Ereignissen die Daten direkt über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) an die zuständige staatliche Stelle gesendet werden.
  d) Die Datenspeicherung und die Datenübermittlung an das Kraftfahrt-Bundesamt und die zuständige Behörde haben den Anforderungen an die Sicherheit im Bereich der Informationstechnologie (Teil 5) zu genügen. Insbesondere müssen die Daten dem Stand der Technik gemäß unter Beachtung der Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 vor Manipulation und mißbräuchlicher Verwendung geschützt werden.
- AFGBV Anlage 1 Teil 4 Anforderungen an Mensch-Maschine-Schnittstellen Abschnitt 14 Interaktion
  Ein Kraftfahrzeug mit autonomer Fahrfunktion, das autonom innerhalb eines festgelegten Betriebsbereichs betrieben wird, erfordert nur in Ausnahmesituationen eine Interaktion mit der Technischen Aufsicht. Insbesondere ist die Mensch-Maschine-Schnittstelle unter Berücksichtigung der folgenden zwei Ausnahmesituationen zu gestalten.
- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.
- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).

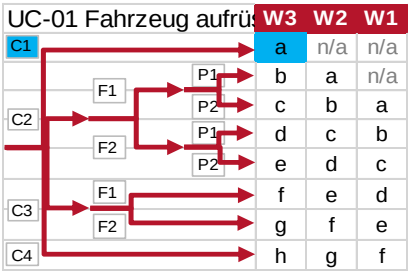
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.
- BOStrab §4 Absatz 2
  Betriebsanlagen und Fahrzeuge sind instandzuhalten. Treten an ihnen während des Betriebes Mängel auf, die die Betriebssicherheit beeinträchtigen können, sind sie ganz oder teilweise außer Betrieb zu nehmen und erforderlichenfalls abzusichern.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert.

Risikograph:



≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzung (Akzeptiertes Standardrisiko beim Arbeiten und der allgemeinen Fahrzeugnutzung)
✖	
✖	
W3	Die angenommene Auswirkung kann unmittelbar eintreten, wenn das Fahrzeug in Betrieb genommen wird. Die Arbeiten finden zum Teil im Hochvoltbereich (Schulung erforderlich) statt. Dadurch, daß der Betriebshofmitarbeiter ein Fahrzeug nach dem anderen in Betrieb nimmt, kann eine Sicherungsmaßnahme vergessen werden (in dem Glauben, daß man diese bereits umgesetzt hat, was jedoch beim vorherigen Fahrzeug realisiert war). Hinweis: Die Beurteilung W3 setzt eine hohe Auftretenswahrscheinlichkeit voraus, welche hier nicht gegeben ist, weil die Arbeiten im HV-Bereich nur einen sehr kleinen Anteil am zeitlichen Arbeitsprozeß haben, jedoch wird ein unerwünschtes Ereignis voraussichtlich am häufigsten bei Arbeiten im HV-Bereich auftreten, weshalb hier W3 zugrunde gelegt wird. Arbeiten außerhalb des HV-Bereiches können mit W1 bewertet werden.

Hinweis:
Die Probefahrt, das Aus- und Einrücken ins Depot erfolgt unter der Sicherheitsrelevanz von UC-44 Fahrt im Depot.

Hinweis:
Die Einstufung ist mit UC-07 Fahrzeug abrüsten vergleichbar.

3.2.2 UC-02 Umlaufanmeldung/-zuweisung

Nachdem das Fahrzeug aufgerüstet ist *(UC-01 → UC-02)* wird der Umlauf (Fahrplan) der ÖV-Leitstelle vom BHMS zugewiesen. Die Zuweisung wird vom Fahrzeug an die ÖV-Leitstelle gemeldet und gegenüber dem BHMS quittiert, wobei die Umlaufdaten (Fahrten und Fahraufträge) von der ÖV-Leitstelle ggf. aktualisiert an das Fahrzeug (ÖV-Bordrechner) plus über die AD-Leitstelle an das AD-Bordsystem übermittelt werden.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Zuweisung des aktualisierten Fahrplanes zum ausrückenden Fahrzeug gemäß Einsatzplanung.	Fahrplan Aktualisierung
BHMS	Konfiguration der Fahrbereitschaft zur Betriebsaufnahme.	Fahrbereitschaft (Betriebsbereitschaft)
AD-Leitstelle	Fahrzeugüberwachung (startet)	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Ein Umlauf ist eine Sequenz von Fahrten, vom Ausrücken aus dem Betriebshof bis zum Einrücken in den Betriebshof, d. h. die Menge von Fahrten, die von einem Fahrzeug an einem (Teil des) Betriebstag(s) durchgeführt werden. Die Identifikation erfolgt über den Betriebstag sowie eine Umlaufnummer.

Hinweis:
Die Umlaufnummer dient zur Identifikation des erwarteten „Fahrzeugs“, allerdings im organisatorischen Sinne, nicht im technischen Sinne eines konkreten Fahrzeugs. Wird eine Route von verschiedenen Fahrzeugen (unterschiedliche Fahrzeugnummern) befahren, entspricht diese der Fahrtroutennummer.

Hinweis:
Die Fahrt entspricht der Bewegung eines Fahrzeugs vom Startpunkt bis zum Endpunkt eines Fahrwegs und wird über den Umlauf bzw. Kurs und die Fahrtnummer identifiziert.

Hinweis:
Der Fahrweg ist eine für eine Fahrt genutzte Route. Diese ist definiert durch eine geordnete Folge geplanter Haltepunkte (bei Leerfahrten nur Start- und Zielpunkt) und ggf. Zwischenpunkte, die den Streckenverlauf eindeutig festlegen.

Hinweis:
Der Fahrauftrag definiert als Oberbegriff eine Vorgabe für die Bewegung eines Fahrzeugs. Die Quelle von Fahraufträgen kann vielfältig sein: Fahrplan, dispositive Maßnahme der Leitstelle, Betriebshof- und Werkstattmanagement etc. Entsprechend ist die Granularität eines Fahrauftrages sehr unterschiedlich, er kann von einer kurzen (Rangier-)Bewegung bis zu einer komplexen Folge von Einsetz- / Fahrplan- / Aussetz-Fahrten reichen.

Hinweis:
Die Mission beschreibt einen Teil einer Fahrt zwischen zwei Haltepunkten / Haltestellen und beinhaltet Angaben zu
- dem Fahrgastwechsel (möglich / nicht möglich, d.h. die Türen werden am Ziel geöffnet bzw. nicht geöffnet)
- der Zeitspanne des Haltens (für den potentiellen Fahrgastwechsel / für das Laden des Fahrzeuges / …)
- der Umlaufnummer inklusive Angaben zum vorgegebenen Fahrweg (Wegpunkte, Route) zum Zielpunkt gemäß Fahrwegplanung der ÖV-Leitstelle
plus optional
- den Informationen zur Haltebucht
- der geplanten Fahrzeit zur Umsetzung der Mission gemäß Fahrwegplanung der ÖV-Leitstelle.

Hinweis:
Die Mission zum Aus- und Einrücken in den Betriebshof gehört in den Umlauf und unterliegt der Verantwortung der ÖV-Leitstelle, auch wenn der erste bzw. letzte Teil auf dem Betriebshof stattfindet, wo offiziell der BHMS zuständig und verantwortlich ist. Der Übergabepunkt ist hier der Abfahrtpunkt oder der Parkplatz zum Ausrücken (nach der Umlaufanmeldung der ÖV-Fahrplandaten durch das BHMS), sowie beim wieder Einrücken der vom BHMS zugewiesene Rückkehrabstellplatz, welcher bei der Umlaufanmeldung vom BHMS zugewiesen wurde.

Hinweis:
Die Abfahrkontrolle (Probefahrt) wird im Ablauf UC-01 → UC-02 → UC-44 → UC-01 absolviert,
hier ist der zweite Aufruf von UC-02 beschrieben, auf welchen das Ausrücken zur Betriebsaufnahme folgt.

Betriebsschutz:
Zugang zum Betriebshof (Sicherheitszone) haben nur ausgebildete und (sicherheitstechnisch) geschulte Mitarbeiter, Fahrgäste haben keinen Zugang.

Situation:
Fahrzeug konfigurieren, Betriebsbereitschaft herstellen (Regelbetrieb).

Aktionen:

- *Nach Bestätigung der Einsatzbereitschaft durch UC-01* konfiguriert der Mitarbeiter des BHMS (über 6) das Fahrzeug mit den Daten des zugewiesenen Umlaufes, welche die Fahrt(en) plus deren Fahraufträge gemäß ÖV-Einsatzplanung beinhalten.
  Hinweis:
  Es gibt neben den Umläufen des ÖV-Betriebes auch Umläufe für Service und Wartung inklusive der erweiterten Abfahrkontrolle (Probefahrt) durch das BHMS.
- Der ÖV-Bordrechner meldet bei der Betriebsaufnahme (über 7) die Daten bei der ÖV-Leitstelle an.
  Sofern es sich um einen Service & Wartungsumlauf handelt, erfolgt die Anmeldung (über 6) beim BHMS.
- Die ÖV-Leitstelle bzw. das BHMS extrahiert die Daten,
  Umlauf → Sequenz von Fahrten → Fahrwege (Routen über Wegpunkte) → Fahraufträge (Fahrt im Depot / Leerfahrt / Fahrgastfahrt) → Fahraufträge.
- Das System von ÖV-Leitstelle / BHMS prüft die Navigationsdaten und genehmigt deren Anwendung durch dessen Freigabe, woraufhin die extrahierten Navigationsdaten übertragen werden,
  - (über 3 bzw. 4) an die AD-Leitstelle,
    welche diese zum Nachweis dokumentiert und (über 8) an das AD-Bordsystem überträgt.
  - (über 7 bzw. 6) an den ÖV-Bordrechner

  Hinweis:
  Sofern eine Aktualisierung der Daten notwendig sein sollte, kann der ÖV-Disponent diese über diverse UCs aktualisieren.
  In beiden Fällen verfügt das Fahrzeug dann über die gültigen und korrekten Navigationsdaten zum Betrieb.
- Der ÖV-Bordrechner prüft die vom BHMS / ÖV-Leitstelle übermittelten Fahrplandaten und speichert diese plus meldet (über 6) Betriebsbereit *(zur Probefahrt / zum Ausrücken)* an das BHMS zurück, welches (über 5) die ÖV-Leitstelle darüber informiert, ob das Fahrzeug abfahrbereit / nicht abfahrbereit ist. Im Falle der Nicht-Abfahrbereitschaft des Fahrzeugs wird die Problematik und gegebenenfalls die Verfügbarkeit eines Ersatzfahrzeuges mitgeteilt.
- Das AD-Bordsystem prüft die von der AD-Leitstelle übermittelten Fahrplandaten der ÖV-Leitstelle gegen die hochauflösende Karte und meldet (nicht) abfahrbereit (über 8) an die Technische Aufsicht der AD-Leitstelle sowie (über 14) an den ÖV-Bordrechner.
- Die Systemüberwachung (Technische Aufsicht) der AD-Leitstelle meldet (über 4) die (nicht) Abfahrbereitschaft mit ggf. Maßnahmen oder Auflagen an den BHMS zurück.
- Der BH-Mitarbeiter stellt sicher, daß sich keine Personen im Fahrzeug befinden, anschließend verläßt er das Fahrzeug (für UC-44 Fahrt im Depot).
  - Der Umlauf Abfahrkontrolle / Probefahrt kann mehrere Missionen enthalten, welche Leerfahrten und Fahrgastfahrten (ohne Fahrgast), in beliebiger Reihenfolge, mit/ohne Türöffnung und andere zu testende Situationen beinhalten kann. Zur Probefahrt gehört die funktionelle Überwachung der Fahrt plus die visuelle Überwachung im Innenraum, z.B. Rauchentwicklung (Nebel) der Klimaanlage. Zum Testende der Abfahrkontrolle / Probefahrt fährt das Fahrzeug zur Prüfstation für die vorgeschriebenen Prüfungen, gemäß der definierten Bereiche in AFGBV §13 Anforderungen an den Halter Absatz 7, welche in UC-01 Fahrzeug aufrüsten beim zweiten Aufruf (UC-01 → UC-02 → UC-44 → UC-01) dokumentiert werden.
  - Der klassische Umlauf (Betrieb) enthält die Fahrplandaten der ÖV-Leitstelle. Diese beginnt mit dem Verlassen des Depots über UC-44 Fahrt im Depot, gefolgt von Leer- und Fahrgastfahrten (mit/ohne Fahrgäste) in beliebiger Reihenfolge, welche über UC-45 MissionCtrl gesteuert werden.
    Der Betrieb endet mit dem wieder Einrücken in das Depot über UC-44 Fahrt im Depot.
  - Der Umlauf Fahrzeugpflege (Service & Wartung) steuert den Ablauf der UC-24 Fundsachen und Sauberkeit im Fahrzeug, UC-25 Waschvorgang, UC-26 Lademanagement, UC-43 Parken und letztendlich den UC-07 Fahrzeug abrüsten, welcher UC-09 Datenentsorgung initiiert.

Juristische Anforderungen:

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA)
  → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV Anlage 1 Teil 1 Abschnitt 1.3 Planung der Fahrpfade und Geschwindigkeiten
  Bei Geschwindigkeitsanpassungen kommt es zu keiner vermeidbaren Beeinträchtigung von Insassen, anderen Verkehrsteilnehmenden und unbeteiligten Dritten. Es gelten folgende Anforderungen:
  a) Geschwindigkeitsbeschränkungen und Änderungen der Geschwindigkeitsbeschränkung werden erkannt und die Geschwindigkeit wird entsprechend angepaßt.
  b) Besondere Anforderungen an die Geschwindigkeit werden erkannt und im Geschwindigkeits- und Fahrtverlauf befolgt (beispielsweise in Bereichen vor Schulen und an Arbeitsstellen an Straßen, an Bushaltestellen, Bahnübergängen, in engen Kurvenradien oder bei Gefällen, in Engstellen, in denen der eigene Fahrstreifen vom Gegenverkehr mitbenutzt werden muß).

c) Zeichen und Weisungen der Polizeibeamten gemäß § 36 der Straßenverkehrs-Ordnung, Wechsellichtzeichen gemäß § 37 der Straßenverkehrs-Ordnung, sonstige Zeichen gemäß der §§ 39 bis 42 der Straßenverkehrs-Ordnung sowie Verkehrseinrichtungen gemäß § 43 der Straßenverkehrs-Ordnung werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
d) Situationen, in denen die Vorfahrt anderen gewährt werden muß (beispielsweise vor Fußgängerüberwegen, in Kreuzungsbereichen oder Einmündungen), werden erkannt und ohne Gefährdung oder Behinderung der Vorfahrtberechtigten bewältigt. Es ist eine berechnete Zeit bis zum Aufprall von mehr als drei Sekunden bezüglich des Vorfahrtberechtigen einzuhalten. Wird von diesen Werten abgewichen, muß dies ausreichend begründet und auf Basis von systematischen Sicherheitsbewertungen nach dem Stand der Technik dokumentiert werden. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO 26262:2018-12 Straßenfahrzeuge – Funktionale Sicherheit1 erfüllt werden.
e) Bauliche Straßengestaltungen mit Auswirkung auf das Verhaltensrecht (beispielsweise bis zu 5 Meter vom Fahrbahnrand einer vorfahrtberechtigten Straße abgesetzte Radwege nach § 9 Absatz 3 der Straßenverkehrs-Ordnung oder abgesenkte Bordsteine nach § 10 der Straßenverkehrs-Ordnung) werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
f) Arbeitsstellen an Straßen, temporär veränderte Fahrbahnverläufe oder Fahrbahnmarkierungen werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
g) Defizite am Zubehör, insbesondere der Verkehrseinrichtungen (zum Beispiel verschlissene, beschädigte, fehlende oder defekte temporäre oder dauerhafte Fahrbahnmarkierungen und Verkehrszeichen, Phantommarkierungen) und der Straßenausstattung, insbesondere solcher nach vorstehenden Buchstaben a bis f werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Dies gilt insbesondere nach Sturm- und sonstigen Witterungsereignissen.

- AFGBV Anlage 1 Teil 1 Abschnitt 1.4 Reaktion auf Umweltbedingungen
  Wetter-, Umwelt- und Straßeninfrastrukturbedingungen (beispielsweise Regen, Sichtbehinderung durch Rauch, Schlaglöcher) werden im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Fahrpfad und Geschwindigkeit sind – bis hin zum Stillstand des Fahrzeugs – so zu wählen, daß die in den Nummern 1.1 bis 1.3 gestellten Anforderungen auch bei geänderten Umweltbedingungen erfüllt werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 6 Übertragung von Daten an das Kraftfahrzeug
  Die zur selbstständigen Bewältigung der Fahraufgabe im autonomen Betrieb notwendigen Daten und Informationen von externen technischen Einheiten (beispielsweise Backends oder Server eines Anbieters, externe Sensoren, Smartphone) müssen vom Kraftfahrzeug sicher empfangen und verwendet werden können. Daten externer Einheiten können im Kraftfahrzeug zur Ausführung der autonomen Fahrfunktionen verwendet werden. Daten und Informationen können beispielsweise bei bestimmten Anwendungsfällen über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) von einer externen technischen Einheit an das Kraftfahrzeug und vom Kraftfahrzeug an eine technische Einheit übertragen werden. Die Übertragung solcher Daten muß insbesondere den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und nach dem aktuellen Stand der Technik abgesichert sein. Das Absicherungskonzept muß die in einer Bedrohungsanalyse identifizierten Risiken mit wirksamen Maßnahmen adressieren und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten. Zur Datenübertragung sollte eine zentrale sichere elektronische Steuereinheit (SECU) genutzt werden. Die SECU dient als Informationsgateway im Kraftfahrzeug. Die SECU kommuniziert intern an die Kommunikationsbusse des Kraftfahrzeugs und an den physischen On-Board-Diagnose II-Anschluß (OBD II) oder an eine proprietäre Schnittstelle eines Herstellers. Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung sind Teil 5 zu entnehmen. Die Integrität, Authentizität und Verfügbarkeit der Datenübertragung sind sicherzustellen. Die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen oder mit Infrastrukturkomponenten ist zulässig. Sie muß auf der Basis einer Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 insbesondere den Anforderungen an die Informationstechnik nach Teil 5 und damit den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen. Während des Betriebs in einer optionalen Testphase ist die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen und Infrastrukturkomponenten zu testen und gegebenenfalls anzupassen.
- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.
- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-

02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).

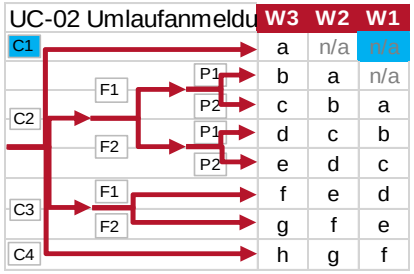
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert.

Risikograph:



≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzung (Akzeptiertes Standardrisiko beim Arbeiten und der allgemeinen Fahrzeugnutzung)
✖	
✖	
W1	Die angenommene Auswirkung kann unmittelbar eintreten, wenn das Fahrzeug in Betrieb genommen wird. Die Arbeit entspricht der Dateneingabe (normale Bürotätigkeit), es gibt keine Arbeiten am Hochvoltsystem. Somit ergibt sich eine Bewertung von W1.

Hinweis:
UC-02 → UC-44 Fahrt im Depot von der aktuellen Position ausrücken / autonom fahren zur nächsten Station von Service & Wartung, der erweiterten Abfahrkontrolle (Probefahrt) ODER zum Ausgang des Betriebshofes.

3.2.3 UC-03 Leerfahrt

Nachdem das Fahrzeug zum Ausrücken UC-44 Fahrt im Depot autonom losgefahren ist, wird aus dieser Fahrt, mit dem Passieren (Missionswechsel) der BHMS-Ausfahrt *(UC-44 → UC-45 → UC-03)* eine Leerfahrt, *gemäß dem Fahrauftrag der ÖV-Leitstelle aus UC-02 Umlaufanmeldung/-zuweisung.* Hierbei fährt das Fahrzeug autonom mit Überwachung durch die technische Aufsicht der AD-Leitstelle ab der Ausfahrt des Betriebshofes ohne Halt weiter zur Starthaltestelle (Einsetzfahrt).

Hinweis:
Sollte die Bereitstellung des Fahrzeuges früher fertig sein als zur Einhaltung der ÖV-Planung notwendig, dann kann das BHMS das Fahrzeug (Zwischen)parken. Der Gefahrenübergang (Wechsel der UCs) erfolgt mit dem Passieren der Ausfahrt.

Neben der Einsetzfahrt (ersten Leerfahrt zu Beginn des Umlaufes), gibt es weitere Leerfahrten, dazu zählen insbesondere die Aussetzfahrt, welche von der Endhaltestelle (der letzten Fahrgastfahrt) zum Betriebshof zurückkehrt. Außerdem kann eine Fahrt Umsetz- und Rangierfahrten als Leerfahrten *(UC-45 → UC-03)* vorsehen.

Hinweis:
Geplante „Fahrten ohne Fahrgäste“ werden als Leerfahrt bezeichnet, sofern diese außerhalb des BHMS erfolgen.

Eine Leerfahrt wird von der ÖV-Leitstelle explizit geplant und ist in den Fahrplandaten hinterlegt, welche im autonom fahrenden Fahrzeug sowohl im ÖV-Bordrechner als auch im AD-Bordsystem vorliegen.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Überwachung des Fahrweges des Fahrzeuges / Platoon gemäß der Fahrplandaten plus sofern notwendig / sinnvoll, das Ergreifen von Maßnahmen, um die Pünktlichkeit wiederherzustellen plus die mitreisenden und potentiellen Fahrgäste über Einhaltung / Abweichung der Pünktlichkeit zu informieren, sowie Unterstützung bei der Sicherstellung des zeitgerechten Erreichens bei Anschlüssen der Fahrt. Sofern erforderlich und sinnvoll Aktualisierung der Fahrplandaten über UC-14 Umlaufänderung oder UC-13 Fahrtänderung. Korrektheit der Außen- und Innenanzeiger über UC-18 Zielbeschilderung außen und innen ändern gewährleisten.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung).
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. Überprüfung (vor der Abfahrt), daß sich kein Fahrgast im Fahrzeug befindet.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Ein Umlauf ist eine Sequenz von Fahrten, vom Ausrücken aus dem Betriebshof bis zum Einrücken in den Betriebshof, d. h. die Menge von Fahrten, die von einem Fahrzeug an einem (Teil des) Betriebstag(s) durchgeführt werden. Die Identifikation erfolgt über den Betriebstag sowie eine Umlaufnummer.

Hinweis:
Die Umlaufnummer dient zur Identifikation des erwarteten „Fahrzeugs“, allerdings im organisatorischen Sinne, nicht im technischen Sinne eines konkreten Fahrzeugs. Wird eine Route von verschiedenen Fahrzeugen (unterschiedliche Fahrzeugnummern) befahren, entspricht diese der Fahrtroutennummer.

Hinweis:
Die Fahrt entspricht der Bewegung eines Fahrzeugs vom Startpunkt bis zum Endpunkt eines Fahrwegs und wird über den Umlauf bzw. Kurs und die Fahrtnummer identifiziert.

Hinweis:
Der Fahrweg ist eine für eine Fahrt genutzte Route. Diese ist definiert durch eine geordnete Folge geplanter Haltepunkte (bei Leerfahrten nur Start- und Zielpunkt) und ggf. Zwischenpunkte, die den Streckenverlauf eindeutig festlegen.

Hinweis:
Der Fahrauftrag definiert als Oberbegriff eine Vorgabe für die Bewegung eines Fahrzeugs. Die Quelle von Fahraufträgen kann vielfältig sein: Fahrplan, dispositive Maßnahme der Leitstelle, Betriebshof- und Werkstattmanagement etc. Entsprechend ist die Granularität eines Fahrauftrages sehr unterschiedlich, er kann von einer kurzen (Rangier-)Bewegung bis zu einer komplexen Folge von Einsetz- / Fahrplan- / Aussetz-Fahrten reichen.

Hinweis:
Die Mission beschreibt einen Teil einer Fahrt zwischen zwei Haltepunkten / Haltestellen und beinhaltet Angaben zu
- dem Fahrgastwechsel (möglich / nicht möglich, d.h. die Türen werden am Ziel geöffnet bzw. nicht geöffnet)
- der Zeitspanne des Haltens (für den potentiellen Fahrgastwechsel / für das Laden des Fahrzeuges / …)
- der Umlaufnummer inklusive Angaben zum vorgegebenen Fahrweg (Wegpunkte, Route) zum Zielpunkt gemäß Fahrwegplanung der ÖV-Leitstelle
plus optional
- den Informationen zur Haltebucht
- der geplanten Fahrzeit zur Umsetzung der Mission gemäß Fahrwegplanung der ÖV-Leitstelle.

Betriebsschutz:
Der Zugang zum Fahrzeug ist gesperrt, vor Abfahrt der UC-03 Leerfahrt ist durch die AD-Leitstelle zu verifizieren, daß sich keine Person im Fahrzeug (Sicherheitszone) befindet.

Hinweis:
Sollte UC-03 Leerfahrt auf UC-44 Fahrt im Depot (über UC-45 MissionCtrl) folgen, dann wurde die Prüfung, daß sich keine Person im Fahrzeug befindet bereits im BHMS umgesetzt, jedoch erfordert die Systematik zur Nachweisbarkeit der Umsetzung der Überwachung eine Videoaufzeichnung, welche die Freigabe durch die Technische Aufsicht (TA) der AD-Leitstelle dokumentiert und diese in der Kommunikationsaufzeichnung gemäß den Aufbewahrungsfristen verfälschungssicher ablegt.

Situation:
Fahrzeug ist konfiguriert und betriebsbereit und verläßt oder kehrt zurück zum BHMS (Regelbetrieb).
Sonderfall: Rangierfahrt (bei Bedarf, z.B. Fahrplananpassung an aktuelle Situation)

Aktionen (0.Fall Leerfahrt als Einsatzfahrt des Regelbetriebes):

- Nachdem das Fahrzeug über UC-44 Fahrt im Depot den Ausgang des BHMS erreicht hat, meldet das AD-Bordsystem das Passieren (Weiterfahrt ohne Halt) und den Missionswechsel *(UC-44 → UC-45 → UC-03)* (über 14) an den ÖV-Bordrechner plus (über 8) an die AD-Leitstelle, welche (über 3) automatisch an die ÖV-Leitstelle weiterleitet.
- Der ÖV-Bordrechner meldet (über 7) den Abschluß der Fahrt (UC-44 Fahrt im Depot) an die ÖV-Leitstelle.
- Weiter mit Aktionen 1.Fall

Aktionen (1.Fall Leerfahrt des Regelbetriebes):

- Das AD-Bordsystem setzt den Missionswechsel über UC-45 MissionCtrl um, welcher jetzt die klassische Leerfahrt startet.
- Das AD-Bordsystem fordert (über 8) von der AD-Leitstelle die optische Überprüfung des Fahrgastraumes an.
  Hinweis:
  Sollte UC-03 Leerfahrt auf UC-44 Fahrt im Depot (über UC-45 MissionCtrl) folgen, dann wurde die Prüfung, daß sich keine Person im Fahrzeug befindet bereits im BHMS umgesetzt, jedoch fordert die Regelschleife diese Prüfung systematisch an. Die Kameraaufzeichnung dokumentiert, daß sich keine Person im Fahrzeug befindet. Damit wird nachgewiesen, daß sich keine Person über das Fahrzeug in die Sicherheitszone von dem BHMS eingeschlichen bzw. (im 0.Fall) herausgeschlichen haben kann.
- Die AD-Leitstelle fordert (über 8) das AD-Bordsystem auf, die Aktivierung der Kameraaufzeichnung plus der Sprechverbindung in den Fahrgastraum (über 16) das AD-Fahrgast-HMI herzustellen.
- Das AD-Fahrgast-HMI öffnet die Sprechverbindung zum (geplant leeren) Fahrgastraum
  plus liefert über die schwenkbare Kamera kontinuierlich Bilder vom Fahrgastraum (während der Prüfung).

- Das AD-Bordsystem zeichnet die Audio- und Videodaten auf und sendet diese beiden Datenströme (über 8) zur AD-Leitstelle.
  - ► Sofern sich Fahrgäste im Fahrzeug befinden sollten, leitet die Technische Aufsicht (TA) der AD-Leitstelle geeignete Maßnahmen ein um das Fahrzeug in den personenfreien Zustand zu bewegen.
  - ► Sobald das Fahrzeug personenfrei ist, meldet die Technische Aufsicht (TA) dieses an das AD-Bordsystem.
- Das AD-Bordsystem leitet, sofern erforderlich die Türschließung ein → UC-06 Türkontrolle.
  Hinweis:
  Es kann sein, daß der letzte Fahrgast bereits bei einer früheren Halteposition / Haltestelle ausgestiegen ist, weshalb jetzt an der Endhaltestelle keine Türöffnung angefordert wurde, folglich müssen die geschlossenen Türen nicht noch einmal geschlossen werden.

  Sofern die Türschließung erforderlich ist, gilt:
  - ► UC-03 Leerfahrt → UC-06 Türkontrolle → UC-45 MissionCtrl → UC-03 Leerfahrt.
  - ► alternativ wird UC-06 übersprungen und UC-45 führt direkt auf UC-03.
- Das AD-Bordsystem informiert (über 14) den ÖV-Bordrechner über die Türschließung damit dieser die Aktualisierung der Anzeiger veranlassen kann.
- Der ÖV-Bordrechner setzt über UC-18 Zielbeschilderung außen und innen ändern die Außen- und Innenanzeiger (über 9 und 11) für die Fahrt gemäß Fahrplan.
  Hinweis:
  Eine Meldung bezüglich der Umsetzung an die ÖV-Leitstelle ist nicht erforderlich.

Hinweis:
Sofern Leerfahrten im Betrieb erforderlich werden, so können diese jederzeit als Fahrplanänderung über UC-14 Umlaufänderung bzw. UC-13 Fahrtänderung eingebracht werden → siehe Aktionen 3.Fall.

Aktionen (2.Fall Leerfahrt als Aussetzfahrt des Regelbetriebes):

- Dieser Fall von UC-03 wird mit dem Erreichen des BHMS zu UC-44 Fahrt im Depot.
  Verhält sich wie Aktionen 1.Fall, aber die Leerfahrt führt von der Endhaltestelle zum BHMS und folgt dem vom BHMS vorgegebenen Prozeß mit dem Übergang der Zuständigkeit, z.B. Parken.

Aktionen (3.Fall Leerfahrt als Rangierfahrt des Sonderbetriebes):

- Der Planer des ÖPNV-Unternehmens hat im Fahrplan Leerfahrten von vorn herein eingeplant oder der ÖV-Disponent nimmt eine Fahrplanänderung über *UC-14 Umlaufänderung* bzw. *UC-13 Fahrtänderung* vor, welches in diesem Fall zu einer Leerfahrt führt.
  Hinweis:
  Insbesondere bei kleine ÖPNV-Unternehmen kann der ÖV-Disponent auch mit den logistischen Aufgaben der Planung, den Service und der technische Wartung der Fahrzeuge in Personalunion verantwortlich sein.

Juristische Anforderungen:

- AFGBV §5 Absatz 5
  Die Hersteller und die Halter von Kraftfahrzeugen mit autonomer Fahrfunktion sind verpflichtet
  ► das Kraftfahrt-Bundesamt bei der Durchführung der Marktüberwachungstätigkeiten zu unterstützen und
  ► dem Kraftfahrt-Bundesamt auf Verlangen die für die Marktüberwachung erforderlichen Unterlagen und Informationen sowie andere technische Spezifikationen unentgeltlich bereitzustellen, wobei die Hersteller auf Verlangen auch einen Zugang zu Software und Algorithmen ermöglichen müssen.
- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA)
  → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
  Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
  Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.1 Generelle Kollisionsvermeidung
  Kollisionen mit anderen Verkehrsteilnehmenden und unbeteiligten Dritten müssen vermieden werden, sofern dies durch
  1. Notbremseingriffe oder
  2. andere Teilnehmende des umgebenden Verkehrs, andere unbeteiligte Dritte oder die Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nicht gefährdende Ausweichmanöver möglich ist. Kann eine Kollision zur Abwendung einer Gefährdung des Lebens der Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nur durch eine Gefährdung des Lebens anderer Teilnehmender des umgebenden Verkehrs oder unbeteiligter Dritter vermieden werden (unvermeidbare alternative Gefährdung von Menschenleben), darf der Schutz der anderen Teilnehmenden des umgebenden Verkehrs und der unbeteiligten Dritten nicht nachrangig gegenüber dem Schutz der Insassen des autonom fahrenden Kraftfahrzeugs erfolgen.

- AFGBV Anlage 1 Teil 1 Abschnitt 1.2 Interaktion mit anderen Verkehrsteilnehmenden
  a) Vorausfahrende Verkehrsteilnehmende auf der Fahrbahn werden erkannt. Es wird jederzeit in jedem Geschwindigkeitsbereich und in jeder möglichen Fahrsituation ein angemessener Sicherheitsabstand eingehalten. Der einzuhaltende Sicherheitsabstand bestimmt sich nach § 4 der Straßenverkehrs-Ordnung.
  b) Der Fahrstreifenwechsel vorausfahrender oder nachfolgender Fahrzeuge, der von einem benachbarten Fahrstreifen in den eigenen Fahrstreifen oder aus dem eigenen Fahrstreifen heraus in einen benachbarten Fahrstreifen erfolgt, wird erkannt und bei der Fahraufgabe entsprechend berücksichtigt.
  c) Situationen, welche einen Fahrstreifenwechsel bedingen (beispielsweise anhaltende oder langsame Fahrzeuge auf der Fahrbahn, Ende eines Fahrstreifens), werden erkannt und geeignete Manöver zum Fahrstreifenwechsel werden sicher durchgeführt.
  d) Einsatzfahrzeuge werden erkannt und geeignete Fahrmanöver sicher durchgeführt.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.3 Planung der Fahrpfade und Geschwindigkeiten
  Bei Geschwindigkeitsanpassungen kommt es zu keiner vermeidbaren Beeinträchtigung von Insassen, anderen Verkehrsteilnehmenden und unbeteiligten Dritten. Es gelten folgende Anforderungen:
  a) Geschwindigkeitsbeschränkungen und Änderungen der Geschwindigkeitsbeschränkung werden erkannt und die Geschwindigkeit wird entsprechend angepaßt.
  b) Besondere Anforderungen an die Geschwindigkeit werden erkannt und im Geschwindigkeits- und Fahrtverlauf befolgt (beispielsweise in Bereichen vor Schulen und an Arbeitsstellen an Straßen, an Bushaltestellen, Bahnübergängen, in engen Kurvenradien oder bei Gefällen, in Engstellen, in denen der eigene Fahrstreifen vom Gegenverkehr mitbenutzt werden muß).
  c) Zeichen und Weisungen der Polizeibeamten gemäß § 36 der Straßenverkehrs-Ordnung, Wechsellichtzeichen gemäß § 37 der Straßenverkehrs-Ordnung, sonstige Zeichen gemäß der §§ 39 bis 42 der Straßenverkehrs-Ordnung sowie Verkehrseinrichtungen gemäß § 43 der Straßenverkehrs-Ordnung werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  d) Situationen, in denen die Vorfahrt anderen gewährt werden muß (beispielsweise vor Fußgängerüberwegen, in Kreuzungsbereichen oder Einmündungen), werden erkannt und ohne Gefährdung oder Behinderung der Vorfahrtberechtigten bewältigt. Es ist eine berechnete Zeit bis zum Aufprall von mehr als drei Sekunden bezüglich des Vorfahrtberechtigen einzuhalten. Wird von diesen Werten abgewichen, muß dies ausreichend begründet und auf Basis von systematischen Sicherheitsbewertungen nach dem Stand der Technik dokumentiert werden. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO 26262:2018-12 Straßenfahrzeuge – Funktionale Sicherheit1 erfüllt werden.
  e) Bauliche Straßengestaltungen mit Auswirkung auf das Verhaltensrecht (beispielsweise bis zu 5 Meter vom Fahrbahnrand einer vorfahrtberechtigten Straße abgesetzte Radwege nach § 9 Absatz 3 der Straßenverkehrs-Ordnung oder abgesenkte Bordsteine nach § 10 der Straßenverkehrs-Ordnung) werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  f) Arbeitsstellen an Straßen, temporär veränderte Fahrbahnverläufe oder Fahrbahnmarkierungen werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  g) Defizite am Zubehör, insbesondere der Verkehrseinrichtungen (zum Beispiel verschlissene, beschädigte, fehlende oder defekte temporäre oder dauerhafte Fahrbahnmarkierungen und Verkehrszeichen, Phantommarkierungen) und der Straßenausstattung, insbesondere solcher nach vorstehenden Buchstaben a bis f werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Dies gilt insbesondere nach Sturm- und sonstigen Witterungsereignissen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.4 Reaktion auf Umweltbedingungen
  Wetter-, Umwelt- und Straßeninfrastrukturbedingungen (beispielsweise Regen, Sichtbehinderung durch Rauch, Schlaglöcher) werden im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Fahrpfad und Geschwindigkeit sind – bis hin zum Stillstand des Fahrzeugs – so zu wählen, daß die in den Nummern 1.1 bis 1.3 gestellten Anforderungen auch bei geänderten Umweltbedingungen erfüllt werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 3 Notfahrfunktion
  Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit einer Notfahrfunktion ausgestattet sein. Muß sich das Kraftfahrzeug im Falle eines Defekts am Kraftfahrzeug in den risikominimalen Zustand versetzen, muß dies mit der Notfahrfunktion erfolgen. Fahrten mit der Notfahrfunktion dürfen nur bei Schrittgeschwindigkeit und aktivierter Warnblinkanlage erfolgen. Der Übergang der autonomen Fahrfunktion aus der normalen Fahrt in die Fahrt mit der Notfahrfunktion ist von dieser Geschwindigkeitsbegrenzung ausgenommen, sofern ein Abbremsen erforderlich ist.
- AFGBV Anlage 1 Teil 1 Abschnitt 4 Manueller Fahrbetrieb
  Im manuellen Fahrbetrieb erfüllt eine fahrzeugführende Person die Fahraufgabe. Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit Vorrichtungen ausgestattet sein, die es einer fahrzeugführenden Person ermöglichen, die Fahraufgabe wahrzunehmen. Ist die Steuerung im manuellen Fahrbetrieb auf Geschwindigkeiten nicht höher als Schrittgeschwindigkeit begrenzt, ist es nicht erforderlich, daß die fahrzeugführende Person sich innerhalb des Kraftfahrzeugs mit autonomer Fahrfunktion aufhält. Die Steuerung kann in diesem Fall über eine im Nahfeld des Kraftfahrzeugs befindliche Fernsteuerung ausgeführt werden. Die maximale Distanz, über die eine Fernsteuerung möglich ist, beträgt 6 Meter, gemessen in gerader Verbindung. Die Einhaltung der maximalen Distanz ist vom Hersteller durch geeignete technische Mittel sicher zu stellen. Soll das Kraftfahrzeug mit autonomer Fahrfunktion im manuellen Fahrbetrieb mit

Geschwindigkeiten höher als Schrittgeschwindigkeit gesteuert werden, muß es mit einem Sitzplatz für die fahrzeugführende Person ausgestattet sein. Der Sitzplatz ist entsprechend der geltenden Vorschriften zu gestalten.

- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.1 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur dynamischen Ausübung der Fahraufgabe gilt:
  a) Zur dauerhaften Überwachung der technischen Ausrüstung werden nicht personenbezogene technische Daten im Kraftfahrzeug erhoben und gespeichert.
  b) Eine Beeinträchtigung der technischen Ausrüstung ist der Technischen Aufsicht unverzüglich anzuzeigen.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.2 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und mit konventionellen Vorrichtungen zur Ausübung der Fahraufgabe gilt:
  Die autonome Fahrfunktion darf nicht erneut aktivierbar sein, solange eine Beeinträchtigung der technischen Ausrüstung besteht.
- AFGBV Anlage 1 Teil 1 Abschnitt 6 Übertragung von Daten an das Kraftfahrzeug
  Die zur selbstständigen Bewältigung der Fahraufgabe im autonomen Betrieb notwendigen Daten und Informationen von externen technischen Einheiten (beispielsweise Backends oder Server eines Anbieters, externe Sensoren, Smartphone) müssen vom Kraftfahrzeug sicher empfangen und verwendet werden können. Daten externer Einheiten können im Kraftfahrzeug zur Ausführung der autonomen Fahrfunktionen verwendet werden. Daten und Informationen können beispielsweise bei bestimmten Anwendungsfällen über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) von einer externen technischen Einheit an das Kraftfahrzeug und vom Kraftfahrzeug an eine technische Einheit übertragen werden. Die Übertragung solcher Daten muß insbesondere den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und nach dem aktuellen Stand der Technik abgesichert sein. Das Absicherungskonzept muß die in einer Bedrohungsanalyse identifizierten Risiken mit wirksamen Maßnahmen adressieren und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten. Zur Datenübertragung sollte eine zentrale sichere elektronische Steuereinheit (SECU) genutzt werden. Die SECU dient als Informationsgateway im Kraftfahrzeug. Die SECU kommuniziert intern an die Kommunikationsbusse des Kraftfahrzeugs und an den physischen On-Board-Diagnose II-Anschluß (OBD II) oder an eine proprietäre Schnittstelle eines Herstellers. Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung sind Teil 5 zu entnehmen. Die Integrität, Authentizität und Verfügbarkeit der Datenübertragung sind sicherzustellen. Die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen oder mit Infrastrukturkomponenten ist zulässig. Sie muß auf der Basis einer Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 insbesondere den Anforderungen an die Informationstechnik nach Teil 5 und damit den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen. Während des Betriebs in einer optionalen Testphase ist die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen und Infrastrukturkomponenten zu testen und gegebenenfalls anzupassen.
- AFGBV Anlage 1 Teil 1 Abschnitt 7.1 Betriebshandbuch
  Zweck des Betriebshandbuchs ist es, mittels detaillierter Vorgaben den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten und der Technischen Aufsicht die richtige Reaktion auf Fehlerfälle zu ermöglichen.
- AFGBV Anlage 1 Teil 1 Abschnitt 8 Sensorik
  Zur technischen Umsetzung der autonomen Fahrfunktion muß eine Sensorik verwendet werden, die alle für die sichere Erfüllung der Fahraufgabe erforderlichen Gegenstände, Daten oder Personen im Umfeld des Kraftfahrzeugs erfaßt und hinsichtlich der Verarbeitung personenbezogener Daten die Vorgaben der Verordnung (EU) 2016/679, des Bundesdatenschutzgesetzes und spezialgesetzlicher datenschutzrechtlicher Vorschriften beachtet. Zur Erfüllung des in Satz 1 genannten Zwecks und unter Einhaltung der genannten Vorgaben kann die Sensorik durch externe Systeme unterstützt werden. Beeinflussen Wetter-, Umwelt- und Infrastrukturbedingungen die Leistungsfähigkeit der Sensorik, werden von der technischen Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion Maßnahmen eingeleitet, um die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken auszugleichen. Die Sensorik ist in das Sicherheitskonzept des Kraftfahrzeugs mit autonomer Fahrfunktion nach Nummer 7.2 und in die permanente Systemüberwachung nach Nummer 5 einzubinden.
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und

den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.

- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).
- AFGBV Anlage 2 Datenspeicherung → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).

Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.
- BOStrab §4 Absatz 2
  Betriebsanlagen und Fahrzeuge sind instandzuhalten. Treten an ihnen während des Betriebes Mängel auf, die die Betriebssicherheit beeinträchtigen können, sind sie ganz oder teilweise außer Betrieb zu nehmen und erforderlichenfalls abzusichern.
- BOStrab §4 Absatz 4
  Durch betriebliche Vorkehrungen ist dafür zu sorgen, daß Betriebsstörungen zügig beseitigt werden, bei Unfällen und gefährlichen Ereignissen unverzüglich Hilfe geleistet wird und insbesondere bei Brandfällen die Möglichkeit zur Selbst- oder Fremdrettung von Personen oder eine Kombination von beidem in Abhängigkeit von den lokalen Verhältnissen besteht.
- BOStrab § 23 Absatz 3
  Bei Fahrbetrieb ohne Fahrzeugführer müssen nachrichtentechnische Anlagen vorhanden sein, die eine vorrangige Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle ermöglichen.
  Hinweis:
  Die Sprechverbindung ist Teil der eingeleiteten Maßnahmen der Technischen Aufsicht (TA) der AD-Leitstelle, wenn sich Personen im Fahrgastraum befinden, wo diese sich bei Leerfahrten nicht aufhalten dürfen.
- BOStrab §43 Absatz 5 Punkt 3
  bei Fahrbetrieb ohne Fahrzeugführer sicherstellen, daß Züge nur bei geschlossenen Türen anfahren können
- BOStrab §52 Absatz 3
  Betriebsanlagen oder Fahrzeuge, die ganz oder teilweise selbsttätig arbeiten oder fernbedient werden, müssen im Rahmen der betrieblichen Erfordernisse von Betriebsbediensteten auf einwandfreie Funktion überwacht werden.

Gefahren nach HAZOP:

- Die potentiellen Gefahren entsprechen den typischen Gefahren der Teilnahme am Straßenverkehr
  - ► Gefahr eines Unfalles, das autonom fahrende Fahrzeug erkennt z.B. einen (oder mehrere) Fußgänger nicht, weshalb es zu einem Unfall kommt ➔ Die Schwere der Verletzung (bis hin zum Tod) der betroffenen Person(en) hängt von den Geschwindigkeiten der Objekte (Fahrzeug und betroffene Verkehrsteilnehmer) bzw. physikalisch, der resultierenden kinetischen einwirkenden Energie ab.
    Hinweis:
    Diese Gefährdung wird vom Fahrzeughersteller (OEM) verantwortet, gemäß
    AFGBV §12 Anforderungen an den Hersteller Absatz 1 Punkt 2
    Der Hersteller eines Kraftfahrzeugs mit autonomer Fahrfunktion hat
    ein Sicherheitskonzept zur funktionalen Sicherheit nach Anlage I Nummer 7.2 zu erstellen, und dabei
    a) auf Basis dieses Sicherheitskonzeptes eine Gefährdungsanalyse nach Anlage I Ziffer 7.2.1 durchzuführen,
    b) das Sicherheitskonzept nach Anlage III Ziffer 3 zu dokumentieren,
    c) die Sicherheit der autonomen Fahrfunktion entsprechend dieses Sicherheitskonzepts zu überprüfen und die Sicherheit gegenüber dem Kraftfahrt-Bundesamt nach den Anforderungen nach Anlage I Ziffer 10 nachzuweisen.
    Hinweis:
    Die Sicherheit wird durch Maßnahmen erzielt, welche in den diversen, bekannten Fahrerassistenzsystemen im Fahrzeug implementiert sind, dazu zählen z.B.
    - *Adaptive Cruise Control (ACC) = Abstandsregeltempomat,*
    - *Advanced Emergency Braking System (AEBS) = Notbremsassistenzsystems,*
    - *Elektronische Stabilitäts-Programm (ESP),*
    - *… .*

- Gefahr eines Unfalles, welcher auf das autonom fahrende Fahrzeug durch andere Verkehrsteilnehmer (Fahrzeuge, Personen) außerhalb des Fahrzeuges ausgeübt wird.
  Hinweis:
  Dieses ist ebenfalls Bestandteil der Gefährdungsanalyse des Fahrzeugherstellers (OEM), weshalb dieses hier nicht noch einmal betrachtet wird.

Wichtig:
Das Funktionale Sicherheitskonzept (FSK) des Fahrzeugherstellers (OEM) kann vom Halter Sicherheits-Maßnahmen zum Betrieb einfordern. Dazu zählt insbesondere der (Remote-)Sicherheitsfahrer bei SAE ≤ 3 bzw. die Überwachung, speziell der Fahrt ($W_{kin} > 0$), durch eine qualifizierte Technische Aufsicht (TA) bei SAE ≥ 4.

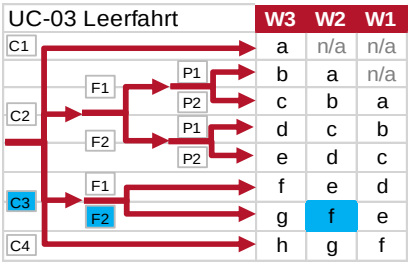
AFGBV §13 Anforderungen an den Halter Absatz 6
Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.

Hinweis:
In diesem Use Case reduziert sich die Gefährdung von SG2, weil bei Leerfahrten keine Fahrgäste existent sind, weshalb auch keine Personenschäden von Fahrzeuginsassen auftreten können.

Hinweis:
Die Gefahr für andere Vulnerable Road User (VRU) ≙ verwundbare Verkehrsteilnehmer bleibt auch dann unverändert bestehen, wenn sich keine Fahrgäste im Fahrzeuginneren aufhalten. (SG1 bleibt unverändert bestehen).

Hinweis:
Dieser UC ruft UC-06 Türkontrolle bzw. UC-18 Zielbeschilderung außen und innen ändern auf, die daraus resultierende Risikobewertung ist jeweils dort hinterlegt.

Risikograph:



≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	C3 Tod mehrerer Personen durch den gefährlichen Vorfall.
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich

3.2.4 UC-04 Fahrgastfahrt

Das Fahrzeug befindet sich an dem Haltepunkt / Haltestelle, von wo aus die nächste, geplante Mission (Abfahrtpunkt), gemäß dem Fahrplan der ÖV-Leitstelle, startet.

Hinweis:
Die Fahrplandaten
► Umlauf = Sequenz von Fahrten, vom Ausrücken aus dem Betriebshof bis zum Einrücken in den Betriebshof,
► Fahrt = Bewegung eines Fahrzeugs vom Startpunkt bis zum Endpunkt eines Fahrweges,
► Fahrweg = Route = Abfolge von geplanten Haltepunkten und ggf. Zwischenpunkten, die den Streckenverlauf eindeutig festlegen.
► Fahrauftrag = definiert die Vorgabe (Fahrgastfahrt, Leerfahrt, Fahrt im Depot) für die Bewegung eines Fahrzeugs.
► Mission = Teil einer Fahrt zwischen zwei Haltepunkten / Haltestellen und beinhaltet Angaben zum Fahrgastwechsel, Haltezeit, …
wurden bereits in UC-02 Umlaufanmeldung/-zuweisung (ÖV-Bordrechner) bzw. UC-44 Fahrt im Depot (AD-Bordsystem) an das Fahrzeug übermittelt. Diese können jederzeit über UC-14 Umlaufänderung bzw. UC-13 Fahrtänderung aktualisiert oder erweitert werden. Sofern erforderlich werden die Außen- und Innenanzeigen über UC-18 Zielbeschilderung außen und innen ändern aktualisiert.

Hinweis:
Es ist nicht zwingend notwendig, bereits zu Beginn der Fahrt alle Missionen an das Fahrzeug zu senden, ein gewisser „Vorrat" an Missionen auf dem Fahrzeug ist jedoch zweckmäßig.

Solange eine weitere Mission vorhanden und diese per fahrzeugseitiger Prüfung ausführbar ist, führt das Fahrzeug die Mission aus, wobei UC-45 MissionCtrl zwischen den einzelnen, differenzierten Verfahren des Fahrauftrages separiert und den zugehörigen Prozeßablauf einleitet, hier wird nur die Fahrgastfahrt (mit / ohne Fahrgast) selbst betrachtet.

Hinweis:
Die Fahrgastfahrt beginnt mit dem Schließen der Tür (sofern erforderlich) und der Abfahrt von dem Haltepunkt / der Haltestelle. Die Mission ist abgeschlossen, wenn das Fahrzeug den nächsten Haltepunkt / Haltestelle erreicht hat, sofern vorgesehen ein Fahrgastwechsel (UC-04 → UC-05 Regelhalt → UC-06 Türkontrolle) stattfindet und dort die Mindesttüröffnungsdauer verstrichen ist.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Überwachung der Fahrplanumsetzung auf Einhaltung der in UC-02 Umlaufanmeldung/-zuweisung übermittelten Fahrplandaten inklusive Pünktlichkeit. Informieren der Fahrgäste über Abweichungen gegenüber dem Fahrplan inklusive Unterstützung bei der Sicherstellung des reibungslosen Reiseablaufes der Fahrgäste. Sofern erforderlich Aktualisierung der Fahrplandaten über UC-14 Umlaufänderung oder UC-13 Fahrtänderung.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung).
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. Überprüfung (vor der Abfahrt), daß die Türen sicher verschlossen sind und während der Fahrt verschlossen bleiben.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Eine Fahrgastfahrt ist eine Fahrt, welche für die Nutzung durch Fahrgäste vorgesehen ist, unabhängig davon ob ein oder mehrere Fahrgäste davon Gebrauch machen.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Fahrzeug ist im Betrieb (Regelbetrieb) und setzt die Missionen der ÖV-Leitstelle *(außerhalb des BHMS)* um.
Hinweis:
Innerhalb des BHMS gibt es keine Fahrgastfahrt, nur UC-44 Fahrt im Depot.

Aktionen:

- Das AD-Bordsystem setzt den Missionswechsel (über UC-45 MissionCtrl) um, welches in Abhängigkeit des Fahrauftrages und der Missionsparameter die klassische UC-04 Fahrgastfahrt startet.

- Das AD-Bordsystem leitet, sofern erforderlich, die Türschließung ein → UC-06 Türkontrolle.
  Hinweis:
  Es besteht die Möglichkeit, daß sich kein Fahrgast im Fahrzeug befindet oder kein Fahrgast einen Aussteigewunsch durch eine Betätigung des Halteknopfes äußern kann plus daß an der Halteposition / Haltestelle keine wartenden, potentiellen Fahrgäste erkannt werden, weshalb der geplante Halt übersprungen wird, d.h. das Fahrzeug fährt ohne Halt weiter. Somit ist es nicht erforderlich die geschlossenen Türen erneut zu schließen.
- Das AD-Bordsystem startet die Mission mit der Abfahrt und das Fahrzeug fährt autonom, gesteuert durch das AD-Bordsystem mit überwachten, geschlossenen Türen. Das AD-Bordsystem sendet kontinuierlich die Standortdaten (GPS) in Korrelation zur hochauflösenden Karte plus weitere technische Daten zur Umsetzungsüberwachung (inklusive der Sicherstellung des Festhalten der Türen in geschlossener Stellung während der Fahrt → UC-06 Türkontrolle) bis der Zielpunkt erreicht ist.
  Hinweis:
  Der Wegpunkt / Zielpunkt unterliegt gedanklich einem Jitter, d.h. Einerseits ist der Zielpunkt der Haltepunkt der Haltestelle, andererseits startet die KI gestützte Fahrgasterkennung, ab den Zeitpunkt wenn der Haltepunkt / Haltestelle sicher detektiert werden kann, (welches von den Kurven des Straßenverlaufes abhängt).
  Die Umsetzung erfolgt in der Software des AD-Bordsystems in der Unit-Ebene.
- Das AD-Bordsystem überwacht den Fahrweg gemäß der vorgegebenen Routenführung (Wegpunkte) infolge des Fahrplans der ÖV-Leitstelle bis zum Erreichen des Zielpunktes.
- Sofern ein Fahrgastwechsel, gemäß der Planung der ÖV-Leitstelle, erlaubt ist,
  - ► startet das AD-Bordsystem die KI gestützte Fahrgasterkennung.
  - ► Sofern ein wartender, potentieller Fahrgast erkannt wird oder ein, sich im Fahrzeug befindender, Fahrgast den Haltewunsch über den Halteknopf ausgelöst hat, dann wird der UC-05 Regelhalt umgesetzt, andernfalls übersprungen → Weiterfahrt ohne Halt.
- Weiter mit nächster Mission (UC-05 Regelhalt) umgesetzt / übersprungen → UC-45 MissionCtrl)

Hinweis:
Die Umsetzung der Schritte wird vom AD-Bordsystem (über 8) an die AD-Leitstelle sowie (über 14) an den ÖV-Bordrechner gemeldet. Der ÖV-Bordrechner überwacht die Umsetzung und Einhaltung der ÖV-Fahrplanung und meldet gemäß den Vorgaben der Geschäftsprozesse des ÖPNV die gewünschten Informationen, ggf. klassifiziert und priorisiert an die ÖV-Leitstelle.

Juristische Anforderungen:

- AFGBV §5 Absatz 5
  Die Hersteller und die Halter von Kraftfahrzeugen mit autonomer Fahrfunktion sind verpflichtet
  ► das Kraftfahrt-Bundesamt bei der Durchführung der Marktüberwachungstätigkeiten zu unterstützen und
  ► dem Kraftfahrt-Bundesamt auf Verlangen die für die Marktüberwachung erforderlichen Unterlagen und Informationen sowie andere technische Spezifikationen unentgeltlich bereitzustellen, wobei die Hersteller auf Verlangen auch einen Zugang zu Software und Algorithmen ermöglichen müssen.
- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA)
  → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
  Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
  Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind.

- AFGBV Anlage 1 Teil 1 Abschnitt 1.1 Generelle Kollisionsvermeidung
  Kollisionen mit anderen Verkehrsteilnehmenden und unbeteiligten Dritten müssen vermieden werden, sofern dies durch
  1. Notbremseingriffe oder
  2. andere Teilnehmende des umgebenden Verkehrs, andere unbeteiligte Dritte oder die Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nicht gefährdende Ausweichmanöver
  möglich ist. Kann eine Kollision zur Abwendung einer Gefährdung des Lebens der Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nur durch eine Gefährdung des Lebens anderer Teilnehmender des umgebenden Verkehrs oder unbeteiligter Dritter vermieden werden (unvermeidbare alternative Gefährdung von Menschenleben), darf der Schutz der anderen Teilnehmenden des umgebenden Verkehrs und der unbeteiligten Dritten nicht nachrangig gegenüber dem Schutz der Insassen des autonom fahrenden Kraftfahrzeugs erfolgen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.2 Interaktion mit anderen Verkehrsteilnehmenden
  a) Vorausfahrende Verkehrsteilnehmende auf der Fahrbahn werden erkannt. Es wird jederzeit in jedem Geschwindigkeitsbereich und in jeder möglichen Fahrsituation ein angemessener Sicherheitsabstand eingehalten. Der einzuhaltende Sicherheitsabstand bestimmt sich nach § 4 der Straßenverkehrs-Ordnung.
  b) Der Fahrstreifenwechsel vorausfahrender oder nachfolgender Fahrzeuge, der von einem benachbarten Fahrstreifen in den eigenen Fahrstreifen oder aus dem eigenen Fahrstreifen heraus in einen benachbarten Fahrstreifen erfolgt, wird erkannt und bei der Fahraufgabe entsprechend berücksichtigt.
  c) Situationen, welche einen Fahrstreifenwechsel bedingen (beispielsweise anhaltende oder langsame Fahrzeuge auf der Fahrbahn, Ende eines Fahrstreifens), werden erkannt und geeignete Manöver zum Fahrstreifenwechsel werden sicher durchgeführt.
  d) Einsatzfahrzeuge werden erkannt und geeignete Fahrmanöver sicher durchgeführt.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.3 Planung der Fahrpfade und Geschwindigkeiten
  Bei Geschwindigkeitsanpassungen kommt es zu keiner vermeidbaren Beeinträchtigung von Insassen, anderen Verkehrsteilnehmenden und unbeteiligten Dritten. Es gelten folgende Anforderungen:
  a) Geschwindigkeitsbeschränkungen und Änderungen der Geschwindigkeitsbeschränkung werden erkannt und die Geschwindigkeit wird entsprechend angepaßt.
  b) Besondere Anforderungen an die Geschwindigkeit werden erkannt und im Geschwindigkeits- und Fahrtverlauf befolgt (beispielsweise in Bereichen vor Schulen und an Arbeitsstellen an Straßen, an Bushaltestellen, Bahnübergängen, in engen Kurvenradien oder bei Gefällen, in Engstellen, in denen der eigene Fahrstreifen vom Gegenverkehr mitbenutzt werden muß).
  c) Zeichen und Weisungen der Polizeibeamten gemäß § 36 der Straßenverkehrs-Ordnung, Wechsellichtzeichen gemäß § 37 der Straßenverkehrs-Ordnung, sonstige Zeichen gemäß der §§ 39 bis 42 der Straßenverkehrs-Ordnung sowie Verkehrseinrichtungen gemäß § 43 der Straßenverkehrs-Ordnung werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  d) Situationen, in denen die Vorfahrt anderen gewährt werden muß (beispielsweise vor Fußgängerüberwegen, in Kreuzungsbereichen oder Einmündungen), werden erkannt und ohne Gefährdung oder Behinderung der Vorfahrtberechtigten bewältigt. Es ist eine berechnete Zeit bis zum Aufprall von mehr als drei Sekunden bezüglich des Vorfahrtberechtigen einzuhalten. Wird von diesen Werten abgewichen, muß dies ausreichend begründet und auf Basis von systematischen Sicherheitsbewertungen nach dem Stand der Technik dokumentiert werden. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO 26262:2018-12 Straßenfahrzeuge – Funktionale Sicherheit1 erfüllt werden.
  e) Bauliche Straßengestaltungen mit Auswirkung auf das Verhaltensrecht (beispielsweise bis zu 5 Meter vom Fahrbahnrand einer vorfahrtberechtigten Straße abgesetzte Radwege nach § 9 Absatz 3 der Straßenverkehrs-Ordnung oder abgesenkte Bordsteine nach § 10 der Straßenverkehrs-Ordnung) werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  f) Arbeitsstellen an Straßen, temporär veränderte Fahrbahnverläufe oder Fahrbahnmarkierungen werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  g) Defizite am Zubehör, insbesondere der Verkehrseinrichtungen (zum Beispiel verschlissene, beschädigte, fehlende oder defekte temporäre oder dauerhafte Fahrbahnmarkierungen und Verkehrszeichen, Phantommarkierungen) und der Straßenausstattung, insbesondere solcher nach vorstehenden Buchstaben a bis f werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Dies gilt insbesondere nach Sturm- und sonstigen Witterungsereignissen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.4 Reaktion auf Umweltbedingungen
  Wetter-, Umwelt- und Straßeninfrastrukturbedingungen (beispielsweise Regen, Sichtbehinderung durch Rauch, Schlaglöcher) werden im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Fahrpfad und Geschwindigkeit sind – bis hin zum Stillstand des Fahrzeugs – so zu wählen, daß die in den Nummern 1.1 bis 1.3 gestellten Anforderungen auch bei geänderten Umweltbedingungen erfüllt werden.

- AFGBV Anlage 1 Teil 1 Abschnitt 3 Notfahrfunktion
  Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit einer Notfahrfunktion ausgestattet sein. Muß sich das Kraftfahrzeug im Falle eines Defekts am Kraftfahrzeug in den risikominimalen Zustand versetzen, muß dies mit der Notfahrfunktion erfolgen. Fahrten mit der Notfahrfunktion dürfen nur bei Schrittgeschwindigkeit und aktivierter Warnblinkanlage erfolgen. Der Übergang der autonomen Fahrfunktion aus der normalen Fahrt in die Fahrt mit der Notfahrfunktion ist von dieser Geschwindigkeitsbegrenzung ausgenommen, sofern ein Abbremsen erforderlich ist.
- AFGBV Anlage 1 Teil 1 Abschnitt 4 Manueller Fahrbetrieb
  Im manuellen Fahrbetrieb erfüllt eine fahrzeugführende Person die Fahraufgabe. Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit Vorrichtungen ausgestattet sein, die es einer fahrzeugführenden Person ermöglichen, die Fahraufgabe wahrzunehmen. Ist die Steuerung im manuellen Fahrbetrieb auf Geschwindigkeiten nicht höher als Schrittgeschwindigkeit begrenzt, ist es nicht erforderlich, daß die fahrzeugführende Person sich innerhalb des Kraftfahrzeugs mit autonomer Fahrfunktion aufhält. Die Steuerung kann in diesem Fall über eine im Nahfeld des Kraftfahrzeugs befindliche Fernsteuerung ausgeführt werden. Die maximale Distanz, über die eine Fernsteuerung möglich ist, beträgt 6 Meter, gemessen in gerader Verbindung. Die Einhaltung der maximalen Distanz ist vom Hersteller durch geeignete technische Mittel sicher zu stellen. Soll das Kraftfahrzeug mit autonomer Fahrfunktion im manuellen Fahrbetrieb mit Geschwindigkeiten höher als Schrittgeschwindigkeit gesteuert werden, muß es mit einem Sitzplatz für die fahrzeugführende Person ausgestattet sein. Der Sitzplatz ist entsprechend der geltenden Vorschriften zu gestalten.
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.1 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur dynamischen Ausübung der Fahraufgabe gilt:
  a) Zur dauerhaften Überwachung der technischen Ausrüstung werden nicht personenbezogene technische Daten im Kraftfahrzeug erhoben und gespeichert.
  b) Eine Beeinträchtigung der technischen Ausrüstung ist der Technischen Aufsicht unverzüglich anzuzeigen.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.2 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und mit konventionellen Vorrichtungen zur Ausübung der Fahraufgabe gilt:
  Die autonome Fahrfunktion darf nicht erneut aktivierbar sein, solange eine Beeinträchtigung der technischen Ausrüstung besteht.
- AFGBV Anlage 1 Teil 1 Abschnitt 6 Übertragung von Daten an das Kraftfahrzeug
  Die zur selbstständigen Bewältigung der Fahraufgabe im autonomen Betrieb notwendigen Daten und Informationen von externen technischen Einheiten (beispielsweise Backends oder Server eines Anbieters, externe Sensoren, Smartphone) müssen vom Kraftfahrzeug sicher empfangen und verwendet werden können. Daten externer Einheiten können im Kraftfahrzeug zur Ausführung der autonomen Fahrfunktionen verwendet werden. Daten und Informationen können beispielsweise bei bestimmten Anwendungsfällen über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) von einer externen technischen Einheit an das Kraftfahrzeug und vom Kraftfahrzeug an eine technische Einheit übertragen werden. Die Übertragung solcher Daten muß insbesondere den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und nach dem aktuellen Stand der Technik abgesichert sein. Das Absicherungskonzept muß die in einer Bedrohungsanalyse identifizierten Risiken mit wirksamen Maßnahmen adressieren und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten. Zur Datenübertragung sollte eine zentrale sichere elektronische Steuereinheit (SECU) genutzt werden. Die SECU dient als Informationsgateway im Kraftfahrzeug. Die SECU kommuniziert intern an die Kommunikationsbusse des Kraftfahrzeugs und an den physischen On-Board-Diagnose II-Anschluß (OBD II) oder an eine proprietäre Schnittstelle eines Herstellers. Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung sind Teil 5 zu entnehmen. Die Integrität, Authentizität und Verfügbarkeit der Datenübertragung sind sicherzustellen. Die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen oder mit Infrastrukturkomponenten ist zulässig. Sie muß auf der Basis einer Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 insbesondere den Anforderungen an die Informationstechnik nach Teil 5 und damit den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen. Während des Betriebs in einer optionalen Testphase ist die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen und Infrastrukturkomponenten zu testen und gegebenenfalls anzupassen.
- AFGBV Anlage 1 Teil 1 Abschnitt 7.1 Betriebshandbuch
  Zweck des Betriebshandbuchs ist es, mittels detaillierter Vorgaben den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten und der Technischen Aufsicht die richtige Reaktion auf Fehlerfälle zu ermöglichen.
- AFGBV Anlage 1 Teil 1 Abschnitt 8 Sensorik
  Zur technischen Umsetzung der autonomen Fahrfunktion muß eine Sensorik verwendet werden, die alle für

die sichere Erfüllung der Fahraufgabe erforderlichen Gegenstände, Daten oder Personen im Umfeld des Kraftfahrzeugs erfaßt und hinsichtlich der Verarbeitung personenbezogener Daten die Vorgaben der Verordnung (EU) 2016/679, des Bundesdatenschutzgesetzes und spezialgesetzlicher datenschutzrechtlicher Vorschriften beachtet. Zur Erfüllung des in Satz 1 genannten Zwecks und unter Einhaltung der genannten Vorgaben kann die Sensorik durch externe Systeme unterstützt werden. Beeinflussen Wetter-, Umwelt- und Infrastrukturbedingungen die Leistungsfähigkeit der Sensorik, werden von der technischen Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion Maßnahmen eingeleitet, um die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken auszugleichen. Die Sensorik ist in das Sicherheitskonzept des Kraftfahrzeugs mit autonomer Fahrfunktion nach Nummer 7.2 und in die permanente Systemüberwachung nach Nummer 5 einzubinden.

- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.
- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).
- AFGBV Anlage 2 Datenspeicherung → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).

Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.
- BOStrab §3 Absatz 2
  Einrichtungen in Betriebsanlagen und Fahrzeugen, die für die Benutzung oder Betätigung durch Fahrgäste bestimmt sind, müssen gut erkennbar und leicht erreichbar sein. Ihre Handhabung muß sich sinnfällig erkennen lassen; Fehlbedienungen dürfen zu keiner Betriebsgefährdung führen.
  Hinweis:
  Einrichtungen (welche für die Nutzung durch Fahrgäste vorgesehen sind) müssen gut erkennbar, (d.h. der Verwendungszweck muß eindeutig und leicht verständlich / logisch) und leicht erreichbar (behindertengerecht und für Kinder geeignet) sein.
- BOStrab §4 Absatz 2
  Betriebsanlagen und Fahrzeuge sind instandzuhalten. Treten an ihnen während des Betriebes Mängel auf, die die Betriebssicherheit beeinträchtigen können, sind sie ganz oder teilweise außer Betrieb zu nehmen und erforderlichenfalls abzusichern.
- BOStrab §4 Absatz 4
  Durch betriebliche Vorkehrungen ist dafür zu sorgen, daß Betriebsstörungen zügig beseitigt werden, bei Unfällen und gefährlichen Ereignissen unverzüglich Hilfe geleistet wird und insbesondere bei Brandfällen die Möglichkeit zur Selbst- oder Fremdrettung von Personen oder eine Kombination von beidem in Abhängigkeit von den lokalen Verhältnissen besteht.
- BOStrab §23 Absatz 3
  Bei Fahrbetrieb ohne Fahrzeugführer müssen nachrichtentechnische Anlagen vorhanden sein, die eine vorrangige Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle ermöglichen.
- BOStrab §43 Absatz 5 Punkt 3
  bei Fahrbetrieb ohne Fahrzeugführer sicherstellen, daß Züge nur bei geschlossenen Türen anfahren können
- BOStrab §43 Absatz 6
  Türen müssen in geschlossener Stellung festgehalten sein. Sie müssen jedoch von Fahrgästen im Notfall geöffnet werden können.

- BOStrab §46 Absatz 4
  Fahrzeuge müssen Einrichtungen für eine Sprechverbindung zwischen Fahrzeugführer und einer Betriebsstelle haben. Notfall-Informationen müssen vorrangig durchgegeben werden können.
- BOStrab §46 Absatz 5
  Personenfahrzeuge eines Zuges, die nicht mit Betriebsbediensteten besetzt sind, müssen ständig verfügbare Einrichtungen für eine Notfall-Sprechverbindung zwischen Fahrgästen und dem Fahrzeugführer haben. ➔ Die Technische Aufsicht (TA) der AD-Leitstelle ist der Fahrzeugführer im automatisierten *(Remote-Sicherheitsfahrer bei ≤ SAE 3)* / autonomen *(≥ SAE4)* Betrieb.
  Hinweis: Im konventionellen Betrieb befindet sich der Sicherheitsfahrer im Fahrzeug.
- BOStrab §46 Absatz 6
  Bei Fahrbetrieb ohne Fahrzeugführer müssen Personenfahrzeuge Einrichtungen für eine Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle haben. Absatz 4 Satz 2 gilt entsprechend.
- BOStrab §52 Absatz 3
  Betriebsanlagen oder Fahrzeuge, die ganz oder teilweise selbsttätig arbeiten oder fernbedient werden, müssen im Rahmen der betrieblichen Erfordernisse von Betriebsbediensteten auf einwandfreie Funktion überwacht werden.
- BOStrab §54 Absatz 3
  Personenzüge dürfen nur so beschleunigt und nur so gebremst werden, daß Fahrgäste nicht mehr als unvermeidbar gefährdet werden.

Gefahren nach HAZOP:

- Die potentiellen Gefahren entsprechen den typischen Gefahren der Teilnahme am Straßenverkehr.
  - ► Gefahr eines Unfalles, das autonom fahrende Fahrzeug erkennt z.B. einen (oder mehrere) Fußgänger nicht, weshalb es zu einem Unfall kommt ➔ Die Schwere der Verletzung (bis hin zum Tod) der betroffenen Person(en) hängt von den Geschwindigkeiten der Objekte (Fahrzeug und betroffene Verkehrsteilnehmer) bzw. physikalisch, der resultierenden kinetischen einwirkenden Energie ab.
    Hinweis:
    Diese Gefährdung wird vom Fahrzeughersteller (OEM) verantwortet, gemäß
    AFGBV §12 Anforderungen an den Hersteller Absatz 1 Punkt 2
    Der Hersteller eines Kraftfahrzeugs mit autonomer Fahrfunktion hat
    ein Sicherheitskonzept zur funktionalen Sicherheit nach Anlage I Nummer 7.2 zu erstellen, und dabei
    a) auf Basis dieses Sicherheitskonzeptes eine Gefährdungsanalyse nach Anlage I Ziffer 7.2.1 durchzuführen,
    b) das Sicherheitskonzept nach Anlage III Ziffer 3 zu dokumentieren,
    c) die Sicherheit der autonomen Fahrfunktion entsprechend dieses Sicherheitskonzepts zu überprüfen und die Sicherheit gegenüber dem Kraftfahrt-Bundesamt nach den Anforderungen nach Anlage I Ziffer 10 nachzuweisen.
    Hinweis:
    Die Sicherheit wird durch Maßnahmen erzielt, welche in den diversen, bekannten Fahrerassistenzsystem im Fahrzeug implementiert sind, dazu zählen z.B.
    - *Adaptive Cruise Control (ACC) = Abstandsregeltempomat,*
    - *Advanced Emergency Braking System (AEBS) = Notbremsassistenzsystems,*
    - *Elektronische Stabilitäts-Programm (ESP),*
    - *… .*
  - ► Gefahr eines Unfalles, welcher auf das autonom fahrende Fahrzeug durch andere Verkehrsteilnehmer (Fahrzeuge, Personen) außerhalb des Fahrzeuges ausgeübt wird.
    Hinweis:
    Dieses ist ebenfalls Bestandteil der Gefährdungsanalyse des Fahrzeugherstellers (OEM), weshalb dieses hier nicht noch einmal betrachtet wird.

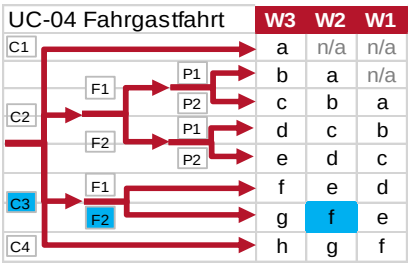
Wichtig:
Das Funktionale Sicherheitskonzept (FSK) des Fahrzeugherstellers (OEM) kann vom Halter Sicherheits-Maßnahmen zum Betrieb einfordern. Dazu zählt insbesondere der (Remote-)Sicherheitsfahrer bei SAE $\leqslant$ 3 bzw. die Überwachung, speziell der Fahrt ($W_{kin} > 0$), durch eine qualifizierte Technische Aufsicht (TA) bei SAE $\geqslant$ 4.

AFGBV §13 Anforderungen an den Halter Absatz 6
Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.

- Tür öffnet während der Fahrt
  Hinweis:
  Die Fahrgäste sind gehalten, sich ausreichenden Halt zu verschaffen und nicht an die Türen anzulehnen.
  Die Fahrgäste können die geöffnete Tür bzw. den Türöffnungsvorgang erkennen. Daher wird davon ausgegangen, daß nur wenige Personen gefährdet werden.
  - ► Tür öffnet verfrüht vor Stillstand
  - ► Tür schließt zu spät, nicht rechtzeitig vor Abfahrt

- ► Tür bleibt während der Fahrt geöffnet, schließt nicht.
- ■ Gefahren aus atypischem, unerwartetem Verhalten des Fahrzeuges z.B. durch eine Störung / Fehlfunktion.

Risikograph:



UC-04 Fahrgastfahrt	W3	W2	W1
C1	a	n/a	n/a
C2 F1 P1	b	a	n/a
C2 F1 P2	c	b	a
C2 F2 P1	d	c	b
C2 F2 P2	e	d	c
C3 F1	f	e	d
C3 F2	g	f	e
C4	h	g	f

≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich

Hinweis:
Die Fahrgastfahrt ist auch zuständig für das „Festhalten der Türen in geschlossener Stellung während der Fahrt“ VDV-Schrift-161-2 Kap. 3.4.2 → UC-06 Türkontrolle.

ISO-26262-03:2018 Clause 6.4.3 Classification of hazardous events ≙ Klassifizierung gefährlicher Ereignisse

Tabelle 1 → S3 = Life-threatening injuries (survival uncertain), fatal injuries

Tabelle 2 → E4 = High probability
Tabelle B.2 → Highway / Country Road,
→ Accelerating / Decelerating / Stopping at traffic light (city street) / Lane change (highway).

Tabelle 3 → C2 = Normally controllable

Hinweis:
C3 = Difficult to control or uncontrollable ← Nicht zutreffend, weil auch das autonome Fahrzeug kontrollierbar ist, es mag Übung erfordern, jedoch ist der Mensch fähig das System zu kontrollieren, sonst würde man es nicht ohne entsprechende, risikominimierende Auflagen (Restriktionen) für die Allgemeinheit zugänglich zulassen.

Tabelle 4 → S3 x E4 x C2 = ASIL-C.

Hinweis:
Die Kontrollierbarkeit des Fahrzeuges (ASIL-C) wird durch den Fahrzeughersteller (OEM) sichergestellt, aber die Technische Aufsicht (TA) der AD-Leitstelle muß die Möglichkeit des Eingreifens haben, d.h. ein Eingriff der Technischen Aufsicht (TA) über das AD-Bordsystem muß die Steuerungsprozesse des Fahrzeuges (OEM) übersteuern können. Folglich muß bei einem autonomen Eingriff durch das AD-Bordsystem sichergestellt werden, daß der Übergang von einem sicheren Betriebszustand in den nachfolgen sicheren Betriebszustand gewährleistet ist. Dieses ist insbesondere bei Änderung der Fahrtroute relevant, die Systemgrenzen (Kammscher Kreis, Elchtest) dürfen nicht überschritten werden. Folglich sind Fahrtroutenänderungen so abzusichern, daß nach dem Passieren des Point of Safe Return (PSR), keine abrupte, unbeherrschbare Routenänderung umgesetzt wird !
(Andernfalls wird ein ASIL-D benötigt).

3.2.5 UC-05 Regelhalt

Das Fahrzeug erreicht einen geplanten Haltepunkt (Haltestelle).
Das AD-Bordsystem steuert die Türfreigabe und leitet zusätzlich, nach Verstreichen der für den Fahrgastwechsel vorgesehenen Mindestdauer, die Weiterfahrt ein.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Erfassung von dem Missionsstatus (Ist-Zustand) der Fahrt mit Abgleich gegenüber den Fahrplandaten (Soll-Zustand) plus ggf. Einleitung von Maßnahmen mittels UC-14 Umlaufänderung oder UC-13 Fahrtänderung.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung).
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle plus Überwachung der Türöffnung.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Der Fahrweg ist eine für eine Fahrt genutzte Route. Diese ist definiert durch eine geordnete Folge geplanter Haltepunkte (bei Leerfahrten nur Start- und Zielpunkt) und ggf. Zwischenpunkte, die den Streckenverlauf eindeutig festlegen.

Hinweis:
Die Mission beschreibt einen Teil einer Fahrt zwischen zwei Haltepunkten / Haltestellen und beinhaltet Angaben zu
- dem Fahrgastwechsel (möglich / nicht möglich, d.h. die Türen werden am Ziel geöffnet bzw. nicht geöffnet)
- der Zeitspanne des Haltens (für den potentiellen Fahrgastwechsel / für das Laden des Fahrzeuges / …)
- der Umlaufnummer inklusive Angaben zum vorgegebenen Fahrweg (Wegpunkte, Route) zum Zielpunkt gemäß Fahrwegplanung der ÖV-Leitstelle
plus optional
- den Informationen zur Haltebucht
- der geplanten Fahrzeit zur Umsetzung der Mission gemäß Fahrwegplanung der ÖV-Leitstelle.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Fahrgastwechsel (Regelbetrieb).

Aktionen:

- Das AD-Bordsystem prüft beim Erreichen des Weg- bzw. Zielpunktes (Gitter der Halteposition / Haltestelle) ob ein Fahrgastwechsel gemäß Fahrplan *der ÖV-Leitstelle* vorgesehen ist.
- Sofern ein Fahrgastwechsel gemäß der Mission erlaubt ist, prüft das AD-Bordsystem ob ein Haltwunsch von einem im Fahrzeug sich befindenden Fahrgast über den Halteknopf ausgelöst wurde, andernfalls wird sobald der Wegpunkt sicher detektierbar ist, über die KI gestützte „Erkennung von Fahrgästen an der Haltestelle“ aus den Umgebungsmeßdaten (z.B. Bild oder LiDAR) auf die Anwesenheit von potentiellen Fahrgästen geprüft.
  Hinweis:
  Ziel des Systems ist, die Erkennung von wartenden Fahrgästen an einer Haltestelle, um bestimmen zu können, ob bei (optionalen) Haltestellen (Bedarfshalt), angehalten werden muß oder nicht. Hierbei soll das System möglichst autark, d.h. nicht von potentiell in einer Haltestelle verbauten Sensorik, abhängig sein. Somit muß die Umsetzung mittels im Fahrzeug verbauter Hardware erfolgen. Da es sich jedoch um ein automatisiertes Fahrzeug handelt, besitzt dieses bereits Sensorik zur Umfeldwahrnehmung, auf die zurückgegriffen werden kann. (Menschen werden als Quader erfaßt, welche stehen oder sich bewegen).
  Die Aufgabe des Busfahrers, der potentiellen Fahrgasterkennung, im konventionellen Betrieb, geht im autonomen Betrieb auf die KI über.
- Sofern ein Halt zugelassen und erforderlich (geäußerter Haltewunsch / erkannter Fahrgast) ist, setzt das AD-Bordsystem den Regelhalt des Fahrzeuges um.
  (Andernfalls wird der Regelhalt übersprungen und das Fahrzeug fährt ohne Halt weiter)
- Das AD-Bordsystem fordert (über 14) per Mitteilung vom ÖV-Bordrechner eine Audio-Durchsage an.
- Der ÖV-Bordrechner sendet (über 11) die Audio-Durchsage an das Fahrgast HMI ÖV.
- Sobald durch das AD-Bordsystem sichergestellt ist, daß das Fahrzeug steht (v = 0,0km/h), sendet das AD-Bordsystem die Türfreigabe (über 19) an das Türsteuergerät des Fahrzeugherstellers (OEM), welches die Türen öffnet, wobei ein akustisches und optisches Warnsignal vom Fahrzeughersteller (OEM) in den Fahrgastraum ausgegeben werden kann.

- Das Türsteuergerät des Fahrzeugherstellers (OEM) sendet (über 19) kontinuierlich Statussignale an das AD-Bordsystem.
- Das AD-Bordsystem leitet (über 14) die kontinuierlichen Statussignale vom Türsteuergerät des Fahrzeugherstellers (OEM) an den ÖV-Bordrechner weiter.
- Der ÖV-Bordrechner beobachtet die Türöffnungszeitspanne und meldet (über 7) den Verlauf (Fahrzeug hält, Türen sind offen) an die ÖV-Leitstelle.
- Das AD-Bordsystem überwacht die Mindestdauer des geplanten Fahrgastwechsels gemäß dem Missionsparameter der Fahrplandaten *der ÖV-Leitstelle*.
- Sobald die Mindestdauer des geplanten Fahrgastwechsels abgelaufen ist sendet (über 8) das AD-Bordsystem die Meldung (z.B. Haltezeit abgelaufen, Abfahrt wird eingeleitet) an die Technische Aufsicht.
- Weiter mit nächster Mission → UC-45 MissionCtrl.
  Hinweis:
  Von der nächsten Mission (Fahrgastfahrt / Leerfahrt / Fahrt im Depot) hängt ab, ob die Türen einfach geschlossen werden oder ob geprüft werden muß, daß sich keine Fahrgäste im Fahrgastraum aufhalten.

Juristische Anforderungen:

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA)
  → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.
- AFGBV Anlage 1 Teil 1 Abschnitt 8 Sensorik
  Zur technischen Umsetzung der autonomen Fahrfunktion muß eine Sensorik verwendet werden, die alle für die sichere Erfüllung der Fahraufgabe erforderlichen Gegenstände, Daten oder Personen im Umfeld des Kraftfahrzeugs erfaßt und hinsichtlich der Verarbeitung personenbezogener Daten die Vorgaben der Verordnung (EU) 2016/679, des Bundesdatenschutzgesetzes und spezialgesetzlicher datenschutzrechtlicher Vorschriften beachtet. Zur Erfüllung des in Satz 1 genannten Zwecks und unter Einhaltung der genannten Vorgaben kann die Sensorik durch externe Systeme unterstützt werden. Beeinflussen Wetter-, Umwelt- und Infrastrukturbedingungen die Leistungsfähigkeit der Sensorik, werden von der technischen Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion Maßnahmen eingeleitet, um die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken auszugleichen. Die Sensorik ist in das Sicherheitskonzept des Kraftfahrzeugs mit autonomer Fahrfunktion nach Nummer 7.2 und in die permanente Systemüberwachung nach Nummer 5 einzubinden.
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt. → t_E Zeitpunkt – Ende der Fahrt.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.2 Technische Vorgaben für das Speichern, Auslesen und Übertragen von Daten
  Das System der Datenspeicherung darf nicht flüchtig sein. Die gespeicherten Daten müssen im stromlosen Zustand erhalten bleiben.
  Ergänzende technische Anforderungen für den Datenspeicher.
- AFGBV Anlage 1 Teil 5 Anforderungen an die Sicherheit im Bereich der Informationstechnologie.

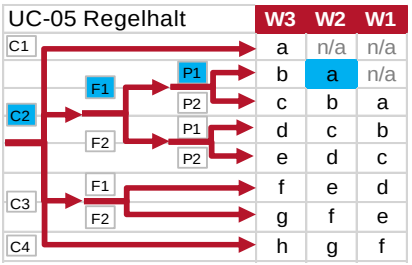
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.
- BOStrab §3 Absatz 2
  Einrichtungen in Betriebsanlagen und Fahrzeugen, die für die Benutzung oder Betätigung durch Fahrgäste bestimmt sind, müssen gut erkennbar und leicht erreichbar sein. Ihre Handhabung muß sich sinnfällig erkennen lassen; Fehlbedienungen dürfen zu keiner Betriebsgefährdung führen.
- BOStrab §4 Absatz 2
  Betriebsanlagen und Fahrzeuge sind instandzuhalten. Treten an ihnen während des Betriebes Mängel auf, die die Betriebssicherheit beeinträchtigen können, sind sie ganz oder teilweise außer Betrieb zu nehmen und erforderlichenfalls abzusichern.
- BOStrab §4 Absatz 4
  Durch betriebliche Vorkehrungen ist dafür zu sorgen, daß Betriebsstörungen zügig beseitigt werden, bei Unfällen und gefährlichen Ereignissen unverzüglich Hilfe geleistet wird und insbesondere bei Brandfällen die Möglichkeit zur Selbst- oder Fremdrettung von Personen oder eine Kombination von beidem in Abhängigkeit von den lokalen Verhältnissen besteht.
- BOStrab §23 Absatz 3
  Bei Fahrbetrieb ohne Fahrzeugführer müssen nachrichtentechnische Anlagen vorhanden sein, die eine vorrangige Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle ermöglichen.
- BOStrab §43 Absatz 3
  Türen müssen Schutzeinrichtungen haben, die verhindern, daß Fahrgäste durch Einklemmen verletzt werden.
- BOStrab §46 Absatz 4
  Fahrzeuge müssen Einrichtungen für eine Sprechverbindung zwischen Fahrzeugführer und einer Betriebsstelle haben. Notfall-Informationen müssen vorrangig durchgegeben werden können.
- BOStrab §46 Absatz 5
  Personenfahrzeuge eines Zuges, die nicht mit Betriebsbediensteten besetzt sind, müssen ständig verfügbare Einrichtungen für eine Notfall-Sprechverbindung zwischen Fahrgästen und dem Fahrzeugführer haben. ➔ Die AD-Leitstelle ist der Fahrzeugführer im automatisierten *(Remote-Sicherheitsfahrer bei ≤ SAE 3)* / autonomen *(≥ SAE4)* Betrieb.
  Hinweis: Im konventionellen Betrieb befindet sich der Sicherheitsfahrer im Fahrzeug.
- BOStrab §46 Absatz 6
  Bei Fahrbetrieb ohne Fahrzeugführer müssen Personenfahrzeuge Einrichtungen für eine Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle haben. Absatz 4 Satz 2 gilt entsprechend.
- BOStrab §52 Absatz 3
  Betriebsanlagen oder Fahrzeuge, die ganz oder teilweise selbsttätig arbeiten oder fernbedient werden, müssen im Rahmen der betrieblichen Erfordernisse von Betriebsbediensteten auf einwandfreie Funktion überwacht werden.
- BOStrab §54 Absatz 3
  Personenzüge dürfen nur so beschleunigt und nur so gebremst werden, daß Fahrgäste nicht mehr als unvermeidbar gefährdet werden.

Gefahren nach HAZOP:

- Die potentiellen Gefahren entsprechen den typischen Gefahren der Teilnahme am Straßenverkehr
  - ► Unaufmerksames (nicht angemessenes Verhalten beim) Aussteigen zum Fahrbahnrand ohne sich z.B. zu vergewissern, ob hier ein Radweg verläuft, wo sich ein Radfahrer nähert.
  - ► Nicht rechtzeitiges, verspätetes Eintreffen von einem Fahrgast / mehrerer Fahrgäste an der Haltestelle, welches zu unaufmerksamem Überqueren der Fahrbahn führen kann, obwohl sich dort Fahrzeuge nähern.
- Tür öffnet und anders als erwartet quetscht das Scharnier eine Person (z.B. Gliedmaße)
  ➔ Vermeidung durch Gegenmaßnahme „Einklemmschutz“
- Tür öffnet auf der falschen Seite, anders als notwendig
  ➔ ist im EVA-Shuttle vom für AP5 verantwortlichen Projektpartner bauseitig ausgeschlossen.

Risikograph:



≙ QM

Begründung zur Wahl der Risikoparameter:

C2	schwere irreversible Verletzung einer oder mehrerer Personen inkl. Tod einer einzigen Person
F1	seltener bis öfterer Aufenthalt im gefährlichen Bereich (Haltezeit << Fahrzeit)
P1	möglich unter bestimmten Bedingungen, *z.B. nicht angemessenes Verhalten / Unaufmerksamkeit.*
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich

Hinweis:
UC-05 → UC-45 MissionCtrl.

3.2.6 UC-06 Türkontrolle

Vor dem Schließen der Tür muß der Türbereich kontrolliert werden. Im automatisierten Fahrzeug erfolgt die Türsteuerung durch das AD-Bordsystem anstatt durch den Fahrer. Sofern es sich um eine Fahrgastfahrt handelt, darf die prinzipielle Sichtprüfung entfallen *(wegen des implementierten Einklemmschutzes)*, bei Leerfahrten oder bei Problemen mit der Türschließung ist die kamerabasierte Erkennung und deren Aufzeichnung zum Nachweis essentiell.

Hinweis:
Die Mission gibt vor ob die Türen am Ziel geöffnet werden oder nicht
plus wieviel Zeit für den Fahrgastwechsel von der ÖV-Leitstelle den Fahrgästen zugestanden (geplant) wurde.

Hinweis:
Am Anfang (vor der Abfahrt) einer Leerfahrt prüft die Technische Aufsicht mittels Kameraüberwachung, daß sich keine Fahrgäste im Fahrzeug befinden, s. ggf. UC-03 Leerfahrt.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Überwachung des Fahrweges gemäß den Fahrplandaten und ggf. Maßnahmen ergreifen um die Pünktlichkeit wiederherzustellen bzw. die Fahrgäste über Verspätungen zu informieren plus diese bei Anschlüssen ihrer Fahrt zu unterstützen.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten, insbesondere daß eine angemessene Zeit für den Fahrgastwechsel für die jeweilige Mission (Datenlieferung) gegeben ist. Aussagekräftige Durchsagen zur Fahrgastinformation (FGI) abrufbar bereitstellen.
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung insbesondere die korrekte Funktionsweise des Türsteuergerätes des Fahrzeuges (OEM). Sicherstellung, daß die Türen vor Abfahrt geschlossen sind.	Überwachung der autonomen Türöffnung und Türschließung. Kommunikation mit Fahrgästen im Problemfall. Einleitung von geeigneten Maßnahmen der Problemlösung.

Hinweis:
Zuständigkeit = Türsteuergerät (OEM) mit Ansteuerung über AD-Bordsystem.

Hinweis:
Die Mission beschreibt einen Teil einer Fahrt zwischen zwei Haltepunkten / Haltestellen und beinhaltet Angaben zu
- dem Fahrgastwechsel (möglich / nicht möglich, d.h. die Türen werden am Ziel geöffnet bzw. nicht geöffnet)
- der Zeitspanne des Haltens (für den potentiellen Fahrgastwechsel / für das Laden des Fahrzeuges / …)
- der Umlaufnummer inklusive Angaben zum vorgegebenen Fahrweg (Wegpunkte, Route) zum Zielpunkt gemäß Fahrwegplanung der ÖV-Leitstelle
plus optional
- den Informationen zur Haltebucht
- der geplanten Fahrzeit zur Umsetzung der Mission gemäß Fahrwegplanung der ÖV-Leitstelle.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Fahrzeug ist im Betrieb (Regelbetrieb) und setzt die Missionen der ÖV-Leitstelle *(außerhalb des BHMS)* um.
Sonderfall: Missionen innerhalb des BHMS.

Aktionen:

- Das AD-Bordsystem setzt den Missionswechsel (über UC-45 MissionCtrl) um, welche in Abhängigkeit der Missionsparameter eine UC-04 Fahrgastfahrt oder UC-03 Leerfahrt oder UC-44 Fahrt im Depot startet, alle leiten sofern notwendig vor Abfahrt die UC-06 Türkontrolle ein.
- Sofern notwendig leitet das AD-Bordsystem das Kommando Tür(zwangs)schließung (über 19) an das Umwelt-IF-AD (Systemgrenze zum Fahrzeug des OEM).
- Das Türsteuergerät (OEM) des Fahrzeuges prüft über die Lichtschranke, ob der Türbereich frei ist.

- Sofern dieses nicht gegeben ist, erfolgt vom Türsteuergerät (OEM) eine Rückmeldung (über 19) an das AD-Bordsystem, welches (über 14) eine Audio-Durchsage vom ÖV-Bordrechner anfordert, welcher (über 11) das Fahrgast HMI ÖV, die optische Warnung und die Durchsage über die Lautsprecher aktiviert.
- Danach sendet das AD-Bordsystem (über 19) erneut das Kommando zur Türschließung an das Umwelt IF AD.
  Hinweis:
  Diese Schleife wiederholt sich (theoretisch) parametrierbar durch den ÖPNV bis die Anzahl der gewünschten Wiederholungen umgesetzt wurde. Danach erfolgt eine Meldung (mit höherer Priorität) an die Technische Aufsicht (TA) zur Dokumentation der aufgetretenen Problematik, welche im Fall von UC-03 Leerfahrt die Situation bereits beobachtet (im Rahmen der Sicherstellung, daß sich kein Fahrgast im Fahrgastraum aufhält).
  → Die Technische Aufsicht (TA) leitet geeignete Maßnahmen zur Lösung ein.
  Hinweis:
  Neben der klassischen Türschließung kann / könnte auch eine Türzwangsschließung mit höherer Kraft umgesetzt werden. Diese ist ein historisch etabliertes, jedoch veraltetes Verfahren um eine Tür sicher zu schließen, welches den Zugführer unterstützen sollte die Tür zu schließen, ohne daß sich eine Person zur Situation begeben mußte. Durch die technische Überwachung der AD-Leitstelle kann dieses heutzutage remote ohne Zeitverlust erfolgen, weshalb die Zwangstürschließung kein unterstützender, sinnvoller Prozeßschritt mehr ist.

- Das Türsteuergerät (OEM) des Fahrzeugs setzt die Türschließung mit der systemeigenen optischen und akustischen Warnung um, wobei der Prozeß vom Einklemmschutz überwacht wird.
  - Sofern der Einklemmschutz ausgelöst wurde, wird die Tür wieder leicht geöffnet, so daß eine eingeklemmte Person sich befreien kann.
  - Danach wiederholt sich der Vorgang der Türschließung.
  - Sofern der Einklemmschutz wiederholt ausgelöst werden sollte, erfolgt eine Meldung (mit Priorität und Kategorie) an die Technische Aufsicht (TA), welche geeignete Maßnahmen zur Lösung der Problematik einleitet.
- Das Türsteuergerät (OEM) des Fahrzeugs bestätigt per Meldung (über 19) die erfolgreiche Türschließung an das AD-Bordsystem.
- Das AD-Bordsystem meldet die Türschließung (über 8) an die AD-Leitstelle sowie (über 14) an den ÖV-Bordrechner.
- Der ÖV-Bordrechner informiert (über 7) die ÖV-Leitstelle über die (mit der erfolgten Türschließung) abgeschlossene Mission.

Juristische Anforderungen:

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA)
  → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.
- AFGBV Anlage 1 Teil 1 Abschnitt 8 Sensorik
  Zur technischen Umsetzung der autonomen Fahrfunktion muß eine Sensorik verwendet werden, die alle für die sichere Erfüllung der Fahraufgabe erforderlichen Gegenstände, Daten oder Personen im Umfeld des Kraftfahrzeugs erfaßt und hinsichtlich der Verarbeitung personenbezogener Daten die Vorgaben der Verordnung (EU) 2016/679, des Bundesdatenschutzgesetzes und spezialgesetzlicher datenschutzrechtlicher Vorschriften beachtet. Zur Erfüllung des in Satz 1 genannten Zwecks und unter Einhaltung der genannten Vorgaben kann die Sensorik durch externe Systeme unterstützt werden. Beeinflussen Wetter-, Umwelt- und Infrastrukturbedingungen die Leistungsfähigkeit der Sensorik, werden von der technischen Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion Maßnahmen eingeleitet, um die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken auszugleichen. Die Sensorik ist in das Sicherheitskonzept des Kraftfahrzeugs mit autonomer Fahrfunktion nach Nummer 7.2 und in die permanente Systemüberwachung nach Nummer 5 einzubinden.
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der

Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt. → t_S Zeitpunkt – Beginn der Fahrt.

- AFGBV Anlage 1 Teil 3 Abschnitt 13.2 Technische Vorgaben für das Speichern, Auslesen und Übertragen von Daten
  Das System der Datenspeicherung darf nicht flüchtig sein. Die gespeicherten Daten müssen im stromlosen Zustand erhalten bleiben.
  Ergänzende technische Anforderungen für den Datenspeicher.
- AFGBV Anlage 1 Teil 5 Anforderungen an die Sicherheit im Bereich der Informationstechnologie.

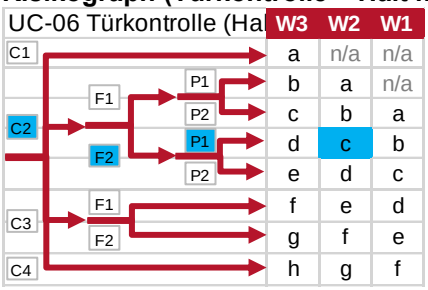
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.
- BOStrab §3 Absatz 2
  Einrichtungen in Betriebsanlagen und Fahrzeugen, die für die Benutzung oder Betätigung durch Fahrgäste bestimmt sind, müssen gut erkennbar und leicht erreichbar sein. Ihre Handhabung muß sich sinnfällig erkennen lassen; Fehlbedienungen dürfen zu keiner Betriebsgefährdung führen.
- BOStrab §4 Absatz 2
  Betriebsanlagen und Fahrzeuge sind instandzuhalten. Treten an ihnen während des Betriebes Mängel auf, die die Betriebssicherheit beeinträchtigen können, sind sie ganz oder teilweise außer Betrieb zu nehmen und erforderlichenfalls abzusichern.
- BOStrab §4 Absatz 4
  Durch betriebliche Vorkehrungen ist dafür zu sorgen, daß Betriebsstörungen zügig beseitigt werden, bei Unfällen und gefährlichen Ereignissen unverzüglich Hilfe geleistet wird und insbesondere bei Brandfällen die Möglichkeit zur Selbst- oder Fremdrettung von Personen oder eine Kombination von beidem in Abhängigkeit von den lokalen Verhältnissen besteht
- BOStrab §23 Absatz 3
  Bei Fahrbetrieb ohne Fahrzeugführer müssen nachrichtentechnische Anlagen vorhanden sein, die eine vorrangige Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle ermöglichen.
- BOStrab §43 Absatz 3
  Türen müssen Schutzeinrichtungen haben, die verhindern, daß Fahrgäste durch Einklemmen verletzt werden.
- BOStrab §43 Absatz 5 Punkt 3
  bei Fahrbetrieb ohne Fahrzeugführer sicherstellen, daß Züge nur bei geschlossenen Türen anfahren können
- BOStrab §43 Absatz 6
  Türen müssen in geschlossener Stellung festgehalten sein. Sie müssen jedoch von Fahrgästen im Notfall geöffnet werden können.
- BOStrab §46 Absatz 4
  Fahrzeuge müssen Einrichtungen für eine Sprechverbindung zwischen Fahrzeugführer und einer Betriebsstelle haben. Notfall-Informationen müssen vorrangig durchgegeben werden können.
- BOStrab §46 Absatz 5
  Personenfahrzeuge eines Zuges, die nicht mit Betriebsbediensteten besetzt sind, müssen ständig verfügbare Einrichtungen für eine Notfall-Sprechverbindung zwischen Fahrgästen und dem Fahrzeugführer haben.
- BOStrab §46 Absatz 6
  Bei Fahrbetrieb ohne Fahrzeugführer müssen Personenfahrzeuge Einrichtungen für eine Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle haben. Absatz 4 Satz 2 gilt entsprechend.
- BOStrab §52 Absatz 3
  Betriebsanlagen oder Fahrzeuge, die ganz oder teilweise selbsttätig arbeiten oder fernbedient werden, müssen im Rahmen der betrieblichen Erfordernisse von Betriebsbediensteten auf einwandfreie Funktion überwacht werden.
- EBO §28 Absatz 4
  Fernbetätigte oder automatisch schließende Türen müssen so beschaffen sein, daß bei ihrer Betätigung Personen nicht gefährdet werden.
- EBO §45 Absatz 7
  Reisezüge sind mit mindestens einem Zugbegleiter zu besetzen, sofern dessen betriebliche Aufgaben nicht von einem anderen Betriebsbeamten oder von technischen Einrichtungen übernommen werden. Sie dürfen ohne Zugbegleiter verkehren, wenn das Schließen der Wagentüren auf den Fahrgastwechsel abgestimmt und das Geschlossensein der Wagentüren vor Abfahrt dem Triebfahrzeugführer angezeigt oder bei einfachen Verhältnissen von ihm festgestellt wird.

Gefahren nach HAZOP:

- Tür öffnet und anders als erwartet quetscht das Scharnier eine Person (z.B. Gliedmaß)
  ➔ Vermeidung durch Gegenmaßnahme „Einklemmschutz“
- Tür öffnet während der Fahrt
  - Tür öffnet verfrüht vor Stillstand
  - Tür schließt zu spät, nicht rechtzeitig vor Abfahrt
  - Tür bleibt während der Fahrt geöffnet, schließt nicht.
- Tür öffnet auf der falschen Seite, anders als notwendig
  ➔ ist im EVA-Shuttle vom für AP5 verantwortlichen Projektpartner bauseitig ausgeschlossen.
- Tür schließt und anders als erwartet quetscht eine Person
  ➔ Vermeidung durch Gegenmaßnahme „Einklemmschutz“
- Rampe / Tritt fährt verfrüht ein, während eine Person sich darauf befindet
- Rampe / Tritt senkt sich verfrüht ab / fährt aus während der Fahrt

Risikograph (Türkontrolle – Halt mit geöffneten Türen):



	W3	W2	W1
C1	a	n/a	n/a
C2 F1 P1	b	a	n/a
C2 F1 P2	c	b	a
C2 F2 P1	d	c	b
C2 F2 P2	e	d	c
C3 F1	f	e	d
C3 F2	g	f	e
C4	h	g	f

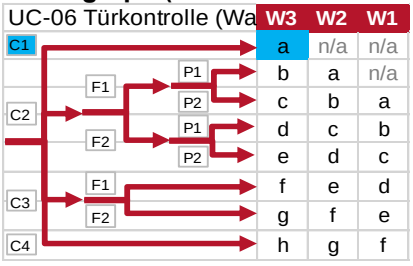
≙ ASIL-A

VDV-Schrift-161-2 Kap. 3.4.1: Verhinderung der Anfahrt mit geöffneten Türen.

Begründung zur Wahl der Risikoparameter:

C2	Die Betriebserfahrungen haben gezeigt, daß im Versagensfalle nur eine Person betroffen ist.
F2	Fahrgäste halten sich im Regelfall häufig in der Nähe der Türen auf.
P1	Gefahrenabwehr ist möglich unter der Bedingung, daß der Fahrgast nicht das Fahrzeug verläßt bzw. ein Sturz vermieden werden kann.
W2	Aufgrund des Einwirkens verschiedenster Bedingungen bis zur unbeabsichtigten Anfahrt wird die Eintrittswahrscheinlichkeit als gering eingestuft.

Risikograph (Türkontrolle – Türschließung):



	W3	W2	W1
C1	a	n/a	n/a
C2 F1 P1	b	a	n/a
C2 F1 P2	c	b	a
C2 F2 P1	d	c	b
C2 F2 P2	e	d	c
C3 F1	f	e	d
C3 F2	g	f	e
C4	h	g	f

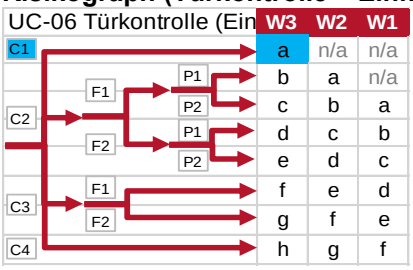
≙ QM

VDV-Schrift-161-2 Kap. 3.4.3: Türschließwarnung (optisch/akustisch)

Begründung zur Wahl der Risikoparameter:

C1	Maximal anzunehmende Auswirkung nach einem Ausfall der Türschließankündigung. Einklemmschutz an der Tür ist aktiv, daher besteht nur eine geringe Verletzungsgefahr (es werden bewährte Bauteile verwendet).
✖	
✖	
W3	Die angenommene Auswirkung kann unmittelbar eintreten, wenn das Fahrzeug bestiegen oder verlassen wird.

Risikograph (Türkontrolle – Einklemmschutz):



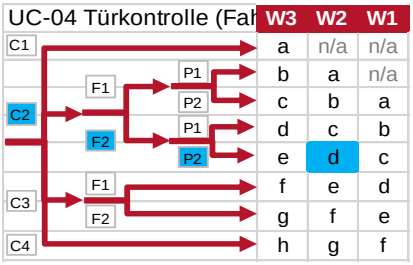
≙ QM

VDV-Schrift-161-2 Kap. 3.4.4: Einklemmschutz während des Schließvorgangs

Begründung zur Wahl der Risikoparameter:

C1	Maximal anzunehmende Auswirkung bei einem Schließen der Tür mit Einklemmen eines Fahrgastes. Durch die weichen gummierten Hauptschließkanten besteht eine geringe Verletzungsgefahr
✖	
✖	
W3	Die angenommene Auswirkung kann unmittelbar eintreten, wenn das Fahrzeug bestiegen oder verlassen wird.

Risikograph (Türkontrolle – Türen in geschlossener Stellung festhalten):



≙ ASIL-B

VDV-Schrift-161-2 Kap. 3.4.2: Festhalten der Türen in geschlossener Stellung während der Fahrt.

Begründung zur Wahl der Risikoparameter:

C2	Die Fahrgäste sind gehalten, sich ausreichenden Halt zu verschaffen und nicht an die Türen anzulehnen. Die Fahrgäste können die geöffnete Tür bzw. den Türöffnungsvorgang erkennen. Daher wird davon ausgegangen, daß nur wenige Personen gefährdet werden.
F2	Fahrgäste halten sich im Regelfall häufig im Türbereich auf.
P2	Gefahrenabwehr ist zwar möglich, die Argumente wurden aber bereits bei der Wahl des Schadensausmaßes berücksichtigt
W2	Der gefährliche Vorfall tritt ein, wenn der Türöffnungswunsch vom Fahrgast betätigt wurde und eine Fehlbedienung des Fahrzeugführers vorliegt.

3.2.7 UC-07 Fahrzeug abrüsten

Am Ende eines Umlaufs wird das Fahrzeug abgerüstet. Weiterhin notwendige manuelle Überprüfungen des Fahrzeugs (z. B. auf Fundsachen) und nicht automatisierbare Tätigkeiten wie das Einstecken des Ladekabels werden durch einen Mitarbeiter des Betriebshofs durchgeführt. Außerdem werden die Bordsysteme (AD-Bordsystem, ÖV-Bordrechner und Peripherie) heruntergefahren.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Auswertung der Statistikdaten	keine
BHMS	Fahrzeugpflege (Service, Reinigung, Fundsachen sichern, erkannte Mängel dokumentieren, Wartung und Instandsetzung)	Betriebsschutz Fahrzeugzustand, Aufrechterhaltung der Einsatzbereitschaft insbesondere Instandhaltung (Pflege und Instandsetzung).
AD-Leitstelle	Bewertung der Ereignisse, sofern die Meldungspriorität dieses erfordert, welches bei Mängeln und Defekten gegeben ist.	Instandsetzungs-anforderungen an das BHMS stellen mit Angabe ob das Fahrzeug ohne eine Instandsetzung bewegt (autonom / ferngesteuert) werden darf.

Hinweis:
Das Betriebshofmanagementsystem (BHMS) umfaßt das Planungs- und Steuerungssystem für alle Vorgänge auf dem Betriebshof, z.B. Abstellen, Rangieren, Kuppeln, Waschen, Tanken, etc. von Bussen.

Betriebsschutz:
Zugang zum Betriebshof (Sicherheitszone) haben nur ausgebildete und (sicherheitstechnisch) geschulte Mitarbeiter, Fahrgäste haben keinen Zugang.

Notfallmaßnahme für eine ggf. eingeschlossene Person sind in der Notfallplanung zu etablieren.

Situation:
Fahrzeug Service (Regelbetrieb).

Aktionen:

- Das Fahrzeug hat mit der letzten Mission seine vorbestimmte Position im BHMS erreicht.
  Das Personal vom BHMS sorgt dafür, daß das Fahrzeug wieder für zukünftige Fahrten einsatzbereit wird, Fundsachen werden gesichert und das Fahrzeug durchläuft die Reinigung. Erkannte Beschädigungen werden aufgenommen und an die Instandhaltung (Pflege und Instandsetzung) gemeldet.
- Die Systeme werden heruntergefahren, wobei ein Nachlaufverhalten möglich ist.
  Sofern erforderlich wird der Pantograph heruntergefahren und das Ladekabel gesteckt, KL15 aus.
  - ▶ Das BHMS veranlaßt (über 6) den ÖV-Bordrechner (UC-07 Fahrzeug abrüsten → UC-09 Datenentsorgung) (über 5) die Datensicherung / Datenentsorgung umzusetzen.
  - ▶ Das BHMS meldet (über 4) das Fahrzeug bei der Technischen Aufsicht (TA) ab.
    Diese veranlaßt automatisiert (über 8) ein Herunterfahren der Systeme, (mit Ausnahme des sich im Fahrzeug befindenden Notrufknopfes und des zugehörigen Notrufsystems).
    Hinweis:
    Der Notrufknopf und das Zweiwege-Kommunikationssystem müssen funktionsfähig bleiben, damit auf Notrufe über den Notdienst unverzüglich angemessen reagiert werden kann, wodurch umgehend sachgerechte Hilfemaßnahmen eingeleitet werden können.

- Das AD-Bordsystem (UC-07 Fahrzeug abrüsten → UC-09 Datenentsorgung) liefert die Ereignismeldungen und ggf. Logfiles (über 8) an die AD-Leitstelle, welche diese bewertet und ggf. Instandsetzungsanforderungen (inklusive Softwareaktualisierungen und Sicherheitspatches → UC-08 Datenaktualisierung) mit Nutzungserlaubnis (erlaubt / erlaubt mit Auflagen / gesperrt) an das BHMS (über 4) stellt.
  Hinweis:
  Sollten keine Mängel vorliegen, gilt das Dokument als Nachweis der technischen Verwendbarkeit.
  - ▶ Sofern ein Instandsetzungsauftrag von der AD-Leitstelle vorliegen sollte, schreibt der Disponent des BHMS die dafür notwendigen Instandsetzungsaufträge und plant deren Umsetzung inklusive der damit ggf. verbundenen nicht Verfügbarkeit des Fahrzeuges.

- Der BH-Disponent informiert (über 5) die ÖV-Leitstelle bzgl. der Verfügbarkeit der einsatzfähigen Fahrzeuge, so daß diese bei der Kapazitätsplanung des ÖPNV angemessen berücksichtigt werden können.

Juristische Anforderungen:

- AFGBV §12 Anforderungen an den Hersteller Absatz 1
  Der Hersteller eines Kraftfahrzeugs mit autonomer Fahrfunktion hat Reparatur- und Wartungsinformationen für das Kraftfahrzeug nach Anlage 3 Nummer 2.3 und 2.6 dieser Verordnung zu erstellen.
  → Welche hier anzuwenden sind.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 1
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen die Fahrzeugsysteme für die aktive und passive Sicherheit des Kraftfahrzeugs mit autonomer Fahrfunktion regelmäßig überprüft werden.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 3
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen ab dem Tag der Zulassung zum Straßenverkehr alle 90 Tage eine Gesamtprüfung nach den Vorgaben des Betriebshandbuchs für das Kraftfahrzeug mit autonomer Fahrfunktion durchgeführt wird.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 4
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß die Ergebnisse der Gesamtprüfungen nach Nummer 3 einschließlich einer Beschreibung aller festgestellten Mängel und durchgeführter Instandsetzungen in einem Bericht dokumentiert und dem Kraftfahrt-Bundesamt sowie der zuständigen Behörde auf Verlangen unverzüglich übermittelt werden, sofern dies erforderlich ist.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 2
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen haben.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 3
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihnen anvertrauten Aufgaben zuverlässig sind; zur Beurteilung ihrer Zuverlässigkeit sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde sowie, bei Einsatz für die Durchführung von Fahrten im manuellen Betrieb, eine Auskunft aus dem Fahrerlaubnisregister vorzulegen; § 8 Absatz 3 gilt entsprechend.
- AFGBV §13 Anforderungen an den Halter Absatz 3
  Der Halter muß sicherstellen, daß Anweisungen zur ordnungsgemäßen Durchführung der Wartungsarbeiten, der Gesamtprüfungen, weiterer Untersuchungen und Fahrten im manuellen Fahrbetrieb vorliegen und daß diese Anweisungen befolgt werden. Die Anweisungen sind zu dokumentieren.
- AFGBV §13 Anforderungen an den Halter Absatz 4
  Berichte über die Durchführung von Wartungsarbeiten, von Gesamtprüfungen und von weiteren Untersuchungen müssen durch den Halter oder die verantwortliche Person unverzüglich schriftlich oder elektronisch erstellt werden. Die Berichte sind zu unterzeichnen. Die Berichte sind zu dokumentieren und vom Halter oder von der für die Technische Aufsicht verantwortlichen Person sechs Monate lang aufzubewahren und nach Ablauf dieser Frist unverzüglich, bei elektronischer Speicherung automatisiert, zu löschen.
- AFGBV §13 Anforderungen an den Halter Absatz 5
  Die Anforderungen zur Dokumentenverwaltung für die Anweisungen nach Absatz 3 und der Berichte nach Absatz 4 müssen dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik wird vermutet, wenn die Vorgaben der ISO 9001:2015 Qualitätsmanagementsysteme – Grundlagen und Begriffe erfüllt

werden. Darüber hinaus muß die Dokumentenverwaltung den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 genügen.

- AFGBV §13 Anforderungen an den Halter Absatz 8
  Der Halter hat für das Kraftfahrzeug mit autonomer Fahrfunktion eine Hauptuntersuchung nach Maßgabe der Anlage VIII in Verbindung mit Anlage VIIIa der Straßenverkehrs-Zulassungs-Ordnung zu veranlassen. Die Frist für die Hauptuntersuchung nach § 29 der Straßenverkehrs-Zulassungs-Ordnung beträgt sechs Monate ab dem Zeitpunkt der Zulassung des Kraftfahrzeugs mit autonomer Fahrfunktion.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA)
  → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV §15 Datenspeicherung Absatz 2
  Die gespeicherten Daten dürfen nur durch das Kraftfahrt-Bundesamt und die zuständige Behörde und nur zum Zweck der Nachprüfung der Erfüllung der Voraussetzungen der Genehmigung und der mit der Genehmigung verbundenen Überwachungspflichten erhoben, gespeichert und verwendet werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 6 Übertragung von Daten an das Kraftfahrzeug
  Die zur selbstständigen Bewältigung der Fahraufgabe im autonomen Betrieb notwendigen Daten und Informationen von externen technischen Einheiten (beispielsweise Backends oder Server eines Anbieters, externe Sensoren, Smartphone) müssen vom Kraftfahrzeug sicher empfangen und verwendet werden können. Daten externer Einheiten können im Kraftfahrzeug zur Ausführung der autonomen Fahrfunktionen verwendet werden. Daten und Informationen können beispielsweise bei bestimmten Anwendungsfällen über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) von einer externen technischen Einheit an das Kraftfahrzeug und vom Kraftfahrzeug an eine technische Einheit übertragen werden. Die Übertragung solcher Daten muß insbesondere den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und nach dem aktuellen Stand der Technik abgesichert sein. Das Absicherungskonzept muß die in einer Bedrohungsanalyse identifizierten Risiken mit wirksamen Maßnahmen adressieren und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten. Zur Datenübertragung sollte eine zentrale sichere elektronische Steuereinheit (SECU) genutzt werden. Die SECU dient als Informationsgateway im Kraftfahrzeug. Die SECU kommuniziert intern an die Kommunikationsbusse des Kraftfahrzeugs und an den physischen On-Board-Diagnose II-Anschluß (OBD II) oder an eine proprietäre Schnittstelle eines Herstellers. Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung sind Teil 5 zu entnehmen. Die Integrität, Authentizität und Verfügbarkeit der Datenübertragung sind sicherzustellen. Die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen oder mit Infrastrukturkomponenten ist zulässig. Sie muß auf der Basis einer Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 insbesondere den Anforderungen an die Informationstechnik nach Teil 5 und damit den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen. Während des Betriebs in einer optionalen Testphase ist die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen und Infrastrukturkomponenten zu testen und gegebenenfalls anzupassen.
- AFGBV Anlage 1 Teil 1 Abschnitt 8 Sensorik
  Zur technischen Umsetzung der autonomen Fahrfunktion muß eine Sensorik verwendet werden, die alle für die sichere Erfüllung der Fahraufgabe erforderlichen Gegenstände, Daten oder Personen im Umfeld des Kraftfahrzeugs erfaßt und hinsichtlich der Verarbeitung personenbezogener Daten die Vorgaben der Verordnung (EU) 2016/679, des Bundesdatenschutzgesetzes und spezialgesetzlicher datenschutzrechtlicher Vorschriften beachtet. Zur Erfüllung des in Satz 1 genannten Zwecks und unter Einhaltung der genannten Vorgaben kann die Sensorik durch externe Systeme unterstützt werden. Beeinflussen Wetter-, Umwelt- und Infrastrukturbedingungen die Leistungsfähigkeit der Sensorik, werden von der technischen Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion Maßnahmen eingeleitet, um die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken auszugleichen. Die Sensorik ist in das Sicherheitskonzept des Kraftfahrzeugs mit autonomer Fahrfunktion nach Nummer 7.2 und in die permanente Systemüberwachung nach Nummer 5 einzubinden.
- AFGBV Anlage 1 Teil 1 Abschnitt 9 Alterung und Abnutzung des Systems
  Das Kraftfahrzeug muß die funktionalen Anforderungen auch bei Alterung und Abnutzung der relevanten Systemkomponenten erfüllen. Beeinflussen Alterungserscheinungen die Leistungsfähigkeit, beispielsweise der Sensorik, gleicht die technische Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken durch geeignete Maßnahmen aus.
- AFGBV Anlage 1 Teil 2 Test- und Validierungsmethoden für Fahrzeuge mit autonomer Fahrfunktion (Abschnitt 10 bis 12) → *Definiert Test- und Validierungsmethoden, welche bei der Implementierung und Validierung anzuwenden sind. Diese juristischen Anforderungen gehören zur rechten Seite des V-Modells und damit nicht zum FSK.*
  Hinweis:
  V-Modell gemäß ISO-26262-02:2018 Kapitel 5.2.2.2d.

- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.2 Technische Vorgaben für das Speichern, Auslesen und Übertragen von Daten
  Das System der Datenspeicherung darf nicht flüchtig sein. Die gespeicherten Daten müssen im stromlosen Zustand erhalten bleiben.
  Ergänzende technische Anforderungen für den Datenspeicher.
  - a) Der Zugang zu den im Kraftfahrzeug mit autonomer Fahrfunktion gespeicherten Daten erfolgt über die normierte 16-polige On-Board-Diagnose-Schnittstelle (16-polige OBD-Schnittstelle) über ein Kommunikationsmodul nach ISO 22900-1:2008-03 Straßenfahrzeuge – Modulare Kommunikationsschnittstelle im Fahrzeug (MVCI) – Teil 1: Hardwaredesign Anforderungen unter Verwendung der proprietären Software des Herstellers oder über die proprietäre Schnittstelle. Ergänzend dazu müssen in bestimmten Situationen oder nach bestimmten Ereignissen die Daten direkt über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) an die zuständige staatliche Stelle gesendet werden.
  - b) Der Zugang und das Herunterladen der gespeicherten Daten über die normierte 16-polige OBD-Schnittstelle oder über die proprietäre Schnittstelle darf nur durch das Kraftfahrt-Bundesamt und die zuständige Behörde erfolgen, sofern dies für deren jeweilige Aufgabenerfüllung nach dieser Verordnung erforderlich ist.
  - c) Im Reparaturfall erfolgt der Zugang zum Datenspeicher im Kraftfahrzeug mit autonomer Fahrfunktion über die normierte 16-polige OBD-Schnittstelle über ein Kommunikationsmodul nach ISO 22900 nur unter Verwendung der proprietären Software des Herstellers oder über die proprietäre Schnittstelle.
  - d) Die Datenspeicherung und die Datenübermittlung an das Kraftfahrt-Bundesamt und die zuständige Behörde haben den Anforderungen an die Sicherheit im Bereich der Informationstechnologie (Teil 5) zu genügen. Insbesondere müssen die Daten dem Stand der Technik gemäß unter Beachtung der Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 vor Manipulation und mißbräuchlicher Verwendung geschützt werden.
- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.
- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).

Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.
- BOStrab §4 Absatz 2
  Betriebsanlagen und Fahrzeuge sind instand zu halten. Treten an ihnen während des Betriebes Mängel auf, die die Betriebssicherheit beeinträchtigen können, sind sie ganz oder teilweise außer Betrieb zu nehmen und erforderlichenfalls abzusichern.

- BOStrab §52 Absatz 3
  Betriebsanlagen oder Fahrzeuge, die ganz oder teilweise selbsttätig arbeiten oder fernbedient werden, müssen im Rahmen der betrieblichen Erfordernisse von Betriebsbediensteten auf einwandfreie Funktion überwacht werden.

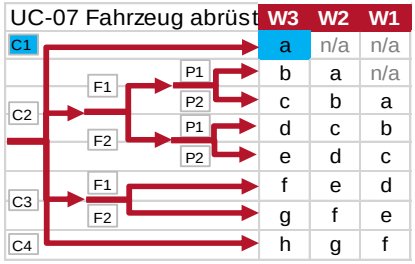
Übertragung etablierter Anforderungen aus der Felderfahrung auf straßengebundenen Verkehrssysteme

- BetrSichV § 4.1 (%)
  Die Notbefreiungsanleitung und die zur Befreiung Eingeschlossener erforderlichen Einrichtungen sind vor der Inbetriebnahme in unmittelbarer Nähe der Anlage bereitzustellen. Wer eine Aufzugsanlage nach Anhang 2 Abschnitt 2 Nummer 2 Buchstabe b betreibt, in der eine Person eingeschlossen werden kann, hat dafür zu sorgen, daß diese Hilfe herbeirufen kann.
  Hinweis:
  Auch wenn ein autonomes Fahrzeug (horizontal arbeitendes Arbeitsmittel) kein Aufzug (vertikal arbeitendes Arbeitsmittel) ist, so muß dennoch eine ggf. eingeschlossene Person die Möglichkeit der Befreiung gegeben werden.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert.
- Gefahr, daß eine Person im Fahrzeug eingeschlossen wird, weil die Türen im abgeschalteten Fahrzeugzustand nicht geöffnet werden können.
  → Maßnahme Notrufsystem bleibt ggf. mittels Wake-Up-Funktionalität aktiv um die AD-Leitstelle im Einschließungsfall als Notdienst im Bedarfsfall zu reaktivieren.
  Hinweis:
  Sollte es eine Notentriegelung geben, kann sich der eingeschlossene Mitarbeiter selbständig befreien, aber das Fahrzeug wäre danach offen, weshalb zur Fahrzeugsicherung ein Verschließen zu veranlassen ist, welches durch den BH-MA oder durch die Technische Aufsicht der AD-Leitstelle umgesetzt werden kann. Sowohl die Notentriegelung, als auch das Wiederverschließen, ist der Technischen Aufsicht der AD-Leitstelle mitzuteilen.

Risikograph (Standardfall):



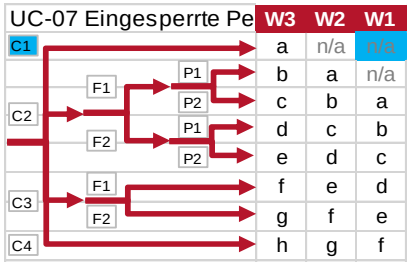
≙ QM

Begründung zur Wahl der Risikoparameter (Standardfall Fahrzeug abrüsten):

C1	Geringe Verletzung (Akzeptiertes Standardrisiko beim Arbeiten)
✖	
✖	
W3	Die angenommene Auswirkung kann unmittelbar eintreten, wenn das Fahrzeug aus dem Betrieb genommen wird. Die Arbeiten finden zum Teil im Hochvoltbereich (Schulung erforderlich) statt. Dadurch, daß der Betriebshofmitarbeiter ein Fahrzeug nach dem anderen außer Betrieb setzt, kann eine Sicherungsmaßnahme vergessen werden (in dem Glauben, daß man diese bereits umgesetzt hat, was jedoch beim vorherigen Fahrzeug realisiert wurde).

Hinweis: Die Einstufung ist mit UC-01 Fahrzeug aufrüsten vergleichbar.

Risikograph (Sonderfall eingesperrte Person):



≙ QM

Begründung zur Wahl der Risikoparameter (Sonderfall Person eingeschlossen):

C1	Geringe Verletzung (Fahrzeug ist für die Nutzung von Personen ausgelegt)
✖	
✖	
W1	Die angenommene Auswirkung (Einschluß einer / mehrerer Personen) kann unmittelbar eintreten, wenn das Fahrzeug aus dem Betrieb genommen wird, z.B. reinigt ein von außen momentan nicht sichtbarer Mitarbeiter im Fahrzeug etwas und ein anderer Mitarbeiter des BHMS sperrt das Fahrzeug (Schlüsselschalter außen) zu, weil er glaubt die Reinigung wäre abgeschlossen, da die Person im Fahrzeug nicht wahrgenommen wurde. Der eingeschlossene Mitarbeiter kann sich bemerkbar machen oder ggf. mit seinem Mobil-Telefon um Hilfe rufen, jedoch ist das keine systembedingte, vorrätige Lösung, weshalb der Notrufknopf im Innenraum des Fahrzeuges auch nach dem Ausschalten des Fahrzeuges in Betrieb sein muß um Sicherzustellen, daß ein Notdienst den Notruf erhält, (sofern es keine mechanische, stets verfügbare Notentriegelung im Fahrzeug gibt). *Hinweis:* *Sollte es eine Notentriegelung geben, kann sich der eingeschlossene Mitarbeiter selbständig befreien, aber das Fahrzeug wäre danach offen, weshalb zur Fahrzeugsicherung ein Verschließen zu veranlassen ist, welches durch den BH-MA oder durch die Technische Aufsicht der AD-Leitstelle umgesetzt werden kann. Sowohl die Notentriegelung, als auch das Wiederverschließen, ist der Technischen Aufsicht der AD-Leitstelle mitzuteilen.*

Hinweis: Die Einstufung ist mit eingesperrten Personen im Aufzug vergleichbar.

3.2.8 UC-08 Datenaktualisierung

Die Datenaktualisierung gehört zur Pflege und Instandsetzung. Diese Tätigkeit wird vom BHMS erledigt, gewöhnlich innerhalb von UC-07 Fahrzeug abrüsten, jedoch können längerfristige Instandhaltungsaufgaben (Pflege, Wartung und Instandsetzung) eine Einplanung vor dem Wiedereinsatz (dem UC-01 Fahrzeug aufrüsten) erfordern.

Die Datenaktualisierung der ÖV-Systeme umfaßt Informationen wie beispielsweise
- Fahrplandaten, Ticketing-Daten,
- Softwareversionen und Konfigurationen.

Die Datensätze werden vom Datenmanagementsystem bereitgestellt und an
- die ÖV-Leitstelle,
- die Fahrzeuge im Fuhrpark und
- die FGI-Kanäle übertragen.

Hierfür werden zunächst die aktuelle Version der Informationen, Software oder Konfigurationen abgerufen und abgeglichen. Im darauffolgenden Schritt werden veraltete Versionen ersetzt und bereits aktuelle Versionen beibehalten.

Die Datenaktualisierung der AD-Systeme beinhaltet die Datenaktualisierung, z.B.
- der hochauflösenden Karte, insbesondere Navigationsdaten
  (Einbahnstraßenführung oder Straßensperrungen durch Bauarbeiten)
- Softwareversionen und Konfigurationen,
- Sicherheitspatches der Cybersecurity (SVM, NVD, NIST ↔ CERT / CSIRT)

Die Datenaktualisierung des Fahrzeugherstellers (OEM) findet im Rahmen der Inspektion / Wartung durch die Fachwerkstatt statt, sofern das BHMS nicht über ausgebildete Fachkräfte (als freie, zugelassene Werkstatt) verfügt.

Hinweis:
Das Datenmanagement beinhaltet die beiden Prozesse zur Datenver- und -entsorgung der Fahrzeuge. Sollfahrplandaten, Tarifdaten, Konfigurationsparameter, neue Firmwareversionen u. Ä. für den ÖV-Bordrechner, das AD-Bordsystem oder die Peripheriegeräte müssen auf die Fahrzeuge übertragen werden; umgekehrt werden Statistikdaten, z. B. vom Fahrgastzählsystem, vom Fahrzeug zurück an die Zentrale geschickt. Diese Prozesse werden üblicherweise während der Abstellung des Fahrzeugs auf dem Betriebshof durchgeführt. Nicht davon umfasst wird der im laufenden Betrieb notwendige Datenaustausch, (beispielsweise Fahrplanänderungen aufgrund dispositiver Maßnahmen, Echtzeitinformationen zum Standort etc.), welcher in den jeweiligen Use Cases beschrieben ist.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Bereitstellen der Daten inklusive ggf. Softwareupdates für Service und Wartung der ÖV-Systeme über den ÖV-Bordrechner.	Wartung und Pflege des ÖV-Bordrechners mit seiner zugehörigen Peripherie.
BHMS	Planung *in Abstimmung mit der ÖV-Leitstelle (Fahrzeugverfügbarkeit)* und Umsetzung der Service und Wartungsvorgaben der Fahrzeuge gemäß Vorgabe der Fahrzeughersteller (OEM).	Wartung und Pflege der Softwarestände auf dem Fahrzeug.
AD-Leitstelle	Bereitstellen der Daten inklusive ggf. Softwareupdates plus Sicherheitspatches innerhalb einer definierten, naheliegenden Zeitspanne für Service und Wartung der AD-Systeme über das AD-Bordsystem.	Wartung und Pflege des AD-Bordsystems mit seiner zugehörigen Peripherie mit Sicherstellung der Aktualität der Systeme.

Hinweis:
Das Betriebshofmanagementsystem (BHMS) umfaßt das Planungs- und Steuerungssystem für alle Vorgänge auf dem Betriebshof, z.B. Abstellen, Rangieren, Kuppeln, Waschen, Tanken, etc. von Bussen.

Betriebsschutz:
Zugang zum Betriebshof (Sicherheitszone) haben nur ausgebildete und (sicherheitstechnisch) geschulte Mitarbeiter, Fahrgäste haben keinen Zugang.

Situation:
Service, Wartung & Pflege – Datenaktualisierung (Regelbetrieb).

Aktionen:

- Das BHMS verantwortet die Pflege und Wartung insbesondere die Einsatzbereitschaft der Fahrzeuge.
  Hinweis:
  Eingesetzte Software ist gemäß der klassischen Unternehmensrichtlinie „Lenkung von Dokumenten“ zu archivieren und gegen Verfälschung zu sichern, d.h. die Datenintegrität ist zu gewährleisten. Dazu zählt auch die Dokumentation mit Angaben einer MD5 / SHA1 Checksumme.
  - ► Das BHMS aktualisiert die Softwareversionen und deren Konfigurationen auf den Fahrzeugen gemäß den Vorgaben der ÖV-Leitstelle.

- Das BHMS aktualisiert die Softwareversionen und deren Konfigurationen auf den Fahrzeugen gemäß den Vorgaben der AD-Leitstelle.
- Das BHMS führt Reparaturen und Wartungsarbeiten an den Fahrzeugen durch, sofern Aktualisierungen (Updates) oder Ersatzteile Softwarestände und Konfigurationen mitbringen, welche von den bisherigen abweichen, stellt das BHMS sicher, daß diese vor der Inbetriebnahme mit Fahrgästen auf Kompatibilität, Funktionalität und Sicherheit geprüft werden.
  Hinweis:
  Der Test, daß die Softwarestände und Konfigurationen zusammen funktionieren, muß einmalig belastbar sichergestellt werden. Jedoch ist nach jeder Instandsetzung eine Probefahrt durchzuführen.
  Hinweis:
  Die Tätigkeit Instandhaltung (Pflege und Instandsetzung) gehört zu UC-07 Fahrzeug abrüsten, aber die dafür notwendigen Ereignisprotokolle (Logfiles) werden der AD-Leitstelle zeitlich erst mit UC-09 Datenentsorgung zur Verfügung gestellt, woraus die Aufträge für Service und Wartung erstellt werden, wobei die Notwendigkeit von UC-08 Datenaktualisierung (Updates und Sicherheitspatches) Berücksichtigung findet, weshalb diese Tätigkeit gewöhnlich innerhalb von UC-07 Fahrzeug abrüsten umgesetzt wird.
- Das BHMS trägt Sorge dafür, daß die Fahrzeuge gemäß den Vorgaben des Fahrzeugherstellers ordnungsgemäß gewartet werden.

Juristische Anforderungen:

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA)
  → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 1
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen die Fahrzeugsysteme für die aktive und passive Sicherheit des Kraftfahrzeugs mit autonomer Fahrfunktion regelmäßig überprüft werden.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 3
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen ab dem Tag der Zulassung zum Straßenverkehr alle 90 Tage eine Gesamtprüfung nach den Vorgaben des Betriebshandbuchs für das Kraftfahrzeug mit autonomer Fahrfunktion durchgeführt wird.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 4
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß die Ergebnisse der Gesamtprüfungen nach Nummer 3 einschließlich einer Beschreibung aller festgestellten Mängel und durchgeführter Instandsetzungen in einem Bericht dokumentiert und dem Kraftfahrt-Bundesamt sowie der zuständigen Behörde auf Verlangen unverzüglich übermittelt werden, sofern dies erforderlich ist.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 3
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihnen anvertrauten Aufgaben zuverlässig sind; zur Beurteilung ihrer Zuverlässigkeit sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde sowie, bei Einsatz für die Durchführung von Fahrten im manuellen Betrieb, eine Auskunft aus dem Fahrerlaubnisregister vorzulegen; § 8 Absatz 3 gilt entsprechend.
- AFGBV §13 Anforderungen an den Halter Absatz 3
  Der Halter muß sicherstellen, daß Anweisungen zur ordnungsgemäßen Durchführung der Wartungsarbeiten, der Gesamtprüfungen, weiterer Untersuchungen und Fahrten im manuellen Fahrbetrieb vorliegen und daß diese Anweisungen befolgt werden. Die Anweisungen sind zu dokumentieren.
- AFGBV §13 Anforderungen an den Halter Absatz 4
  Berichte über die Durchführung von Wartungsarbeiten, von Gesamtprüfungen und von weiteren Untersuchungen müssen durch den Halter oder die verantwortliche Person unverzüglich schriftlich oder

elektronisch erstellt werden. Die Berichte sind zu unterzeichnen. Die Berichte sind zu dokumentieren und vom Halter oder von der für die Technische Aufsicht verantwortlichen Person sechs Monate lang aufzubewahren und nach Ablauf dieser Frist unverzüglich, bei elektronischer Speicherung automatisiert, zu löschen.

- AFGBV §13 Anforderungen an den Halter Absatz 5
  Die Anforderungen zur Dokumentenverwaltung für die Anweisungen nach Absatz 3 und der Berichte nach Absatz 4 müssen dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik wird vermutet, wenn die Vorgaben der ISO 9001:2015 Qualitätsmanagementsysteme – Grundlagen und Begriffe erfüllt werden. Darüber hinaus muß die Dokumentenverwaltung den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 genügen.
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.2 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und mit konventionellen Vorrichtungen zur Ausübung der Fahraufgabe gilt:
  Die autonome Fahrfunktion darf nicht erneut aktivierbar sein, solange eine Beeinträchtigung der technischen Ausrüstung besteht.
- AFGBV Anlage 1 Teil 1 Abschnitt 8
  Zur technischen Umsetzung der autonomen Fahrfunktion muß eine Sensorik verwendet werden, die alle für die sichere Erfüllung der Fahraufgabe erforderlichen Gegenstände, Daten oder Personen im Umfeld des Kraftfahrzeugs erfaßt und hinsichtlich der Verarbeitung personenbezogener Daten die Vorgaben der Verordnung (EU) 2016/679, des Bundesdatenschutzgesetzes und spezialgesetzlicher datenschutzrechtlicher Vorschriften beachtet. Zur Erfüllung des in Satz 1 genannten Zwecks und unter Einhaltung der genannten Vorgaben kann die Sensorik durch externe Systeme unterstützt werden. Beeinflussen Wetter-, Umwelt- und Infrastrukturbedingungen die Leistungsfähigkeit der Sensorik, werden von der technischen Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion Maßnahmen eingeleitet, um die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken auszugleichen. Die Sensorik ist in das Sicherheitskonzept des Kraftfahrzeugs mit autonomer Fahrfunktion nach Nummer 7.2 und in die permanente Systemüberwachung nach Nummer 5 einzubinden.
- AFGBV Anlage 1 Teil 1 Abschnitt 9 Alterung und Abnutzung des Systems
  Das Kraftfahrzeug muß die funktionalen Anforderungen auch bei Alterung und Abnutzung der relevanten Systemkomponenten erfüllen. Beeinflussen Alterungserscheinungen die Leistungsfähigkeit, beispielsweise der Sensorik, gleicht die technische Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken durch geeignete Maßnahmen aus.
- AFGBV Anlage 1 Teil 2 Test- und Validierungsmethoden für Fahrzeuge mit autonomer Fahrfunktion (Abschnitt 10 bis 12) → *Definiert Test- und Validierungsmethoden, welche bei der Implementierung und Validierung anzuwenden sind. Diese juristischen Anforderungen gehören zur rechten Seite des V-Modells und damit nicht zum FSK*.
  Hinweis:
  V-Modell gemäß ISO-26262-02:2018 Kapitel 5.2.2.2d.
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt. → *siehe AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse*.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.2
  a) Der Zugang zu den im Kraftfahrzeug mit autonomer Fahrfunktion gespeicherten Daten erfolgt über die normierte 16-polige On-Board-Diagnose-Schnittstelle (16-polige OBD-Schnittstelle) über ein Kommunikationsmodul nach ISO 22900-1:2008-03 Straßenfahrzeuge – Modulare Kommunikationsschnittstelle im Fahrzeug (MVCI) – Teil 1: Hardwaredesign Anforderungen unter Verwendung der proprietären Software des Herstellers oder über die proprietäre Schnittstelle. Ergänzend dazu müssen in bestimmten Situationen oder nach bestimmten Ereignissen die Daten direkt über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) an die zuständige staatliche Stelle gesendet werden.
  d) Die Datenspeicherung und die Datenübermittlung an das Kraftfahrt-Bundesamt und die zuständige Behörde haben den Anforderungen an die Sicherheit im Bereich der Informationstechnologie (Teil 5) zu

genügen. Insbesondere müssen die Daten dem Stand der Technik gemäß unter Beachtung der Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 vor Manipulation und mißbräuchlicher Verwendung geschützt werden.

- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.

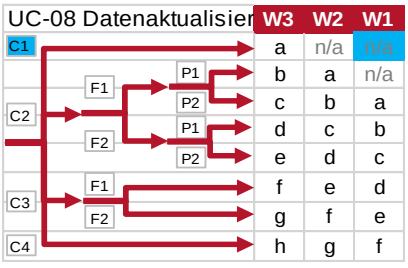
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.
- BOStrab §4 Absatz 2
  Betriebsanlagen und Fahrzeuge sind instandzuhalten. Treten an ihnen während des Betriebes Mängel auf, die die Betriebssicherheit beeinträchtigen können, sind sie ganz oder teilweise außer Betrieb zu nehmen und erforderlichenfalls abzusichern.
- BOStrab §4 Absatz 4
  Durch betriebliche Vorkehrungen ist dafür zu sorgen, daß Betriebsstörungen zügig beseitigt werden, bei Unfällen und gefährlichen Ereignissen unverzüglich Hilfe geleistet wird und insbesondere bei Brandfällen die Möglichkeit zur Selbst- oder Fremdrettung von Personen oder eine Kombination von beidem in Abhängigkeit von den lokalen Verhältnissen besteht.
- BOStrab §7 Absatz 2
  Der Unternehmer ist verpflichtet, bei der Auswahl, Aus- und Fortbildung, Verwendung und Beaufsichtigung der Betriebsbediensteten die Sorgfalt anzuwenden, die eine sichere und ordnungsgemäße Beförderung von Personen erfordert.
- BOStrab §52 Absatz 3
  Betriebsanlagen oder Fahrzeuge, die ganz oder teilweise selbsttätig arbeiten oder fernbedient werden, müssen im Rahmen der betrieblichen Erfordernisse von Betriebsbediensteten auf einwandfreie Funktion überwacht werden.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert.
- Die Systeme sind hinsichtlich der Verwundbarkeit zu überwachen und zeitnah zu sichern, sobald ein Sicherheitspatch verfügbar ist.
  ➔ Maßnahme: Ein Software Vulnerability Management (SVM) ist zu etablieren, welches das Infektionspotential überwacht und (sofern möglich) geeignete Maßnahmen der Risikominderung etabliert.
- Für neue Software ist der Nachweis der einwandfreien Funktionalität und Kompatibilität zu erbringen.
  → Toolqualifizierung.

Risikograph (Regelbetrieb Softwareupdate gemäß Linux Prozeß ≙ getestet und validiert):

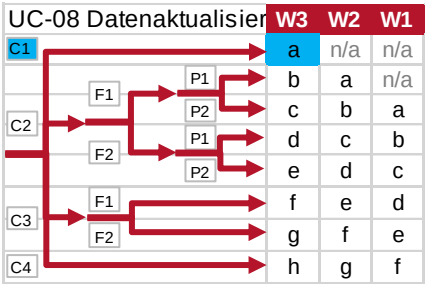


≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzung (Akzeptiertes Standardrisiko). Die Aufgabe der Datenaktualisierung entspricht dem Installieren von Software.
✖	
✖	
W1	Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich. *Hinweis:* *Updates selbst haben eine relativ hohe Auftretenswahrscheinlichkeit, jedoch ist die Gebrauchsfähigkeit der Aktualisierungen (Updates) abhängig von den Absicherungen (Tests), welche vor dem Verteilen an die breite Masse, vom Hersteller umgesetzt werden. Die Tests wiederum sind von einer breiten Vielfallt von unterschiedlichen Systemen abhängig, weshalb ein vernünftiges Testen, von multiplen, voneinander unabhängigen, sowie ausgebildeten Kräften umgesetzt werden sollte, damit die Erkennung von potentiellen Fehlern mehrfach abgesichert und dadurch das Risiko von unerwünschten Ereignissen deutlich reduziert ist. Software die quelltextoffen und damit transparent ist, ermöglicht außerdem das Erkennen von strukturellen Fehlern.*

Risikograph (Regelbetrieb Softwareupdate gemäß Microsoft Windows Prozeß ≙ ungetestet):



≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzung (Akzeptiertes Standardrisiko). Die Aufgabe der Datenaktualisierung entspricht dem Installieren von Software.
✖	
✖	
W3	Eine relativ hohe Auftretenswahrscheinlichkeit und häufige unerwünschte Ereignisse sind wahrscheinlich. *Hinweis:* *Die Auftretenswahrscheinlichkeit ist von der Absicherung des Validierungsprozesses des OS (OEM) abhängig.*

3.2.9 UC-09 Datenentsorgung

Nachdem der Umlauf beendet (UC-07 Fahrzeug abrüsten → UC-09) ist und das Fahrzeug sich auf dem Betriebshof befindet, sendet der ÖV-Bordrechner statistische Daten (Fahrgastzähldaten, Ticketverkaufsdaten, Ankunfts- und Abfahrtszeiten etc.) an das Statistik-Hintergrundsystem, wo sie für die spätere Auswertung gespeichert werden. Nach erfolgreicher Übertragung der Daten werden diese vom ÖV-Bordrechner gelöscht.

Während der autonomen Fahrt werden die Systeme der technischen Ausrüstung überwacht, wobei nicht personenbezogene technische Daten im Kraftfahrzeug erhoben und gespeichert werden, welche mit der Datenentsorgung an die AD-Leitstelle zur ordnungsgemäßen Datenarchivierung, gemäß den Aufbewahrungsfristen, übergeben werden.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Datensicherung, Datenaufbewahrung und zeitgerechte Datenentsorgung	Die OV-Leitstelle ist für die Datenarchivierung der Fahrgastdaten gemäß den Aufbewahrungspflichten verantwortlich.
BHMS	Datensicherung, Datenaufbewahrung und Datenentsorgung unter Beachtung der Betriebsvorschriften (Verfahrensanweisung / Arbeitsvorschrift) zur Datensicherung, Datennutzung und Datenentsorgung	Gewährleistung des vorschriftsmäßigen Umgangs mit Daten.
AD-Leitstelle	Datensicherung, Datenaufbewahrung und zeitgerechte Datenentsorgung	Die AD-Leitstelle ist für die Datenarchivierung der AD-Fahrzeugdaten inklusive der Überwachungs-aufzeichnung gemäß den Aufbewahrungspflichten verantwortlich. Die Berichte sind zu dokumentieren und vom Halter oder von der für die Technische Aufsicht verantwortlichen Person sechs Monate lang aufzubewahren und nach Ablauf dieser Frist unverzüglich, bei elektronischer Speicherung automatisiert, zu löschen.

Hinweis:
Das Betriebshofmanagementsystem (BHMS) umfaßt das Planungs- und Steuerungssystem für alle Vorgänge auf dem Betriebshof, z.B. Abstellen, Rangieren, Kuppeln, Waschen, Tanken, etc. von Bussen.

Hinweis:
Zuständigkeit = ÖV-Bordrechner für die Sicherung der ÖV-Fahrgastdaten (Statistikwerte, z.B. Anzahl Fahrgäste).
Zuständigkeit = AD-Bordsystem für die Sicherung der AD-Fahrzeugdaten (Ereignisse / Logfiles).

Betriebsschutz:
Zugang zum Betriebshof und der ÖV- bzw. AD-Leitstelle (jeweilige Sicherheitszone) haben nur ausgebildete und (sicherheitstechnisch) geschulte Mitarbeiter, Fahrgäste haben keinen Zugang.

Situation:
Automatisierte Datensicherung / -archivierung zum Einsatzende (Regelbetrieb).

Aktionen:

- Der ÖV-Bordrechner setzt die Datensicherung der Statistikdaten und die anschließende Datenentsorgung (Löschung der Daten) in den ÖV-Fahrzeugsystemen gemäß DSGVO um.
  Die ÖV-Leitstelle ist für die ÖV-Datenarchivierung gemäß den Aufbewahrungspflichten verantwortlich.
- Das AD-Bordsystem setzt die Datensicherung der Fahrzeugdaten (Ereignismeldungen und Logfiles) plus die anschließende Datenentsorgung (Löschung der Daten) in den AD-Fahrzeugsystemen gemäß DSGVO um.

- Die AD-Leitstelle überprüft die Ereignismeldungen (kategorisiert und priorisiert) plus die Meldungen aus dem Software Vulnerability Management (SVM) auf einen resultierenden Handlungsbedarf und leitet im Bedarfsfall die Instandsetzung (Auftrag an das BHMS) inklusive ggf. UC-08 Datenaktualisierung ein.
  Hinweis:
  Sofern keine Instandsetzungsanforderung(en) aus den Ereignismeldungen hervorgehen, ist dieses zum Zwecke des Nachweises der Prüfung zu dokumentieren.
  Die AD-Leitstelle ist für die AD-Datenarchivierung gemäß den Aufbewahrungspflichten verantwortlich.
  Hinweis (AFGBV § 13 Anforderungen an den Halter Absatz 4):
  Zur dauerhaften Überwachung der technischen Ausrüstung werden nicht personenbezogene technische Daten im Kraftfahrzeug erhoben und gespeichert. → Diese werden mit der Datenentsorgung an die AD-Leitstelle zur ordnungsgemäßen Datenarchivierung, gemäß den Aufbewahrungsfristen, übergeben.

Juristische Anforderungen:

- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 1
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen die Fahrzeugsysteme für die aktive und passive Sicherheit des Kraftfahrzeugs mit autonomer Fahrfunktion regelmäßig überprüft werden.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 4
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß die Ergebnisse der Gesamtprüfungen nach Nummer 3 einschließlich einer Beschreibung aller festgestellten Mängel und durchgeführter Instandsetzungen in einem Bericht dokumentiert und dem Kraftfahrt-Bundesamt sowie der zuständigen Behörde auf Verlangen unverzüglich übermittelt werden, sofern dies erforderlich ist.
- AFGBV §13 Anforderungen an den Halter Absatz 3
  Der Halter muß sicherstellen, daß Anweisungen zur ordnungsgemäßen Durchführung der Wartungsarbeiten, der Gesamtprüfungen, weiterer Untersuchungen und Fahrten im manuellen Fahrbetrieb vorliegen und daß diese Anweisungen befolgt werden. Die Anweisungen sind zu dokumentieren.
- AFGBV §13 Anforderungen an den Halter Absatz 4
  Berichte über die Durchführung von Wartungsarbeiten, von Gesamtprüfungen und von weiteren Untersuchungen müssen durch den Halter oder die verantwortliche Person unverzüglich schriftlich oder elektronisch erstellt werden. Die Berichte sind zu unterzeichnen. Die Berichte sind zu dokumentieren und vom Halter oder von der für die Technische Aufsicht verantwortlichen Person sechs Monate lang aufzubewahren und nach Ablauf dieser Frist unverzüglich, bei elektronischer Speicherung automatisiert, zu löschen.
- AFGBV §13 Anforderungen an den Halter Absatz 5
  Die Anforderungen zur Dokumentenverwaltung für die Anweisungen nach Absatz 3 und der Berichte nach Absatz 4 müssen dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik wird vermutet, wenn die Vorgaben der ISO 9001:2015 Qualitätsmanagementsysteme – Grundlagen und Begriffe erfüllt werden. Darüber hinaus muß die Dokumentenverwaltung den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 genügen.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA)
  → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV §15 Datenspeicherung Absatz 2
  Die gespeicherten Daten dürfen nur durch das Kraftfahrt-Bundesamt und die zuständige Behörde und nur zum Zweck der Nachprüfung der Erfüllung der Voraussetzungen der Genehmigung und der mit der Genehmigung verbundenen Überwachungspflichten erhoben, gespeichert und verwendet werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.1 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur dynamischen Ausübung der Fahraufgabe gilt:
  a) Zur dauerhaften Überwachung der technischen Ausrüstung werden nicht personenbezogene technische Daten im Kraftfahrzeug erhoben und gespeichert.
  b) Eine Beeinträchtigung der technischen Ausrüstung ist der Technischen Aufsicht unverzüglich anzuzeigen.
- AFGBV Anlage 1 Teil 1 Abschnitt 7.2 Sicherheitskonzept
  In dem Sicherheitskonzept ist die Sicherheit der Fahrfunktion zu bewerten. Mit einem systematischen Vorgehen müssen die für die Operational Design Domain (ODD) relevanten gefährlichen Szenarien und Ereignisse identifiziert und in einer Risikoanalyse bewertet werden. Um Gefährdungen zu verhindern oder deren Risiko auf ein akzeptables Maß zu mindern, muß ausgehend von erkannten Risiken für die entsprechenden Szenarien und Ereignisse ein Systemverhalten definiert oder müssen Systemverbesserungen umgesetzt werden. Die Systematik muß dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO/PAS 21448:2019-01 Straßenfahrzeuge – Sicherheit der beabsichtigten Funktion erfüllt werden. Die ausreichende Vollständigkeit

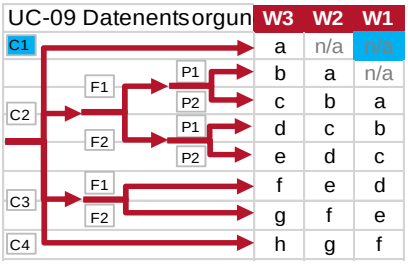
der Szenarien wird auf Basis von Validierungsfahrten oder anderen Datenaufzeichnungen im Fahrbetrieb durch statistische Analysen belegt.
Hinweis:
ISO-21448:2022 Road vehicles – Safety of the intended functionality (SOTIF)
Hinweis:
AFGBV Anlage 3 Dokumentationspflichten des Herstellers Kapitel 3 spezifiziert die Anforderungen

- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.2 Technische Vorgaben für das Speichern, Auslesen und Übertragen von Daten
  Das System der Datenspeicherung darf nicht flüchtig sein. Die gespeicherten Daten müssen im stromlosen Zustand erhalten bleiben.
- AFGBV Anlage 2 Datenspeicherung
  Während des Betriebs sind bei den in § 1g Absatz 2 des Straßenverkehrsgesetzes genannten Anlässen im Kraftfahrzeug mit autonomer Fahrfunktion folgende Daten zu erfassen.
  → Tabelle s. Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert.
  - ► Besondere Sorgfalt ist zu gewährleisten bei den Anforderungen zur Datensicherung, deren Verwendung und Löschung gemäß den juristisch vorgegeben Aufbewahrungszeiten.
    (Klassifizierung von Unterlagen und deren Datenarchivierung).

Risikograph:



≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzung (Akzeptiertes Standardrisiko beim Arbeiten / Büro- / IT-Tätigkeiten)
✖	
✖	
W1	Eine sehr geringe Auftretenswahrscheinlichkeit (nur einmal am Tag) und nur wenige unerwünschte Ereignisse sind wahrscheinlich

3.2.10 UC-10 Fahrgastzählung

In einigen Fahrzeugen sind Fahrgastzähleinrichtungen installiert. Diese sammeln Daten über ein- und ausgestiegene Personen und senden diese an den ÖV-Bordrechner. Dieser sendet die Daten dann in einem bestimmten Intervall oder auf Anforderung an die ÖV-Leitstelle. Dort können sie zur Anzeige des aktuellen Besetztgrades und in Verbindung mit den historischen Zähldaten aus dem Statistik-Hintergrundsystem zur Aktualisierung der Auslastungsprognose verwendet werden.

Anmerkung:
Werden die Fahrgastzähldaten ausschließlich für statistische Zwecke genutzt, kann auf die Echtzeitübertragung verzichtet werden. Die Zähldaten werden dann i. d. R. am Ende des Betriebstages auf dem Betriebshof direkt an das Hintergrundsystem übertragen (siehe UC-09 Datenentsorgung).

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Datensicherung, Datenauswertung und zeitgerechte Datenaufbewahrung bis zur zeitgerechten Datenentsorgung.	Die ÖV-Leitstelle ist verantwortlich für die Datenauswertung inklusive der Datenarchivierung der Fahrgastdaten gemäß den Aufbewahrungspflichten, s. ggf. UC-09 Datenentsorgung.
BHMS	Das BHMS ist zuständig für die Datenentsorgung (gemäß UC-09 Datenentsorgung) der Fahrgastdaten unter Beachtung der Betriebsvorschriften (Verfahrensanweisung / Arbeitsvorschrift) zur Datensicherung, Datennutzung und Datenentsorgung inklusive deren Übermittlung an die ÖV Leitstelle.	Gewährleistung des vorschriftsmäßigen Umgangs mit Daten.
AD-Leitstelle	keine	keine

Hinweis:
Das Betriebshofmanagementsystem (BHMS) umfaßt das Planungs- und Steuerungssystem für alle Vorgänge auf dem Betriebshof, z.B. Abstellen, Rangieren, Kuppeln, Waschen, Tanken, etc. von Bussen.

Hinweis:
Zuständigkeit = ÖV-Bordrechner für die Sicherung der ÖV-Fahrgastdaten (Statistikwerte, z.B. Anzahl Fahrgäste).

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Statistische Auswertung (Regelbetrieb).

Aktionen:

- Diese Tätigkeit wird in der Regel als Bestandteil von UC-09 Datenentsorgung umgesetzt.

Juristische Anforderungen:

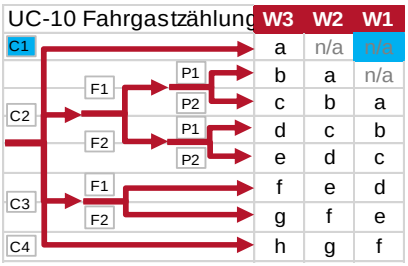
- AFGBV Anlage 1 Teil 5 Anforderungen an die Sicherheit im Bereich der Informationstechnologie
- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.

- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert.

Risikograph:



≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzungen durch den gefährlichen Vorfall (Akzeptiertes Standardrisiko bei Bürotätigkeiten, hier Statistik)
✖	
✖	
W1	Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich

3.2.11 UC-11 Stauerkennung

Erkennt der ÖV-Bordrechner, daß das Fahrzeug sich wahrscheinlich in einer Stausituation befindet (geringe Strecke innerhalb einer bestimmten Zeit zurückgelegt), sendet er eine Meldung an die ÖV-Leitstelle. Die Staumeldung wird dem Disponenten angezeigt, der aufgrund der Information ggf. notwendige Maßnahmen einleiten kann. Sobald die periodisch geprüfte Staubedingung nicht mehr vorliegt, sendet der ÖV-Bordrechner eine entsprechende Meldung an die ÖV-Leitstelle.

Hinweis:
Die Erkennung, daß eine Stausituation vorliegt, kann alternativ auch auf Basis der periodischen Standortmeldungen in der ÖV-Leitstelle erfolgen.
(Dann entfällt entsprechend die hier dargestellte Kommunikation zwischen Fahrzeug und ÖV-Leitstelle).

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Überwachung der Fahrplaneinhaltung plus ergreifen von Maßnahmen, sofern erforderlich.	Umsetzbarkeit der Fahrplandaten, insbesondere Pünktlichkeit unter Beachtung, daß eine angemessene Zeit für den Fahrgastwechsel für die jeweilige Mission gegeben ist. Aussagekräftige Durchsagen zur Fahrgastinformation (FGI) abrufbar bereitstellen.
BHMS	keine	keine
AD-Leitstelle	keine	keine

Hinweis:
Zuständigkeit = ÖV-Bordrechner für die Erfassung (Speicherung) der ÖV-Fahrgastdaten (Statistikwerte, Fortschritt der Fahrt / Mission), sofern nicht eine kontinuierliche Fortschrittsmeldung an die ÖV-Leitstelle erfolgt. Es obliegt dem ÖPNV Unternehmen die für ihn geeignete Methodik festzulegen und umzusetzen.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Statistische Auswertung Fahrplan Pünktlichkeit (Regelbetrieb).

Aktionen:

- Der ÖV-Bordrechner überwacht die Einhaltung der von der ÖV-Leitstelle geplanten Fahrplandaten und meldet die Abweichungen entweder kontinuierlich oder gesammelt am Ende des Umlaufes / Tages an die ÖV-Leitstelle zur statistischen Auswertung im Rahmen des kontinuierlichen Verbesserungsprozesses (KVP).
  Hinweis:
  Unter Überwachung (Monitoring) versteht man alle Arten von systematischen Erfassungen, Messungen und Beobachtungen eines Vorgangs oder Prozesses mittels technischer Hilfsmittel oder anderer Beobachtungssysteme sowie dessen analytische Auswertung (inkl. Bewertung anhand von spezifischen Metriken) zur Verifikation, um bei dem beobachteten Ablauf oder Prozeß festzustellen, daß dieser den gewünschten Verlauf nimmt und bestimmte Schwellwerte eingehalten werden.

Juristische Anforderungen:

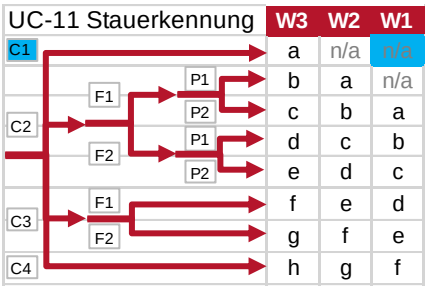
- AFGBV Anlage 1 Teil 5 Anforderungen an die Sicherheit im Bereich der Informationstechnologie
- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.

- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert.

Risikograph:



≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzungen durch den gefährlichen Vorfall. (Akzeptiertes Standardrisiko bei Bürotätigkeiten, hier automatisierte Prozeßfortschrittsüberwachung)
✖	
✖	
W1	Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich

3.2.12 UC-12 Systemüberwachung und ggf. Störmeldung

Die Komponenten eines Fahrzeugsystems werden im gesamten laufenden Betrieb, d.h. von der Aufrüstung (Vorbereitung), über den Betrieb, bis hin zur Abrüstung (Nachbereitung) überwacht, mit Prozessen, welche den Reifegrad Automotive SPICE® Capability Level 2 erfüllen.

Dieses kann manuell durch eine Servicekraft (BHMS / Werkstatt) oder im konventionellen Betrieb durch das Fahrpersonal umgesetzt werden, wobei automatisierte Systemprüfungen über Statusmeldungen einfließen.

Im autonomen Fahrbetrieb erfolgt dieses über (teil-)automatisierte Systeme mit Bilderkennung und Messung von Parametern von Komponenten, welche an die zuständige Stelle übermittelt werden.

In Abhängigkeit vom Geschäftsprozeß kann während der Auf- und Abrüstung die zuständige Stelle das Betriebshofmanagementsystem (BHMS) sein, wobei das Fahrzeug neben der autonomen Fahrt auch per Fernsteuerung manuell gesteuert werden kann. Im autonomen Fahrbetrieb erfolgt die Überwachung durch die technische Aufsicht in der AD-Leitstelle.

Prinzipieller Ablauf von Störungen und deren Handhabung:

- Im Regelbetrieb tritt an einer Komponente eine Störung auf.
  Hinweis:
  Mehrere gleichzeitig auftretende Störungen können von unterschiedlichen Systemen oder Funktionen parallel behandelt werden.
- Die Störung wird von der Systemüberwachung erkannt.
  Hinweis:
  Diese kann von der Komponente selbst oder einer anderen Komponente, z.B. durch das Ausbleiben (Time-out) einer Statusänderung auf der Schnittstelle, erkannt werden.
- Die Systemüberwachung leitet Maßnahmen der Fehlerkorrektur und/oder der potentiellen Schadensminderung ein.
  Hinweis:
  Dieses kann z.B. ein Ersatzwert (sicherer Zustand oder Zeitersatzwert aus der Interpolation) oder auch das Hinzuschalten von Dämpfungs- bzw. Unterstützungsleistung sein.
- Dokumentation des Ereignisses (Ereignismeldung im Protokoll)
- Kommunikation der (Warn-)Meldung an den Fahrer (im konventionellen Betrieb) bzw. zur AD-Leitstelle (im autonomen Betrieb) sowie, sofern dieses sinnvoll und zweckmäßig ist, Benachrichtigung / Einbindung von weiteren Einheiten (BHMS / ÖV-Leitstelle, FGI, FG-NFM und/oder Bergungs- und Einsatzkräfte).

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Überwachung Fahrplandaten plus Aktualisierung der Fahrplanumsetzung auf Einhaltung der Fahrplandaten inklusive Pünktlichkeit. Informieren der Fahrgäste über Abweichungen gegenüber dem Fahrplan inklusive Unterstützung bei der Sicherstellung des reibungslosen Reiseablaufes der Fahrgäste.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung).
BHMS	Instandhaltung und Wartung der Systeme inklusive Nachweis der technischen Verwendbarkeit.	Instandhaltung und Wartung der Systeme zur Sicherstellung der Betriebsfähigkeit.
AD-Leitstelle	Fahrzeugüberwachung und Konfiguration der Fahrbereitschaft zur Aufrechterhaltung der Betriebsfortsetzung, sofern möglich. Andernfalls Bergung veranlassen.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Die planbare Instandhaltung durch das BHMS findet nach dem regulären Abrüsten und vor dem Wiedereinsatz, dem Aufrüsten statt.
Im Störungsfall des laufenden Betriebes hat das BHMS keine Tätigkeit, sofern es sich nicht um die Bereitstellung eines Ersatzfahrzeuges oder die Bergung des defekten Fahrzeuges handelt.

Hinweis:
Auf dem Betriebshof können eigenständig Umläufe für Service und Wartung durch das BHMS erstellt und angewendet werden. In diesem Fall übernimmt das BHMS die Rolle des Disponenten, welcher das Anfahren von internen Servicestationen (statt öffentlichen Haltestellen) auf dem BHMS organisiert. Somit wird aus dem Informieren der Fahrgäste, die Information an das Personal der Arbeitsstation.

Hinweis:
Das Operator-HMI (AD) übernimmt die Freigabe sowie Steuerung von Fahrfunktionen inklusive Konfliktbehandlung durch den Operator im Fahrzeug im autonomen Fahrbetrieb.

Hinweis:
Das Fahrzeug-Interface stellt lesenden Zugriff auf technische Zustandsdaten des Fahrzeugs (z.B. Batterie-Ladezustand) zur Verfügung.

Hinweis:
Das Verkehrsinfrastruktur-Interface umfaßt die Kommunikation mit ansteuerbaren Verkehrs-Infrastruktur-Elementen auf der Strecke und im Betriebshof (LSA, Poller, Schranke, etc.)

Hinweis:
Das Umwelt-IF (AD) umfaßt die Sensorik zur Umwelterfassung und -kommunikation für das automatisierte Fahren. Hierzu zählen Kameras, Radar, LiDAR, AD-Infrastruktur, C2I-Kommunikation und C2C-Kommunikation. Die Aktorik umfaßt sämtliche Einrichtungen, die zur Durchführung des automatisierten Fahrens benötigt werden (Lenkung, Antrieb, Bremse), sowie Türsteuerung, Blinker, Warnleuchten, Hupe, etc.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Fahrzeug befindet sich im Regelbetrieb mit Systemüberwachung
→ Ereignisfall (Besondere Situation / Ereignis → planbarer Regelbetrieb).

Aktionen der Systemüberwachung:

- Die AD-Leitstelle überwacht die autonome Fahrfunktion der Fahrzeuge und reagiert auf Meldungen (über 8) unter Berücksichtigung der Priorisierung.
  Hinweis:
  Die technische Aufsicht der AD-Leitstelle überwacht die fahrerlosen, autonomen Fahrzeuge und greift (ggf. über UC-28 Eingriffsnotwendigkeit Technische Aufsicht) im Bedarfsfall in die Fahrfunktion ein, wobei ein Eingriff die autonome Fahrfunktion beendet. Die technische Aufsicht kann unter Beachtung der gesetzlichen Vorschriften die autonome Fahrfunktion wieder aktivieren.
  Hinweis:
  Ein Eingriff durch den Menschen beendet automatisch den Betriebsmodus „autonome Fahrt“.
  Die Unterstützung des Fahrers, jetzt Technische Aufsicht, durch die Fahrerassistenzsysteme des Fahrzeuges (OEM) bleibt erhalten.
- Die Systemüberwachung der ÖV-Leitstelle wertet die Meldungen des ÖV-Bordrechners aus und greift regulierend ein sofern dispositive Maßnahmen erforderlich / sinnvoll sind.
  Hinweis:
  Hierzu zählen z.B. die Umleitung des Fahrzeuges im Stau (z.B. durch einen Unfall auf der Strecke), sowie das Aussenden eines Ersatzfahrzeuges, falls das geplante Fahrzeug im Stau feststeckt, damit die Fahrgäste von den noch nicht bedienten Haltepositionen /-stellen abgeholt werden.
- Der ÖV-Bordrechner überwacht die Fahrgastinformationssysteme (Fahrgastanzeiger, etc.) und steuert die automatisierten Ansagen bzgl. Fahrgastinformationen (Haltestelle / -position), welche ggf. auch von der ÖV-Leitstelle ferngesteuert werden können.
- Das AD-Bordsystem überwacht die autonome Fahrt über die Sensorik und die Peripherie des Fahrzeugs und kommuniziert sowohl mit der AD-Leitstelle, als auch über die AD-Infrastruktur mit dem Fahrgast. Störungen werden (über 8) an die Technische Aufsicht der AD-Leitstelle sowie informativ (über 14) an den ÖV-Bordrechner übermittelt.
- Das BHMS überwacht die Reparatur- und Wartungsinformationen für das Kraftfahrzeug gemäß den Herstellervorgaben, führt die juristisch vorgeschriebenen Fahrfunktionsprüfungen durch und erstellt die zugehörige Nachweisdokumentation inklusive Dokumentation der Defekte und deren Behebung.
  Hinweis:
  Das BHMS nutzt die Abstellzeit (downtime) für die Reinigung, Wartung und Instandhaltung, sowie die Absicherung der Aufrechterhaltung der Betriebsbereitschaft inklusive Durchführung der regelmäßigen Gesamtprüfung zur Genehmigungserhaltung.
  Hinweis:
  Solange sich das Fahrzeug auf dem Betriebshof befindet werden die Meldungen vom ÖV-Bordrechner (über 6) an das BHMS statt (über 7) an die ÖV-Leitstelle gesendet.

Situation:
Fahrzeug befindet sich im Regelbetrieb als eine Störung erkannt wird.

Aktionen der Störungserkennung autonome Fahrt:

- Die AD-Leitstelle erkennt eine Störung durch
  - eingeschränkte Sicht, z.B. Nebel
    → AFGBV Anlage 1 Teil 1 Abschnitt 1.4 Reaktion auf Umweltbedingungen
  - technische Werte, z.B. Außentemperatur im Gefrierbereich
    → AFGBV Anlage 1 Teil 1 Abschnitt 1.4 Reaktion auf Umweltbedingungen
  - das Vermissen von Routine-Meldungen
  - die Aufforderung zur Übernahme durch das AD-Bordsystem
    ← UC-28 Eingriffsnotwendigkeit Technische Aufsicht.

- Das AD-Bordsystem erkennt eine Störung durch
  - die Systemüberwachung
    Hinweis:
    Das AD-Bordsystem überwacht kontinuierlich die autonome Fahrt über die Sensorik und die Peripherie des Fahrzeugs und sendet technische Informationen (über 8) an die AD-Leitstelle.
  - die Meldung eines Bauteils z.B. der AD-Peripherie

Hinweis:
Das AD-Bordsystem meldet Störungen (über 8) an die AD-Leitstelle zur Bearbeitung, sowie (über 14) informativ an den ÖV-Bordrechner. Der ÖV-Bordrechner verarbeitet die Störungsinformation und meldet, sofern sich das Fahrzeug außerhalb des Betriebshofes befindet und gewünscht, dieses (über 7) an die ÖV Leitstelle zur weiteren Bearbeitung. Sollte sich das Fahrzeug im Betriebshof befinden, so erfolgt die Meldung (über 6) an das BHMS.

Aktionen (Einleitung von Maßnahmen) der Störungsbehandlung autonome Fahrt:

- Die Systemüberwachung des AD-Bordsystems leitet stabilisierende Maßnahmen der Fehlerkorrektur, Stabilisierung, Robustheit ein und überprüft ob die Maßnahmen hinreichend wirksam sind.
  - Sofern die Maßnahmen hinreichend sind, erfolgt ein Ereigniseintrag.
    Hinweis: hinreichend bedeutet, daß die Maßnahmen die Störung kompensieren können.
  - Sofern die Maßnahmen unzureichend sind, erfolgt (über 8) eine Warnmeldung (z.B. Meldung: Lenkung ist schwergängig, Unterstützungsleistung ist häufig aktiv) an die AD-Leitstelle.
    Hinweis:
    unzureichend bedeutet, daß die Maßnahmen die Störung nur teilweise, jedoch ausreichend, kompensieren können (Warnlampe Gelb).
    Hinweis:
    Abhängig von der Art der Störung kann das AD-Bordsystem durch das Aktivieren des Warnblinkers die Umgebung warnen. Folglich kann ein Eingriff der Technischen Aufsicht (TA) der AD-Leitstelle notwendig werden, um den Warnblinker wieder zu deaktivieren oder das Fahrzeug manuell zu übernehmen.
  - Sofern die Maßnahmen ungenügend sind, wird das Minimum Risk Manoeuvre (MRM) ausgeführt und das AD-Bordsystem meldet (über 8) die Systemstörung an die AD-Leitstelle sowie (über 14) an den ÖV-Bordrechner.
    Hinweis: ungenügend bedeutet, daß die Maßnahmen die Störung nicht ausreichend kompensieren können ⚠ Warnlampe Rot.
    Hinweis: Bei einem Minimum Risk Manoeuvre (MRM) ist unabhängig der Kategorie (A bis E) der Warnblinker zu aktivieren.
    - Die Technische Aufsicht (TA) der AD-Leitstelle analysiert die Ursache / Auslösung des Minimum Risk Manoeuvres (MRM) und ergreift geeignete Maßnahmen um die Störung zu beheben damit der reibungslose Betrieb fortgeführt werden kann, sofern dieses nicht möglich sein sollte werden Maßnahmen ergriffen, welche das Schadenspotential bestmöglich reduzieren. Dazu kann die AD-Leitstelle weitere Daten vom Fahrzeug über das AD-Bordsystem anfordern, z.B.
      - Daten auslesen (über 17) vom Fahrzeug-Interface.
      - Daten auslesen (über 18) vom Verkehrs-Infrastruktur-Interface.
      - Daten lesen und schreiben (über 19) vom Umwelt-Interface AD.
        Hinweis (Randbedingung):
        Die Außenumgebung vor dem Fahrzeug wird (über UM0.19.2 CameraImage) übertragen.
      - Der Fahrgastraum kann über das Operator HMI AD (über 15) eingesehen werden, hierbei sind die Datenschutzvorschriften nach Artikel 35 der Verordnung (EU) 2016/679, insbesondere die Anforderungen an die Informationstechnik nach Teil 5 und damit die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 einzuhalten. Die Fahrgäste sind vor der Einsicht über das Aktivieren der Kamera dbzgl. anzusprechen (Umsetzung der Informationspflicht).
        Hinweis (Randbedingung):
        Die Innenraumumgebung kann (über UM0.15.3 CamaraImage) eingesehen werden.
      - Das AD-Bordsystem kann auf Basis von Statistikdaten, KI gestützt, Vorschläge zur Behebung der Störung der AD-Leitstelle unterbreiten. ← UC-31 Entscheidungshilfe (Fahrtfortsetzung).
    - Sofern das Minimum Risk Manoeuvre (MRM) durch einen Defekt am Kraftfahrzeug ausgelöst wurde, muß die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage I Ziffer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
    - Die Technische Aufsicht (TA) der AD-Leitstelle informiert (über 3) die ÖV-Leitstelle falls ein Fahrzeugausfall vorliegen oder eine Außerbetriebnahme sinnvoll sein sollte → UC-27 Ersatzfahrzeug bereitstellen.
      Hinweis:
      Das AD-Bordsystem meldet Störungen zur Bearbeitung (über 8) an die AD-Leitstelle sowie informativ (über 14) an den ÖV-Bordrechner. Der ÖV-Bordrechner verarbeitet die Störungsinformation und meldet, sofern sich das Fahrzeug außerhalb des Betriebshofes befindet und gewünscht, dieses (über 7) an die ÖV Leitstelle zur weiteren Bearbeitung. Sollte sich das Fahrzeug im Betriebshof befinden, so erfolgt die Meldung (über 6) an das BHMS.

Aktionen der Störungserkennung Disposition (Fahrplanabweichung / Pünktlichkeit):

- Die ÖV-Leitstelle erkennt eine Fahrplanabweichung (Störung der Pünktlichkeit).
  Hinweis:
  Dieses kann durch Verkehrsdurchsagen / Staumeldungen / TMC realisiert werden.
- Der ÖV-Bordrechner erkennt eine Fahrplanabweichung (Störung der Pünktlichkeit) durch Istwert zu Sollwert Vergleich der aktuellen Position.
- Das AD-Bordsystem erkennt bei der Missionsprüfung, daß die geplante Mission nicht umsetzbar ist, weil die geplante(n) Sollzeit(en) zwischen zwei Wegpunkten eine Geschwindigkeit erfordert, welche über der Geschwindigkeitsbegrenzung liegt, weshalb die Mission abzulehnen ist.
  (Vorsätzlicher Verstoß gegen die StVO ist zu unterlassen).
  Hinweis:
  Das AD-Bordsystem kann die notwendigen Fahrzeiten auf Basis der Geschwindigkeitsbegrenzung selbständig berechnen (automatisiert beheben) und dieses als Information an die ÖV-Leitstelle mit der Fehlermeldung zu der FZ-Mission (Anteil der ÖV-Mission) rückmelden, z.B. Fehler in den Fahrzeiten durch Geschwindigkeitsbegrenzung. Die daraus ermittelte Korrektur geht als Vorschlag an den ÖV-Disponenten, welcher den Anteil der ÖV-Mission und den Fahrplan entsprechend aktualisiert, sowie ggf. über das FGI ausrollt.
- Das AD-Bordsystem erkennt bei der Missionsprüfung, wenn eine / mehrere Position(en) nicht in der hochauflösenden Karte eingezeichnet sind, woraufhin die Nicht-Umsetzbarkeit als Störungsmeldung (nicht behebbare Fehler) zur Bearbeitung an die ÖV-Leitstelle (über 14 + 7) sowie informativ (über 8) an die AD-Leitstelle rückgemeldet wird.

Aktionen (Einleitung von Maßnahmen) der Störungsbehandlung Disposition:

- Der Disponent aktualisiert den Fahrplanung
  - → UC-13 Fahrtänderung
  - → UC-14 Umlaufänderung
  - → UC-15 Neuen Umlauf hinzufügen

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.
- AFGBV §13 Anforderungen an den Halter Absatz 4
  Berichte über die Durchführung von Wartungsarbeiten, von Gesamtprüfungen und von weiteren Untersuchungen müssen durch den Halter oder die verantwortliche Person unverzüglich schriftlich oder elektronisch erstellt werden. Die Berichte sind zu unterzeichnen. Die Berichte sind zu dokumentieren und vom Halter oder von der für die Technische Aufsicht verantwortlichen Person sechs Monate lang aufzubewahren und nach Ablauf dieser Frist unverzüglich, bei elektronischer Speicherung automatisiert, zu löschen.
- AFGBV §13 Anforderungen an den Halter Absatz 5
  Die Anforderungen zur Dokumentenverwaltung für die Anweisungen nach Absatz 3 und der Berichte nach Absatz 4 müssen dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik wird vermutet, wenn die Vorgaben der ISO 9001:2015 Qualitätsmanagementsysteme – Grundlagen und Begriffe erfüllt werden. Darüber hinaus muß die Dokumentenverwaltung den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 genügen.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach §1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie in der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik, Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik über einen Abschluß verfügt als
  - ► Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert),
  - ► Bachelor, Master oder
  - ► staatlich geprüfter Techniker.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 2
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie eine entsprechende Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen hat.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 3
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muß, und
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 4
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihr anvertrauten Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes zuverlässig ist.
  Zur Beurteilung der Zuverlässigkeit im Sinne des Satzes 2 Nummer 4 sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde, eine Auskunft aus dem Fahrerlaubnisregister sowie eine Auskunft über Eintragungen aus dem Fahreignungsregister vorzulegen. Sofern in dem Fahrerlaubnisregister mehr als drei Punkte eingetragen sind, ist die Zuverlässigkeit nicht gegeben. § 8 Absatz 3 gilt bezüglich Satz 3 entsprechend.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 2
  Die als Technische Aufsicht eingesetzte natürliche Person darf sich mit Zustimmung des Halters zur Erfüllung ihrer Pflichten weiterer geeigneter natürlicher Personen bedienen, die über mindestens drei Jahre Berufserfahrung im Bereich des Verkehrs- oder Kraftfahrzeugwesens verfügen. Die eingesetzten natürlichen Personen müssen wiederkehrend, mindestens jedoch jährlich beim Hersteller in Bezug auf den Umgang mit dem Kraftfahrzeug sowie wesentliche Veränderungen am Kraftfahrzeug oder der autonomen Fahrfunktion geschult werden. Die Schulung ist mit einer praktischen Prüfung einschließlich der Bewältigung simulierter Betriebsstörungen abzuschließen. Der erfolgreiche Abschluß der Schulung von eingesetzten natürlichen Personen ist von der Technischen Aufsicht zu dokumentieren. Sollen die eingesetzten natürlichen Personen Fahrten im manuellen Fahrbetrieb übernehmen oder Fahrmanöver freigeben, müssen diese Personen eine gültige Fahrerlaubnis besitzen. Die Klasse der Fahrerlaubnis muß der des Fahrzeugs mit autonomer Fahrfunktion entsprechen.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 3
  Befindet sich das Kraftfahrzeug mit autonomer Fahrfunktion im risikominimalen Zustand im Sinne des § 1d Absatz 4 des Straßenverkehrsgesetzes, hat die als Technische Aufsicht eingesetzte natürliche Person eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durchzuführen, bevor sie dessen Beendigung veranlassen darf. Das Ergebnis der Untersuchung ist zu dokumentieren. Wurde der risikominimale Zustand durch einen Defekt am Kraftfahrzeug ausgelöst, muß nach Erreichen des risikominimalen Zustands die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage 1 Nummer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
  Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist ungeachtet der Sätze 1 und 3 das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen. In diesen Fällen erfolgt die Untersuchung der Technischen Aufsicht gemäß Satz 1 im Nachgang des Abtransports auf Grundlage der gespeicherten Fahrdaten.
- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
  Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro

Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind.

- AFGBV Anlage 1 Teil 1 Abschnitt 1.1 Generelle Kollisionsvermeidung
  Kollisionen mit anderen Verkehrsteilnehmenden und unbeteiligten Dritten müssen vermieden werden, sofern dies durch
  1. Notbremseingriffe oder
  2. andere Teilnehmende des umgebenden Verkehrs, andere unbeteiligte Dritte oder die Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nicht gefährdende Ausweichmanöver möglich ist. Kann eine Kollision zur Abwendung einer Gefährdung des Lebens der Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nur durch eine Gefährdung des Lebens anderer Teilnehmender des umgebenden Verkehrs oder unbeteiligter Dritter vermieden werden (unvermeidbare alternative Gefährdung von Menschenleben), darf der Schutz der anderen Teilnehmenden des umgebenden Verkehrs und der unbeteiligten Dritten nicht nachrangig gegenüber dem Schutz der Insassen des autonom fahrenden Kraftfahrzeugs erfolgen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.2 Interaktion mit anderen Verkehrsteilnehmenden
  a) Vorausfahrende Verkehrsteilnehmende auf der Fahrbahn werden erkannt. Es wird jederzeit in jedem Geschwindigkeitsbereich und in jeder möglichen Fahrsituation ein angemessener Sicherheitsabstand eingehalten. Der einzuhaltende Sicherheitsabstand bestimmt sich nach § 4 der Straßenverkehrs-Ordnung.
  b) Der Fahrstreifenwechsel vorausfahrender oder nachfolgender Fahrzeuge, der von einem benachbarten Fahrstreifen in den eigenen Fahrstreifen oder aus dem eigenen Fahrstreifen heraus in einen benachbarten Fahrstreifen erfolgt, wird erkannt und bei der Fahraufgabe entsprechend berücksichtigt.
  c) Situationen, welche einen Fahrstreifenwechsel bedingen (beispielsweise anhaltende oder langsame Fahrzeuge auf der Fahrbahn, Ende eines Fahrstreifens), werden erkannt und geeignete Manöver zum Fahrstreifenwechsel werden sicher durchgeführt.
  d) Einsatzfahrzeuge werden erkannt und geeignete Fahrmanöver sicher durchgeführt.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.3 Planung der Fahrpfade und Geschwindigkeiten
  Bei Geschwindigkeitsanpassungen kommt es zu keiner vermeidbaren Beeinträchtigung von Insassen, anderen Verkehrsteilnehmenden und unbeteiligten Dritten. Es gelten folgende Anforderungen:
  a) Geschwindigkeitsbeschränkungen und Änderungen der Geschwindigkeitsbeschränkung werden erkannt und die Geschwindigkeit wird entsprechend angepaßt.
  b) Besondere Anforderungen an die Geschwindigkeit werden erkannt und im Geschwindigkeits- und Fahrtverlauf befolgt (beispielsweise in Bereichen vor Schulen und an Arbeitsstellen an Straßen, an Bushaltestellen, Bahnübergängen, in engen Kurvenradien oder bei Gefällen, in Engstellen, in denen der eigene Fahrstreifen vom Gegenverkehr mitbenutzt werden muß).
  c) Zeichen und Weisungen der Polizeibeamten gemäß § 36 der Straßenverkehrs-Ordnung, Wechsellichtzeichen gemäß § 37 der Straßenverkehrs-Ordnung, sonstige Zeichen gemäß der §§ 39 bis 42 der Straßenverkehrs-Ordnung sowie Verkehrseinrichtungen gemäß § 43 der Straßenverkehrs-Ordnung werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  d) Situationen, in denen die Vorfahrt anderen gewährt werden muß (beispielsweise vor Fußgängerüberwegen, in Kreuzungsbereichen oder Einmündungen), werden erkannt und ohne Gefährdung oder Behinderung der Vorfahrtberechtigten bewältigt. Es ist eine berechnete Zeit bis zum Aufprall von mehr als drei Sekunden bezüglich des Vorfahrtberechtigen einzuhalten. Wird von diesen Werten abgewichen, muß dies ausreichend begründet und auf Basis von systematischen Sicherheitsbewertungen nach dem Stand der Technik dokumentiert werden. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO 26262:2018-12 Straßenfahrzeuge – Funktionale Sicherheit erfüllt werden.
  e) Bauliche Straßengestaltungen mit Auswirkung auf das Verhaltensrecht (beispielsweise bis zu 5 Meter vom Fahrbahnrand einer vorfahrtberechtigten Straße abgesetzte Radwege nach § 9 Absatz 3 der Straßenverkehrs-Ordnung oder abgesenkte Bordsteine nach § 10 der Straßenverkehrs-Ordnung) werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  f) Arbeitsstellen an Straßen, temporär veränderte Fahrbahnverläufe oder Fahrbahnmarkierungen werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  g) Defizite am Zubehör, insbesondere der Verkehrseinrichtungen (zum Beispiel verschlissene, beschädigte, fehlende oder defekte temporäre oder dauerhafte Fahrbahnmarkierungen und Verkehrszeichen, Phantommarkierungen) und der Straßenausstattung, insbesondere solcher nach vorstehenden Buchstaben a bis f werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Dies gilt insbesondere nach Sturm- und sonstigen Witterungsereignissen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.4 Reaktion auf Umweltbedingungen
  Wetter-, Umwelt- und Straßeninfrastrukturbedingungen (beispielsweise Regen, Sichtbehinderung durch Rauch, Schlaglöcher) werden im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Fahrpfad und Geschwindigkeit sind – bis hin zum Stillstand des Fahrzeugs – so zu wählen, daß die in den Nummern 1.1 bis 1.3 gestellten Anforderungen auch bei geänderten Umweltbedingungen erfüllt werden.

- AFGBV Anlage 1 Teil 1 Abschnitt 2 Risikominimaler Zustand
  Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur Ausübung der Fahraufgabe gilt: Das Kraftfahrzeug kann nur auf Veranlassung der Technischen Aufsicht den risikominimalen Zustand verlassen.
- AFGBV Anlage 1 Teil 1 Abschnitt 3 Notfahrfunktion
  Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit einer Notfahrfunktion ausgestattet sein. Muß sich das Kraftfahrzeug im Falle eines Defekts am Kraftfahrzeug in den risikominimalen Zustand versetzen, muß dies mit der Notfahrfunktion erfolgen. Fahrten mit der Notfahrfunktion dürfen nur bei Schrittgeschwindigkeit und aktivierter Warnblinkanlage erfolgen. Der Übergang der autonomen Fahrfunktion aus der normalen Fahrt in die Fahrt mit der Notfahrfunktion ist von dieser Geschwindigkeitsbegrenzung ausgenommen, sofern ein Abbremsen erforderlich ist.
- AFGBV Anlage 1 Teil 1 Abschnitt 4 Manueller Fahrbetrieb
  Im manuellen Fahrbetrieb erfüllt eine fahrzeugführende Person die Fahraufgabe. Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit Vorrichtungen ausgestattet sein, die es einer fahrzeugführenden Person ermöglichen, die Fahraufgabe wahrzunehmen. Ist die Steuerung im manuellen Fahrbetrieb auf Geschwindigkeiten nicht höher als Schrittgeschwindigkeit begrenzt, ist es nicht erforderlich, daß die fahrzeugführende Person sich innerhalb des Kraftfahrzeugs mit autonomer Fahrfunktion aufhält. Die Steuerung kann in diesem Fall über eine im Nahfeld des Kraftfahrzeugs befindliche Fernsteuerung ausgeführt werden. Die maximale Distanz, über die eine Fernsteuerung möglich ist, beträgt 6 Meter, gemessen in gerader Verbindung. Die Einhaltung der maximalen Distanz ist vom Hersteller durch geeignete technische Mittel sicher zu stellen. Soll das Kraftfahrzeug mit autonomer Fahrfunktion im manuellen Fahrbetrieb mit Geschwindigkeiten höher als Schrittgeschwindigkeit gesteuert werden, muß es mit einem Sitzplatz für die fahrzeugführende Person ausgestattet sein. Der Sitzplatz ist entsprechend der geltenden Vorschriften zu gestalten.
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.1 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur dynamischen Ausübung der Fahraufgabe gilt:
  a) Zur dauerhaften Überwachung der technischen Ausrüstung werden nicht personenbezogene technische Daten im Kraftfahrzeug erhoben und gespeichert.
  b) Eine Beeinträchtigung der technischen Ausrüstung ist der Technischen Aufsicht unverzüglich anzuzeigen.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.2 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und mit konventionellen Vorrichtungen zur Ausübung der Fahraufgabe gilt:
  Die autonome Fahrfunktion darf nicht erneut aktivierbar sein, solange eine Beeinträchtigung der technischen Ausrüstung besteht.
- AFGBV Anlage 1 Teil 1 Abschnitt 8 Sensorik
  Zur technischen Umsetzung der autonomen Fahrfunktion muß eine Sensorik verwendet werden, die alle für die sichere Erfüllung der Fahraufgabe erforderlichen Gegenstände, Daten oder Personen im Umfeld des Kraftfahrzeugs erfaßt und hinsichtlich der Verarbeitung personenbezogener Daten die Vorgaben der Verordnung (EU) 2016/679, des Bundesdatenschutzgesetzes und spezialgesetzlicher datenschutzrechtlicher Vorschriften beachtet. Zur Erfüllung des in Satz 1 genannten Zwecks und unter Einhaltung der genannten Vorgaben kann die Sensorik durch externe Systeme unterstützt werden. Beeinflussen Wetter-, Umwelt- und Infrastrukturbedingungen die Leistungsfähigkeit der Sensorik, werden von der technischen Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion Maßnahmen eingeleitet, um die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken auszugleichen. Die Sensorik ist in das Sicherheitskonzept des Kraftfahrzeugs mit autonomer Fahrfunktion nach Nummer 7.2 und in die permanente Systemüberwachung nach Nummer 5 einzubinden.
- AFGBV Anlage 1 Teil 1 Abschnitt 9 Alterung und Abnutzung des Systems
  Das Kraftfahrzeug muß die funktionalen Anforderungen auch bei Alterung und Abnutzung der relevanten Systemkomponenten erfüllen. Beeinflussen Alterungserscheinungen die Leistungsfähigkeit, beispielsweise der Sensorik, gleicht die technische Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken durch geeignete Maßnahmen aus.
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der

Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.

- AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse
  Details → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV Anlage 1 Teil 3 Abschnitt 13.2 Technische Vorgaben für das Speichern, Auslesen und Übertragen von Daten → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV Anlage 1 Teil 4 Abschnitt 14.1 Die Technische Aufsicht erteilt eine Fahrmanöverfreigabe an das Kraftfahrzeug mit autonomer Fahrfunktion
  Die technische Ausrüstung versetzt das Kraftfahrzeug in den risikominimalen Zustand, da die Fortsetzung der Fahrt aufgrund einer Verkehrssituation nicht fortgesetzt werden kann. Das Verlassen des risikominimalen Zustands erfolgt mit Unterstützung der Technischen Aufsicht. Folgendes ist hierbei zu beachten:
  a) Die autonome Fahrfunktion kann initial der Technischen Aufsicht mögliche Fahrmanöver zur Fortsetzung der Fahrt vorschlagen und ausreichend Daten zur Beurteilung der Situation liefern.
  b) Wird durch die Technische Aufsicht ein Fahrmanöver vorgegeben, so muß dieses durch die autonome Fahrfunktion validiert werden.
  Unabhängig von den Buchstaben a und b darf das Fahrmanöver nicht ausgeführt werden, wenn daraus eine Gefährdung der am Verkehr Teilnehmenden und unbeteiligter Dritter resultieren würde.
  Die sichere Ausführung oder Nichtausführung solcher Fahrmanöver obliegt weiterhin der autonomen Fahrfunktion mit systemseitiger Auswertung der aktuellen Verkehrssituation vor Ort.
- AFGBV Anlage 1 Teil 4 Abschnitt 14.2 Übernahme der Fahraufgabe durch manuelle Steuerung außerhalb des festgelegten Betriebsbereichs.
  Erreicht die autonome Fahrt die Grenzen des festgelegten Betriebsbereichs, muß das Kraftfahrzeug durch die autonome Funktion in den risikominimalen Zustand versetzt werden. Wird die Fahrt außerhalb der Grenzen des festgelegten Betriebsbereichs durch eine fahrzeugführende Person fortgesetzt, ist die fahrzeugführende Person mittels eines geeigneten Interaktionskonzepts zur Aktivität aufzufordern. Sofern das Stehenbleiben des Kraftfahrzeugs mit autonomer Fahrfunktion den umlaufenden Verkehr oder Dritte behindern würde, ist die Aufforderung durch einen entsprechenden Hinweis zu ergänzen. Die Aufforderung ist in ihrer Intensität fortlaufend zu steigern. Die Aufforderung kann beispielsweise durch Signaltöne in zunehmender Lautstärke oder durch Vibrationen mit zunehmender Intensität erfolgen.

Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

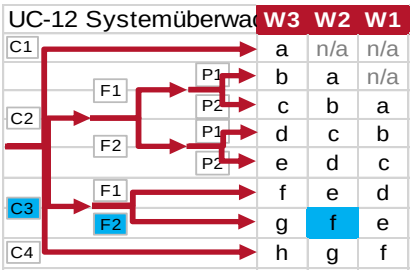
- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.
- BOStrab §3 Absatz 2
  Einrichtungen in Betriebsanlagen und Fahrzeugen, die für die Benutzung oder Betätigung durch Fahrgäste bestimmt sind, müssen gut erkennbar und leicht erreichbar sein. Ihre Handhabung muß sich sinnfällig erkennen lassen; Fehlbedienungen dürfen zu keiner Betriebsgefährdung führen.
- BOStrab §4 Absatz 2
  Betriebsanlagen und Fahrzeuge sind instandzuhalten. Treten an ihnen während des Betriebes Mängel auf, die die Betriebssicherheit beeinträchtigen können, sind sie ganz oder teilweise außer Betrieb zu nehmen und erforderlichenfalls abzusichern.
- BOStrab §4 Absatz 4
  Durch betriebliche Vorkehrungen ist dafür zu sorgen, daß Betriebsstörungen zügig beseitigt werden, bei Unfällen und gefährlichen Ereignissen unverzüglich Hilfe geleistet wird und insbesondere bei Brandfällen die Möglichkeit zur Selbst- oder Fremdrettung von Personen oder eine Kombination von beidem in Abhängigkeit von den lokalen Verhältnissen besteht.
- BOStrab §23 Absatz 3
  Bei Fahrbetrieb ohne Fahrzeugführer müssen nachrichtentechnische Anlagen vorhanden sein, die eine vorrangige Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle ermöglichen.
- BOStrab §43 Absatz 5 Punkt 3
  bei Fahrbetrieb ohne Fahrzeugführer sicherstellen, daß Züge nur bei geschlossenen Türen anfahren können
- BOStrab §43 Absatz 6
  Türen müssen in geschlossener Stellung festgehalten sein. Sie müssen jedoch von Fahrgästen im Notfall geöffnet werden können.
- BOStrab §46 Absatz 4
  Fahrzeuge müssen Einrichtungen für eine Sprechverbindung zwischen Fahrzeugführer und einer Betriebsstelle haben. Notfall-Informationen müssen vorrangig durchgegeben werden können.

- BOStrab §46 Absatz 5
  Personenfahrzeuge eines Zuges, die nicht mit Betriebsbediensteten besetzt sind, müssen ständig verfügbare Einrichtungen für eine Notfall-Sprechverbindung zwischen Fahrgästen und dem Fahrzeugführer haben.
  ➔ *Die Technische Aufsicht (TA) der AD-Leitstelle ist der Fahrzeugführer im autonomen Betrieb*.
- BOStrab §46 Absatz 6
  Bei Fahrbetrieb ohne Fahrzeugführer müssen Personenfahrzeuge Einrichtungen für eine Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle haben. Absatz 4 Satz 2 gilt entsprechend.
- BOStrab §52 Absatz 3
  Betriebsanlagen oder Fahrzeuge, die ganz oder teilweise selbsttätig arbeiten oder fernbedient werden, müssen im Rahmen der betrieblichen Erfordernisse von Betriebsbediensteten auf einwandfreie Funktion überwacht werden.
- BOStrab §54 Absatz 3
  Personenzüge dürfen nur so beschleunigt und nur so gebremst werden, daß Fahrgäste nicht mehr als unvermeidbar gefährdet werden.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.
- Die angemessene Sicherheit der Fahrgäste während der Fahrt obliegt zum großen Anteil den Systemen der autonomen Fahrt des Fahrzeugherstellers (OEM) oder dem Hersteller des AD-Tuning-Kits, welche im Gefahrenfall ein Minimum Risk Manoeuvre (MRM) umsetzen, weshalb der verbleibende Anteil der Störungsmeldung als informativ QM (C) betrachtet werden kann, **aber**
  ISO-26262-03:2018 Clause 7.4.3.1 Sicherheitsanforderungen müssen dem Automotive Safety Integrity Level (ASIL) der Funktion und dem zugehörigen Sicherheitsziel entsprechen.
  Hinweis Fahrt = ASIL-C.
  Dekomposition siehe Hinweis unter der zweiten „Begründung zur Wahl der Risikoparameter“.

Risikograph (Fahrt / erweiterte Abfahrkontrolle ≙ Probefahrt):

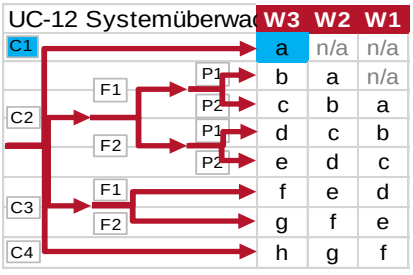


≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich

Risikograph (Ereigniseintrag):



≙ QM(C)

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzungen durch den gefährlichen Vorfall, weil als Gegenmaßnahme das Minimum Risk Manoeuvre (MRM) durch die Systeme des Fahrzeugherstellers (OEM) oder des AD-Tuning-Kits die Gefährdung der Fahrgäste limitiert.
✖	
✖	
W3	Eine relativ hohe Auftretenswahrscheinlichkeit und häufige unerwünschte Ereignisse sind wahrscheinlich.

Hinweis:
Eine Funktion / Signal mit einer Sicherheitsrelevanz von ASIL-D (D) kann durch Gegenmaßnahmen der Robustheit und Überwachung so abgesichert werden, daß der sichere Zustand durch eine automatisierte Gegensteuerung gewährleitet wird, d.h. eine drohende Signalunterschreitung des Minimalwertes wird durch Unterstützungsleistung vermieden, eine Signalübersteuerung des Maximalwertes wird durch Übersteuerungsschutz / Derating auf zulässige Werte begrenzt. Solange die Aufrechterhaltung des sicheren Bereiches gewährleistet wird, reicht zur Dokumentation ein Ereignisspeichereintrag, welcher, weil der Fahrer dieses nicht bemerkt, somit auch keinen Einfluß auf die Beherrschbarkeit haben kann, mit einer Sicherheitsrelevanz QM(D) zu bewerten ist. Sofern die automatisierten Gegenmaßnahmen eine ausreichende Minderung des Effektes zur Aufrechterhaltung der Beherrschbarkeit, aber keine vollständige Kompensation gewährleisten, ist eine Warnlampe Gelb anzuzeigen, welche mit ASIL-A (D) bewertet wird. Sobald die automatisierten Gegenmaßnahmen keine ausreichende Minderung des Effektes zur Aufrechterhaltung der Beherrschbarkeit mehr gewährleisten, ist die Warnlampe Rot mit mindestens der Sicherheitsrelevanz der Funktion / des Signales anzuwenden!
Aber technisch unterscheidet sich der Signalwert der Fehlerkennung nur durch den mathematischen Zahlenwert, z.B.
0 = keine Fehlermeldung an Fahrer, jedoch ist ein Ereignisspeichereintrag möglich
1 = Fehlermeldung Gelb an Fahrer bzw. 2 = Fehlermeldung Rot an Fahrer.
Da die Absicherung Gelb = ASIL-A (D) hinreichend ist, muß diese für Rot auch hinreichend sein, Dieses ist jedoch nicht erfüllend, d.h. zur Absicherung einer ASIL-D Funktion / Signal wird eine ASIL-C (D) Absicherung + ASIL-A (D) Absicherung (Warnlampe Gelb/Rot) + ASIL-QM (D) Absicherung (Ereignisspeichereintrag) angewendet. Die ASIL-C (D) Absicherung muß den Fahrer eindeutig und unmißverständlich dazu bringen sein Fahrzeug unverzüglich zum Stillstand zu bewegen, weshalb ein aufgeschaltetes Rütteln des Lenkrades, welches durch den ACC-Fahrspurassistenten oder die Müdigkeitserkennung bekannt und somit vom Fahrer beherrschbar, geeignet ist. Zur Erkennung, daß es unterschiedliche Signale sind, sollte ein abweichendes Rüttelmuster spezifiziert werden. Bei der autonomen Fahrt ist das Rüttelmuster durch eine priorisierte Warnmeldung an die Technische Aufsicht (TA) der AD-Leitstelle umzusetzen.

ISO-26262-03:2018 Clause 7.4.3.1 Sicherheitsanforderungen müssen dem Automotive Safety Integrity Level (ASIL) der Funktion entsprechen.

3.2.13 UC-13 Fahrtänderung

Aufgrund einer ungeplanten Störung sind Anpassungen einzelner Fahrten notwendig. Neben der Fahrtverschiebung, die eine rein zeitliche Anpassung des ursprünglichen Fahrplans verursacht, kommen Änderungen des Fahrwegs, die meist sowohl zeitliche als auch räumliche Korrekturen notwendig machen, am häufigsten vor. So dient eine Umleitung der Umfahrung einer durch z. B. einen Unfall verursachten Blockade oder Störung eines ursprünglich geplanten Streckenabschnitts. Teilweise existieren hierfür bereits vorgeplante Umleitungsrouten (z. B. aufgrund geplanter Bauarbeiten, Veranstaltungen oder häufiger vorkommender ungeplanter Störungen), die bei Bedarf aktiviert werden können. Ist kein geeigneter vorgeplanter Umleitungsfahrweg vorhanden, wird (manuell) eine andere Streckenführung auf Basis des bekannten Streckennetzes gewählt. In geeigneten Fällen kann eine Umleitung auch dazu verwendet werden, um Verspätungen aufzuholen (Abkürzung).

Wenn eine Wendestelle nicht befahrbar ist oder um eine außergewöhnlich hohe Fahrgastnachfrage zu bedienen, kann eine Fahrt über die geplante Wendestelle hinaus auf einen geplanten Streckenabschnitt verlängert werden. Diese Maßnahme bezeichnet man als Langwende. Eine Kurzwende hingegen läßt ein Fahrzeug vor Erreichen der planmäßigen Endhaltestelle wenden, um beispielsweise eine sehr große Verspätung aufzuholen und/oder einen gestörten Streckenast nicht zu befahren.

Hinweis:
Auf dem Betriebshof können eigenständig Fahrten und Fahrtänderungen für Service und Wartung durch das BHMS erstellt und angewendet werden. In diesem Fall tauschen ÖV-Leitstelle und das BHMS die Rollen, statt öffentliche Haltestellen werden jetzt interne Servicestationen auf dem BHMS angefahren.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Zuweisung der aktualisierten Fahrplandaten sowie Überwachung der Fahrplanumsetzung auf Einhaltung der Fahrplandaten inklusive Pünktlichkeit. Informieren der Fahrgäste über Abweichungen gegenüber dem Fahrplan inklusive Unterstützung bei der Sicherstellung des reibungslosen Reiseablaufes der Fahrgäste.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung).
BHMS	keine (im Regelbetrieb)	keine (im Regelbetrieb)
AD-Leitstelle	Konfiguration der Fahrbereitschaft zur Betriebsfortsetzung. Fahrzeugüberwachung	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Ein Umlauf ist eine Sequenz von Fahrten, vom Ausrücken aus dem Betriebshof bis zum Einrücken in den Betriebshof, d. h. die Menge von Fahrten, die von einem Fahrzeug an einem (Teil des) Betriebstag(s) durchgeführt werden. Die Identifikation erfolgt über den Betriebstag sowie eine Umlaufnummer.

Hinweis:
Die Umlaufnummer dient zur Identifikation des erwarteten „Fahrzeugs“, allerdings im organisatorischen Sinne, nicht im technischen Sinne eines konkreten Fahrzeugs. Wird eine Route von verschiedenen Fahrzeugen (unterschiedliche Fahrzeugnummern) befahren, entspricht diese der Fahrtroutennummer.

Hinweis:
Die Fahrt entspricht der Bewegung eines Fahrzeugs vom Startpunkt bis zum Endpunkt eines Fahrwegs und wird über den Umlauf bzw. Kurs und die Fahrtnummer identifiziert.

Hinweis:
Der Fahrweg ist eine für eine Fahrt genutzte Route. Diese ist definiert durch eine geordnete Folge geplanter Haltepunkte (bei Leerfahrten nur Start- und Zielpunkt) und ggf. Zwischenpunkte, die den Streckenverlauf eindeutig festlegen.

Hinweis:
Der Fahrauftrag definiert als Oberbegriff eine Vorgabe für die Bewegung eines Fahrzeugs. Die Quelle von Fahraufträgen kann vielfältig sein: Fahrplan, dispositive Maßnahme der Leitstelle, Betriebshof- und Werkstattmanagement etc. Entsprechend ist die Granularität eines Fahrauftrages sehr unterschiedlich, er kann von einer kurzen (Rangier-)Bewegung bis zu einer komplexen Folge von Einsetz- / Fahrplan- / Aussetz-Fahrten reichen.

Hinweis:
Die Mission beschreibt einen Teil einer Fahrt zwischen zwei Haltepunkten / Haltestellen und beinhaltet Angaben zu
- dem Fahrgastwechsel (möglich / nicht möglich, d.h. die Türen werden am Ziel geöffnet bzw. nicht geöffnet)
- der Zeitspanne des Haltens (für den potentiellen Fahrgastwechsel / für das Laden des Fahrzeuges / …)
- der Umlaufnummer inklusive Angaben zum vorgegebenen Fahrweg (Wegpunkte, Route) zum Zielpunkt gemäß Fahrwegplanung der ÖV-Leitstelle
plus optional
- den Informationen zur Haltebucht
- der geplanten Fahrzeit zur Umsetzung der Mission gemäß Fahrwegplanung der ÖV-Leitstelle.

Hinweis:
Fahrtänderungen für Service & Wartungsumläufe / -fahrten / -fahrwege / -fahraufträge / -missionen obliegen dem BHMS eigenständig.

Betriebsschutz:
Zugang zur ÖV-Leitstelle (Sicherheitszone) haben nur ausgebildete und (sicherheitstechnisch) geschulte Mitarbeiter, Fahrgäste haben keinen Zugang.

Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Fahrplan / Fahrrouten Aktualisierung (Regelbetrieb).

Aktionen:

- Der Disponent der ÖV-Leitstelle leitet dispositive Maßnahmen ein.
- Die ÖV-Leitstelle prüft ob die Maßnahmen ausführbar sind.
  - Extraktion der Sequenz von Fahrten mit den jeweiligen Start- und Endpunkten aus dem Umlauf
  - Extraktion der Fahrwege (Routen) der Fahrten → Wegpunkte des Umlaufes
  - Extraktion der Fahraufträge (Fahrgast- Leer-, Rangier- oder Fahrt im Depot) aus dem Umlauf
  - Extraktion der Mission(en) = Teilstück(e) zwischen zwei Haltepunkten / -stellen aus den Fahrten
  - Freigabe der Umlaufnummer und der aktuellen Fahrplandaten.
- Die ÖV-Leitstelle übermittelt (über 3) die aktuellen Fahrplandaten (Fahrten + Fahraufträge und die Missionen) des Umlaufes an die AD-Leitstelle, welche diese zum AD-Bordsystem (über 8) weiterleitet.
  - Das AD-Bordsystem prüft die Daten gegen die hochauflösende Karte und meldet im Problemfall eine Störmeldung (UC-13 → UC-12 Systemüberwachung und ggf. Störmeldung, über 8 plus 14 informativ)
- Die ÖV-Leitstelle übermittelt (über 7) die aktuellen Fahrplandaten (Fahrten + Fahraufträge und die Missionen) des Umlaufes an den ÖV-Bordrechner, welcher diese einließt und prüft, (z.B. ob alle notwendigen Durchsagen hinterlegt sind). Das Ergebnis der kumulativen Prüfung wird an die ÖV-Leitstelle rückgemeldet.

Juristische Anforderungen:

- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
  Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
  Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.1 Generelle Kollisionsvermeidung
  Kollisionen mit anderen Verkehrsteilnehmenden und unbeteiligten Dritten müssen vermieden werden, sofern dies durch
  1. Notbremseingriffe oder
  2. andere Teilnehmende des umgebenden Verkehrs, andere unbeteiligte Dritte oder die Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nicht gefährdende Ausweichmanöver möglich ist. Kann eine Kollision zur Abwendung einer Gefährdung des Lebens der Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nur durch eine Gefährdung des Lebens anderer Teilnehmender des umgebenden Verkehrs oder unbeteiligter Dritter vermieden werden (unvermeidbare alternative Gefährdung von Menschenleben), darf der Schutz der anderen Teilnehmenden des umgebenden Verkehrs und der unbeteiligten Dritten nicht nachrangig gegenüber dem Schutz der Insassen des autonom fahrenden Kraftfahrzeugs erfolgen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.2 Interaktion mit anderen Verkehrsteilnehmenden
  a) Vorausfahrende Verkehrsteilnehmende auf der Fahrbahn werden erkannt. Es wird jederzeit in jedem Geschwindigkeitsbereich und in jeder möglichen Fahrsituation ein angemessener Sicherheitsabstand eingehalten. Der einzuhaltende Sicherheitsabstand bestimmt sich nach § 4 der Straßenverkehrs-Ordnung.

b) Der Fahrstreifenwechsel vorausfahrender oder nachfolgender Fahrzeuge, der von einem benachbarten Fahrstreifen in den eigenen Fahrstreifen oder aus dem eigenen Fahrstreifen heraus in einen benachbarten Fahrstreifen erfolgt, wird erkannt und bei der Fahraufgabe entsprechend berücksichtigt.
c) Situationen, welche einen Fahrstreifenwechsel bedingen (beispielsweise anhaltende oder langsame Fahrzeuge auf der Fahrbahn, Ende eines Fahrstreifens), werden erkannt und geeignete Manöver zum Fahrstreifenwechsel werden sicher durchgeführt.
d) Einsatzfahrzeuge werden erkannt und geeignete Fahrmanöver sicher durchgeführt.

- AFGBV Anlage 1 Teil 1 Abschnitt 1.3 Planung der Fahrpfade und Geschwindigkeiten
  Bei Geschwindigkeitsanpassungen kommt es zu keiner vermeidbaren Beeinträchtigung von Insassen, anderen Verkehrsteilnehmenden und unbeteiligten Dritten. Es gelten folgende Anforderungen:
  a) Geschwindigkeitsbeschränkungen und Änderungen der Geschwindigkeitsbeschränkung werden erkannt und die Geschwindigkeit wird entsprechend angepaßt.
  b) Besondere Anforderungen an die Geschwindigkeit werden erkannt und im Geschwindigkeits- und Fahrtverlauf befolgt (beispielsweise in Bereichen vor Schulen und an Arbeitsstellen an Straßen, an Bushaltestellen, Bahnübergängen, in engen Kurvenradien oder bei Gefällen, in Engstellen, in denen der eigene Fahrstreifen vom Gegenverkehr mitbenutzt werden muß).
  c) Zeichen und Weisungen der Polizeibeamten gemäß § 36 der Straßenverkehrs-Ordnung, Wechsellichtzeichen gemäß § 37 der Straßenverkehrs-Ordnung, sonstige Zeichen gemäß der §§ 39 bis 42 der Straßenverkehrs-Ordnung sowie Verkehrseinrichtungen gemäß § 43 der Straßenverkehrs-Ordnung werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  d) Situationen, in denen die Vorfahrt anderen gewährt werden muß (beispielsweise vor Fußgängerüberwegen, in Kreuzungsbereichen oder Einmündungen), werden erkannt und ohne Gefährdung oder Behinderung der Vorfahrtberechtigten bewältigt. Es ist eine berechnete Zeit bis zum Aufprall von mehr als drei Sekunden bezüglich des Vorfahrtberechtigen einzuhalten. Wird von diesen Werten abgewichen, muß dies ausreichend begründet und auf Basis von systematischen Sicherheitsbewertungen nach dem Stand der Technik dokumentiert werden. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO 26262:2018-12 Straßenfahrzeuge – Funktionale Sicherheit erfüllt werden.
  e) Bauliche Straßengestaltungen mit Auswirkung auf das Verhaltensrecht (beispielsweise bis zu 5 Meter vom Fahrbahnrand einer vorfahrtberechtigten Straße abgesetzte Radwege nach § 9 Absatz 3 der Straßenverkehrs-Ordnung oder abgesenkte Bordsteine nach § 10 der Straßenverkehrs-Ordnung) werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  f) Arbeitsstellen an Straßen, temporär veränderte Fahrbahnverläufe oder Fahrbahnmarkierungen werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  g) Defizite am Zubehör, insbesondere der Verkehrseinrichtungen (zum Beispiel verschlissene, beschädigte, fehlende oder defekte temporäre oder dauerhafte Fahrbahnmarkierungen und Verkehrszeichen, Phantommarkierungen) und der Straßenausstattung, insbesondere solcher nach vorstehenden Buchstaben a bis f werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Dies gilt insbesondere nach Sturm- und sonstigen Witterungsereignissen.
- AFGBV Anlage 1 Teil 1 Abschnitt 6 Übertragung von Daten an das Kraftfahrzeug
  Die zur selbstständigen Bewältigung der Fahraufgabe im autonomen Betrieb notwendigen Daten und Informationen von externen technischen Einheiten (beispielsweise Backends oder Server eines Anbieters, externe Sensoren, Smartphone) müssen vom Kraftfahrzeug sicher empfangen und verwendet werden können. Daten externer Einheiten können im Kraftfahrzeug zur Ausführung der autonomen Fahrfunktionen verwendet werden. Daten und Informationen können beispielsweise bei bestimmten Anwendungsfällen über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) von einer externen technischen Einheit an das Kraftfahrzeug und vom Kraftfahrzeug an eine technische Einheit übertragen werden. Die Übertragung solcher Daten muß insbesondere den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und nach dem aktuellen Stand der Technik abgesichert sein. Das Absicherungskonzept muß die in einer Bedrohungsanalyse identifizierten Risiken mit wirksamen Maßnahmen adressieren und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten. Zur Datenübertragung sollte eine zentrale sichere elektronische Steuereinheit (SECU) genutzt werden. Die SECU dient als Informationsgateway im Kraftfahrzeug. Die SECU kommuniziert intern an die Kommunikationsbusse des Kraftfahrzeugs und an den physischen On-Board-Diagnose II-Anschluß (OBD II) oder an eine proprietäre Schnittstelle eines Herstellers. Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung sind Teil 5 zu entnehmen. Die Integrität, Authentizität und Verfügbarkeit der Datenübertragung sind sicherzustellen. Die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen oder mit Infrastrukturkomponenten ist zulässig. Sie muß auf der Basis einer Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 insbesondere den Anforderungen an die Informationstechnik nach Teil 5 und damit den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen. Während des Betriebs in einer optionalen Testphase ist die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen und Infrastrukturkomponenten zu testen und gegebenenfalls anzupassen.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert.
  Hinweis:
  Dieses ist gültig für die Planung der Fahrzeugbewegung, die Routenführung über die Wegpunkte / Stützstellen des Umlaufs → Sequenz der Fahrten → Fahrwege → Fahraufträge → Missionen.
- Anders als ursprünglich geplant soll das autonom fahrende Fahrzeug, während der Fahrgastwechselzeit, jetzt aufgrund einer Fahrtänderung unmittelbar (ad hoc) die Routenführung (Wegpunkte) ändern, wodurch sich die Fahrplanzeiten verändern. Dadurch kann ein geplanter Zeitpunkt des Haltens zu einem Zeitpunkt des Fahrens werden, welches eine abrupte Türschließung ohne Vorwarnung auslöst.
- Anders als ursprünglich geplant soll das autonom fahrende Fahrzeug, jetzt aufgrund einer Fahrtänderung unmittelbar (ad hoc) abbiegen statt dem Straßenverlauf gerade aus zu folgen. Die momentan gefahrene Geschwindigkeit ist zu hoch für die durch den Straßenverlauf vorgegebene Kurvenführung, d.h. die auftretende Seitenführungskraft (im Zusammenhang mit der Längsführungskraft) kann das Rad des Fahrzeuges, insbesondere Aufgrund von sich ggf. negativ dazu addierenden Wetterbedingungen (Nässe), nicht auf die Straße übertragen (Kammscher Kreis, siehe Abbildung 6 Kammscher Kreis). Die Fahrerassistenzsysteme des Fahrzeugherstellers (OEM), welche das Autonomous Driving System (ADS) des Fahrzeugherstellers (OEM) unterstützen, können aufgrund der Kurzfristigkeit (ad hoc abbiegen) dieses nicht kompensieren, insbesondere weil die Eingriffsmöglichkeit der Technischen Aufsicht (TA) über das AD-Bordsystem (ADBS) die Fahrzeugfunktion des (OEM) im Eingriffsfall übersteuern können muß. Die Reaktionsfähigkeit der Technischen Aufsicht (TA) der AD-Leitstelle, welche über die Fahrplanänderung informiert wird, kann dieses nicht abfangen, weil nicht vorhersehbar ist, wann exakt das AD-Bordsystem dieses im Fahrzeug umsetzt.
  Hinweis:
  Im konventionellen Betrieb des Individualverkehrs kann das Navigationssystem schnell neue Strecken berechnen, aber der Fahrer entscheidet (kontrolliert) wann das Manöver umgesetzt wird. In der autonomen Fahrt wird dieses vom AD-Bordsystem selbständig umgesetzt, weshalb der exakte Zeitpunkt der Umsetzung der Änderung der Fahrtroute nicht für die Technische Aufsicht (TA) der AD-Leitstelle vorhersehbar ist, wodurch ein ggf. notwendiger menschlicher Eingriff zum Abfangen / Übersteuern der autonomen Aktion nicht gewährleistet ist. Folglich sind Fahrtroutenänderungen so abzusichern, daß nach dem Passieren des Point of Safe Return (PSR), keine abrupte, unbeherrschbare Routenänderung umgesetzt wird, wobei insbesondere die Systemgrenzen (Kammscher Kreis, Elchtest) nicht überschritten werden dürfen. Andernfalls würde die autonome Fahrt, durch die unkontrollierbare Fahrtänderung zu einem nicht geeigneten Zeitpunkt, zu einer unkontrollierbaren Situation → ISO-26262-Band 3: 2018 – Tabelle 3: „C3 Difficult to control or uncontrollable“, was zu einer ASIL-D Bewertung führt.
  Hinweis:
  Bei der Verifikation der implementierten, automatisierten Schutzmaßnahmen auf dem Testgelände (Kreiselfläche) sind, zum Schutz der Sicherheitsfahrer, Geschwindigkeitsbegrenzungen als Sicherheitsauflage (Maßnahme) anzuordnen, welche langsam Schrittweise über den Testablauf erhöht werden können um die Systemgrenze der implementierten Sicherheit iterativ zu ermitteln.

Kammscher Kreis:

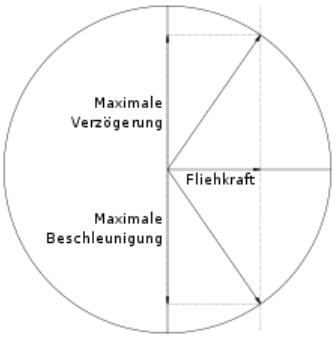
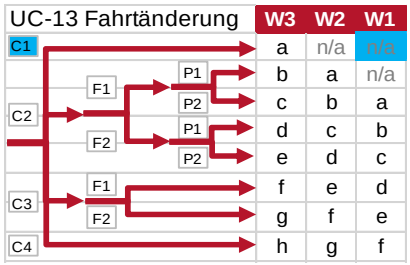


Abbildung 6 Kammscher Kreis

Bild Wikipedia, https://de.wikipedia.org/wiki/Kammscher_Kreis

Risikograph (Planung Fahrzeugbewegung):

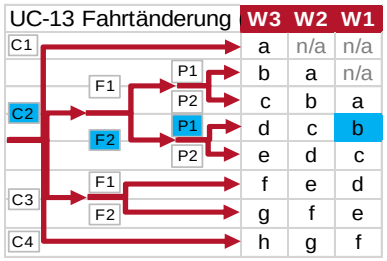


≙ QM(D)

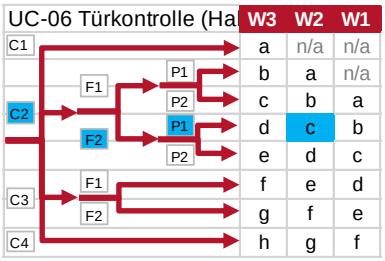
Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzungen durch den gefährlichen Vorfall. (Akzeptiertes Standardrisiko bei Bürotätigkeiten)
✖	
✖	
W1	Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich.

Risikograph (Fahrtänderung der Wegpunkte im Stillstand, v=0km/h):



≙ ASIL-A(D) ←

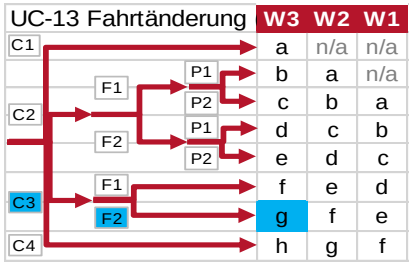


≙ ASIL-A(D)

Begründung zur Wahl der Risikoparameter:
VDV-Schrift-161-2 Kap. 3.4.1: Verhinderung der Anfahrt mit geöffneten Türen

C2	Die Betriebserfahrungen haben gezeigt, daß im Versagensfalle nur eine Person betroffen ist
F2	Fahrgäste halten sich im Regelfall häufig in der Nähe der Türen auf
P1	Gefahrenabwehr ist möglich unter der Bedingung, daß der Fahrgast nicht das Fahrzeug verläßt bzw. ein Sturz vermieden werden kann.
W1	Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich. *Hinweis:* *Bewertung ist Abweichend zu VDV-Originaleinstufung, weil hier die Fahrtänderung zu diesem Zeitpunkt kumulativ hinzukommen müßte, welches die Wahrscheinlichkeit reduziert.* *VDV-Originaleinstufung:* *W2 Aufgrund des Einwirkens verschiedenster Bedingungen bis zur unbeabsichtigten Anfahrt wird die Eintrittswahrscheinlichkeit als gering eingestuft.*

Risikograph (Fahrtänderung der Wegpunkte während der Fahrt):



≙ ASIL-D

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen durch den gefährlichen Vorfall
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich
✖	
W3	Eine relativ hohe Auftretenswahrscheinlichkeit und häufige unerwünschte Ereignisse sind wahrscheinlich.

3.2.14 UC-14 Umlaufänderung

Sind aufgrund von Störungen Maßnahmen erforderlich, die über die Anpassung einzelner Fahrten hinausgehen, sind Veränderungen eines oder mehrerer Umläufe notwendig.

Dabei können einzelne Fahrten ausfallen, wenn z. B. ganze Streckenabschnitte unpassierbar sind oder Fahrpersonal oder Fahrzeuge fehlen. Je nach betrieblicher Situation kann es auch zu Teilausfällen kommen, z.B. wenn eine Fahrt während ihres Verlaufs unterbrochen werden muss.

Fahrten können auch eingefügt werden, verursacht durch beispielsweise ein außergewöhnlich hohes Fahrgastaufkommen. Die zusätzliche Fahrt wird in einem passenden bestehenden Umlauf, etwa während einer längeren Pause oder am Ende des planmäßigen Umlaufs, hinzugefügt.

Hinweis:
Auf dem Betriebshof können eigenständig Umläufe und Umlaufänderungen für Service und Wartung durch das BHMS erstellt und angewendet werden. In diesem Fall tauschen ÖV-Leitstelle und das BHMS die Rollen, statt öffentliche Haltestellen werden jetzt interne Servicestationen auf dem BHMS angefahren.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Zuweisung der aktualisierten Fahrplandaten sowie Überwachung der Fahrplanumsetzung auf Einhaltung der Fahrplandaten inklusive Pünktlichkeit. Informieren der Fahrgäste über Abweichungen gegenüber dem Fahrplan inklusive Unterstützung bei der Sicherstellung des reibungslosen Reiseablaufes der Fahrgäste.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung).
BHMS	keine (im Regelbetrieb)	keine (im Regelbetrieb)
AD-Leitstelle	Konfiguration der Fahrbereitschaft zur Betriebsfortsetzung. Fahrzeugüberwachung	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Ein Umlauf ist eine Sequenz von Fahrten, vom Ausrücken aus dem Betriebshof bis zum Einrücken in den Betriebshof, d. h. die Menge von Fahrten, die von einem Fahrzeug an einem (Teil des) Betriebstag(s) durchgeführt werden. Die Identifikation erfolgt über den Betriebstag sowie eine Umlaufnummer.

Hinweis:
Die Umlaufnummer dient zur Identifikation des erwarteten „Fahrzeugs“, allerdings im organisatorischen Sinne, nicht im technischen Sinne eines konkreten Fahrzeugs. Wird eine Route von verschiedenen Fahrzeugen (unterschiedliche Fahrzeugnummern) befahren, entspricht diese der Fahrtroutennummer.

Hinweis:
Die Fahrt entspricht der Bewegung eines Fahrzeugs vom Startpunkt bis zum Endpunkt eines Fahrwegs und wird über den Umlauf bzw. Kurs und die Fahrtnummer identifiziert.

Hinweis:
Der Fahrweg ist eine für eine Fahrt genutzte Route. Diese ist definiert durch eine geordnete Folge geplanter Haltepunkte (bei Leerfahrten nur Start- und Zielpunkt) und ggf. Zwischenpunkte, die den Streckenverlauf eindeutig festlegen.

Hinweis:
Der Fahrauftrag definiert als Oberbegriff eine Vorgabe für die Bewegung eines Fahrzeugs. Die Quelle von Fahraufträgen kann vielfältig sein: Fahrplan, dispositive Maßnahme der Leitstelle, Betriebshof- und Werkstattmanagement etc. Entsprechend ist die Granularität eines Fahrauftrages sehr unterschiedlich, er kann von einer kurzen (Rangier-)Bewegung bis zu einer komplexen Folge von Einsetz- / Fahrplan- / Aussetz-Fahrten reichen.

Hinweis:
Die Mission beschreibt einen Teil einer Fahrt zwischen zwei Haltepunkten / Haltestellen und beinhaltet Angaben zu
- dem Fahrgastwechsel (möglich / nicht möglich, d.h. die Türen werden am Ziel geöffnet bzw. nicht geöffnet)
- der Zeitspanne des Haltens (für den potentiellen Fahrgastwechsel / für das Laden des Fahrzeuges / …)
- der Umlaufnummer inklusive Angaben zum vorgegebenen Fahrweg (Wegpunkte, Route) zum Zielpunkt gemäß Fahrwegplanung der ÖV-Leitstelle
plus optional
- den Informationen zur Haltebucht
- der geplanten Fahrzeit zur Umsetzung der Mission gemäß Fahrwegplanung der ÖV-Leitstelle.

Hinweis:
Fahrtänderungen für Service & Wartungsumläufe / -fahrten / -fahrwege / -fahraufträge / -missionen obliegen dem BHMS eigenständig.

Betriebsschutz:
Zugang zur ÖV-Leitstelle (Sicherheitszone) haben nur ausgebildete und (sicherheitstechnisch) geschulte Mitarbeiter, Fahrgäste haben keinen Zugang.

Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Fahrplan / Fahrrouten Aktualisierung (Regelbetrieb).

Aktionen:

- Der Disponent der ÖV-Leitstelle leitet dispositive Maßnahmen ein.
- Die ÖV-Leitstelle prüft ob die Maßnahmen ausführbar sind.
  - Anmeldung des Umlaufes mit Umlaufnummer des Fahrzeuges
  - Extraktion der Sequenz von Fahrten mit den jeweiligen Start- und Endpunkten aus dem Umlauf
  - Extraktion der Fahrwege (Routen) der Fahrten → Wegpunkte des Umlaufes
  - Extraktion der Fahraufträge (Fahrgast- Leer-, Rangier- oder Fahrt im Depot) aus dem Umlauf
  - Extraktion der Mission(en) = Teilstück(e) zwischen zwei Haltepunkten / -stellen aus den Fahrten
  - Freigabe der Umlaufnummer und der aktuellen Fahrplandaten.
- Die ÖV-Leitstelle übermittelt (über 3) die aktuellen Fahrplandaten (Fahrten + Fahraufträge und die Missionen) des Umlaufes an die AD-Leitstelle, welche diese zum AD-Bordsystem (über 8) weiterleitet.
  - Das AD-Bordsystem prüft die Daten gegen die hochauflösende Karte und meldet im Problemfall eine Störmeldung (UC-14 → UC-12 Systemüberwachung und ggf. Störmeldung)
- Die ÖV-Leitstelle übermittelt (über 7) die aktuellen Fahrplandaten (Fahrten + Fahraufträge und die Missionen) des Umlaufes an den ÖV-Bordrechner, welcher diese einließt und prüft, (z.B. ob alle notwendigen Durchsagen hinterlegt sind). Das Ergebnis der Prüfung wird an die ÖV-Leitstelle rückgemeldet.

Juristische Anforderungen:

- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
  Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
  Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.1 Generelle Kollisionsvermeidung
  Kollisionen mit anderen Verkehrsteilnehmenden und unbeteiligten Dritten müssen vermieden werden, sofern dies durch
  1. Notbremseingriffe oder
  2. andere Teilnehmende des umgebenden Verkehrs, andere unbeteiligte Dritte oder die Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nicht gefährdende Ausweichmanöver möglich ist. Kann eine Kollision zur Abwendung einer Gefährdung des Lebens der Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nur durch eine Gefährdung des Lebens anderer Teilnehmender des umgebenden Verkehrs oder unbeteiligter Dritter vermieden werden (unvermeidbare alternative Gefährdung von Menschenleben), darf der Schutz der anderen Teilnehmenden des umgebenden Verkehrs und der unbeteiligten Dritten nicht nachrangig gegenüber dem Schutz der Insassen des autonom fahrenden Kraftfahrzeugs erfolgen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.2 Interaktion mit anderen Verkehrsteilnehmenden
  a) Vorausfahrende Verkehrsteilnehmende auf der Fahrbahn werden erkannt. Es wird jederzeit in jedem Geschwindigkeitsbereich und in jeder möglichen Fahrsituation ein angemessener Sicherheitsabstand eingehalten. Der einzuhaltende Sicherheitsabstand bestimmt sich nach § 4 der Straßenverkehrs-Ordnung.
  b) Der Fahrstreifenwechsel vorausfahrender oder nachfolgender Fahrzeuge, der von einem benachbarten Fahrstreifen in den eigenen Fahrstreifen oder aus dem eigenen Fahrstreifen heraus in einen benachbarten Fahrstreifen erfolgt, wird erkannt und bei der Fahraufgabe entsprechend berücksichtigt.

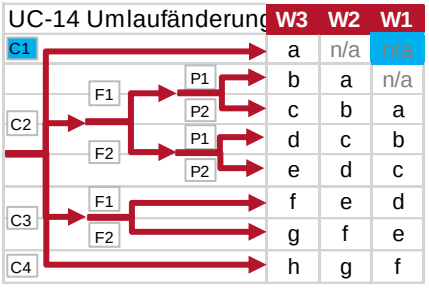
c) Situationen, welche einen Fahrstreifenwechsel bedingen (beispielsweise anhaltende oder langsame Fahrzeuge auf der Fahrbahn, Ende eines Fahrstreifens), werden erkannt und geeignete Manöver zum Fahrstreifenwechsel werden sicher durchgeführt.
d) Einsatzfahrzeuge werden erkannt und geeignete Fahrmanöver sicher durchgeführt.

- AFGBV Anlage 1 Teil 1 Abschnitt 1.3 Planung der Fahrpfade und Geschwindigkeiten
  Bei Geschwindigkeitsanpassungen kommt es zu keiner vermeidbaren Beeinträchtigung von Insassen, anderen Verkehrsteilnehmenden und unbeteiligten Dritten. Es gelten folgende Anforderungen:
  a) Geschwindigkeitsbeschränkungen und Änderungen der Geschwindigkeitsbeschränkung werden erkannt und die Geschwindigkeit wird entsprechend angepaßt.
  b) Besondere Anforderungen an die Geschwindigkeit werden erkannt und im Geschwindigkeits- und Fahrtverlauf befolgt (beispielsweise in Bereichen vor Schulen und an Arbeitsstellen an Straßen, an Bushaltestellen, Bahnübergängen, in engen Kurvenradien oder bei Gefällen, in Engstellen, in denen der eigene Fahrstreifen vom Gegenverkehr mitbenutzt werden muß).
  c) Zeichen und Weisungen der Polizeibeamten gemäß § 36 der Straßenverkehrs-Ordnung, Wechsellichtzeichen gemäß § 37 der Straßenverkehrs-Ordnung, sonstige Zeichen gemäß der §§ 39 bis 42 der Straßenverkehrs-Ordnung sowie Verkehrseinrichtungen gemäß § 43 der Straßenverkehrs-Ordnung werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  d) Situationen, in denen die Vorfahrt anderen gewährt werden muß (beispielsweise vor Fußgängerüberwegen, in Kreuzungsbereichen oder Einmündungen), werden erkannt und ohne Gefährdung oder Behinderung der Vorfahrtberechtigten bewältigt. Es ist eine berechnete Zeit bis zum Aufprall von mehr als drei Sekunden bezüglich des Vorfahrtberechtigen einzuhalten. Wird von diesen Werten abgewichen, muß dies ausreichend begründet und auf Basis von systematischen Sicherheitsbewertungen nach dem Stand der Technik dokumentiert werden. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO 26262:2018-12 Straßenfahrzeuge – Funktionale Sicherheit erfüllt werden.
  e) Bauliche Straßengestaltungen mit Auswirkung auf das Verhaltensrecht (beispielsweise bis zu 5 Meter vom Fahrbahnrand einer vorfahrtberechtigten Straße abgesetzte Radwege nach § 9 Absatz 3 der Straßenverkehrs-Ordnung oder abgesenkte Bordsteine nach § 10 der Straßenverkehrs-Ordnung) werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  f) Arbeitsstellen an Straßen, temporär veränderte Fahrbahnverläufe oder Fahrbahnmarkierungen werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  g) Defizite am Zubehör, insbesondere der Verkehrseinrichtungen (zum Beispiel verschlissene, beschädigte, fehlende oder defekte temporäre oder dauerhafte Fahrbahnmarkierungen und Verkehrszeichen, Phantommarkierungen) und der Straßenausstattung, insbesondere solcher nach vorstehenden Buchstaben a bis f werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Dies gilt insbesondere nach Sturm- und sonstigen Witterungsereignissen.
- AFGBV Anlage 1 Teil 1 Abschnitt 6 Übertragung von Daten an das Kraftfahrzeug
  Die zur selbstständigen Bewältigung der Fahraufgabe im autonomen Betrieb notwendigen Daten und Informationen von externen technischen Einheiten (beispielsweise Backends oder Server eines Anbieters, externe Sensoren, Smartphone) müssen vom Kraftfahrzeug sicher empfangen und verwendet werden können. Daten externer Einheiten können im Kraftfahrzeug zur Ausführung der autonomen Fahrfunktionen verwendet werden. Daten und Informationen können beispielsweise bei bestimmten Anwendungsfällen über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) von einer externen technischen Einheit an das Kraftfahrzeug und vom Kraftfahrzeug an eine technische Einheit übertragen werden. Die Übertragung solcher Daten muß insbesondere den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und nach dem aktuellen Stand der Technik abgesichert sein. Das Absicherungskonzept muß die in einer Bedrohungsanalyse identifizierten Risiken mit wirksamen Maßnahmen adressieren und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten. Zur Datenübertragung sollte eine zentrale sichere elektronische Steuereinheit (SECU) genutzt werden. Die SECU dient als Informationsgateway im Kraftfahrzeug. Die SECU kommuniziert intern an die Kommunikationsbusse des Kraftfahrzeugs und an den physischen On-Board-Diagnose II-Anschluß (OBD II) oder an eine proprietäre Schnittstelle eines Herstellers. Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung sind Teil 5 zu entnehmen. Die Integrität, Authentizität und Verfügbarkeit der Datenübertragung sind sicherzustellen. Die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen oder mit Infrastrukturkomponenten ist zulässig. Sie muß auf der Basis einer Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 insbesondere den Anforderungen an die Informationstechnik nach Teil 5 und damit den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen. Während des Betriebs in einer optionalen Testphase ist die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen und Infrastrukturkomponenten zu testen und gegebenenfalls anzupassen.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert.
  Hinweis:
  Dieses ist gültig für die Planung der Fahrzeugbewegung, der Routenführung über die Wegpunkte / Stützstellen des Umlaufs → Sequenz der Fahrten → Fahrwege → Fahraufträge → Missionen.
- Anders als ursprünglich geplant soll das autonom fahrende Fahrzeug, während der Fahrgastwechselzeit, jetzt aufgrund einer Fahrtänderung unmittelbar (ad hoc) die Routenführung (Wegpunkte) ändern, wodurch sich die Fahrplanzeiten verändern. Dadurch kann ein geplanter Zeitpunkt des Haltens zu einem Zeitpunkt des Fahrens werden, welches eine abrupte Türschließung ohne Vorwarnung auslöst.
- Anders als ursprünglich geplant soll das autonom fahrende Fahrzeug, jetzt aufgrund einer Umlaufänderung, welche eine Fahrtänderung verursacht, unmittelbar (ad hoc) abbiegen statt dem Straßenverlauf geradeaus zu folgen. Die momentan gefahrene Geschwindigkeit ist zu hoch für die durch den Straßenverlauf vorgegebene Kurvenführung, d.h. die auftretende Seitenführungskraft (im Zusammenhang mit der Längsführungskraft) kann das Rad des Fahrzeuges, insbesondere Aufgrund von sich ggf. negativ dazu addierenden Wetterbedingungen (Nässe), nicht auf die Straße übertragen (Kammscher Kreis). Die Fahrerassistenzsysteme des Fahrzeugherstellers (OEM), welche das Autonomous Driving System (ADS) des Fahrzeugherstellers (OEM) unterstützen, können aufgrund der Kurzfristigkeit (ad hoc abbiegen) dieses nicht kompensieren, insbesondere weil die Eingriffsmöglichkeit der Technischen Aufsicht (TA) über das AD-Bordsystem (ADBS) die Fahrzeugfunktion des (OEM) im Eingriffsfall übersteuern können muß. Die Reaktionsfähigkeit der Technischen Aufsicht (TA) der AD-Leitstelle, welche über die Fahrplanänderung informiert wird, kann dieses nicht abfangen, weil nicht vorhersehbar ist, wann exakt das AD-Bordsystem dieses im Fahrzeug umsetzt.
  Hinweis:
  Im konventionellen Betrieb des Individualverkehrs kann das Navigationssystem schnell neue Strecken berechnen, aber der Fahrer entscheidet (kontrolliert) wann das Manöver umgesetzt wird. In der autonomen Fahrt wird dieses vom AD-Bordsystem selbständig umgesetzt, weshalb der exakte Zeitpunkt der Umsetzung der Änderung der Fahrtroute nicht für die Technische Aufsicht (TA) der AD-Leitstelle vorhersehbar ist, wodurch ein ggf. notwendiger menschlicher Eingriff zum Abfangen / Übersteuern der autonomen Aktion nicht gewährleistet ist. Folglich sind Fahrtroutenänderungen so abzusichern, daß nach dem Passieren des Point of Safe Return (PSR), keine abrupte, unbeherrschbare Routenänderung umgesetzt wird, wobei insbesondere die Systemgrenzen (Kammscher Kreis, Elchtest) nicht überschritten werden dürfen. Andernfalls würde die autonome Fahrt, durch die unkontrollierbare Fahrtänderung zu einem nicht geeigneten Zeitpunkt, zu einer unkontrollierbaren Situation → ISO-26262-Band 3: 2018 – Tabelle 3: „C3 Difficult to control or uncontrollable“, was zu einer ASIL-D Bewertung führt.
  Hinweis:
  Bei der Verifikation der implementierten, automatisierten Schutzmaßnahmen auf dem Testgelände (Kreiselfläche) sind, zum Schutz der Sicherheitsfahrer, Geschwindigkeitsbegrenzungen als Sicherheitsauflage (Maßnahme) anzuordnen, welche langsam Schrittweise über den Testablauf erhöht werden können um die Systemgrenze der implementierten Sicherheit iterativ zu ermitteln.

Risikograph (Planung Fahrzeugbewegung):

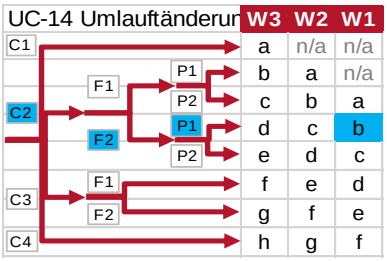


≙ QM(D)

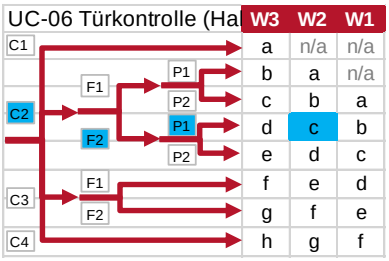
Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzungen durch den gefährlichen Vorfall. (Akzeptiertes Standardrisiko bei Bürotätigkeiten)
✖	
✖	
W1	Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich.

Risikograph (Umlaufänderung verursacht Änderung der Wegpunkte im Stillstand, v=0km/h):



≙ ASIL-A(D) ←

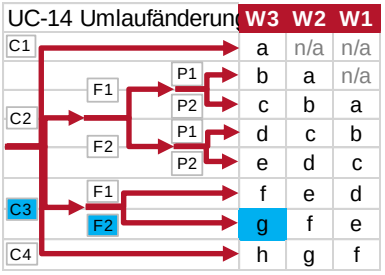


← ASIL-A(D)

Begründung zur Wahl der Risikoparameter:
VDV-Schrift-161-2 Kap. 3.4.1: Verhinderung der Anfahrt mit geöffneten Türen

C2	Die Betriebserfahrungen haben gezeigt, daß im Versagensfalle nur eine Person betroffen ist
F2	Fahrgäste halten sich im Regelfall häufig in der Nähe der Türen auf
P1	Gefahrenabwehr ist möglich unter der Bedingung, daß der Fahrgast nicht das Fahrzeug verläßt bzw. ein Sturz vermieden werden kann.
W1	Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich. *Hinweis:* *Bewertung ist Abweichend zu VDV-Originaleinstufung, weil hier die Missionsänderung und damit der Wegpunkte zu diesem Zeitpunkt kumulativ hinzukommen müßte, welches die Wahrscheinlichkeit reduziert.* *VDV-Originaleinstufung:* *W2 Aufgrund des Einwirkens verschiedenster Bedingungen bis zur unbeabsichtigten Anfahrt wird die Eintrittswahrscheinlichkeit als gering eingestuft.*

Risikograph (Umlaufänderung und damit der Wegpunkte während der Fahrt):



≙ ASIL-D

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen durch den gefährlichen Vorfall
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich
✖	
W3	Eine relativ hohe Auftretenswahrscheinlichkeit und häufige unerwünschte Ereignisse sind wahrscheinlich.

3.2.15 UC-15 Neuen Umlauf hinzufügen

Reicht eine zusätzliche Fahrt als Reaktion auf eine erhöhte Fahrgastnachfrage oder störungsbedingt verlängerte Fahrzeiten auf einer Linie nicht aus, kann ein zusätzliches Fahrzeug auf einem neuen Umlauf (oft Verstärkerumlauf genannt) eingesetzt werden. Dazu wird ein neuer Umlauf erzeugt, auf dem sich weiteres Fahrpersonal anmeldet.

Hinweis:
Auf dem Betriebshof können eigenständig Umläufe für Service und Wartung durch das BHMS erstellt und angewendet werden. In diesem Fall übernimmt das BHMS die Rolle des Disponenten, welcher das Anfahren von internen Servicestationen (statt öffentlichen Haltestellen) auf dem BHMS organisiert. Somit wird aus dem Informieren der Fahrgäste, die Information an das Personal der Arbeitsstation.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Zuweisung der aktualisierten Fahrplandaten sowie Überwachung der Fahrplanumsetzung auf Einhaltung der Fahrplandaten inklusive Pünktlichkeit. Informieren der Fahrgäste über Abweichungen gegenüber dem Fahrplan inklusive Unterstützung bei der Sicherstellung des reibungslosen Reiseablaufes der Fahrgäste.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung).
BHMS	keine (im Regelbetrieb)	keine (im Regelbetrieb)
AD-Leitstelle	Konfiguration der Fahrbereitschaft zur Betriebsfortsetzung. Fahrzeugüberwachung	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Ein Umlauf ist eine Sequenz von Fahrten, vom Ausrücken aus dem Betriebshof bis zum Einrücken in den Betriebshof, d. h. die Menge von Fahrten, die von einem Fahrzeug an einem (Teil des) Betriebstag(s) durchgeführt werden. Die Identifikation erfolgt über den Betriebstag sowie eine Umlaufnummer.

Hinweis:
Die Umlaufnummer dient zur Identifikation des erwarteten „Fahrzeugs“, allerdings im organisatorischen Sinne, nicht im technischen Sinne eines konkreten Fahrzeugs. Wird eine Route von verschiedenen Fahrzeugen (unterschiedliche Fahrzeugnummern) befahren, entspricht diese der Fahrtroutennummer.

Hinweis:
Die Fahrt entspricht der Bewegung eines Fahrzeugs vom Startpunkt bis zum Endpunkt eines Fahrwegs und wird über den Umlauf bzw. Kurs und die Fahrtnummer identifiziert.

Hinweis:
Der Fahrweg ist eine für eine Fahrt genutzte Route. Diese ist definiert durch eine geordnete Folge geplanter Haltepunkte (bei Leerfahrten nur Start- und Zielpunkt) und ggf. Zwischenpunkte, die den Streckenverlauf eindeutig festlegen.

Hinweis:
Der Fahrauftrag definiert als Oberbegriff eine Vorgabe für die Bewegung eines Fahrzeugs. Die Quelle von Fahraufträgen kann vielfältig sein: Fahrplan, dispositive Maßnahme der Leitstelle, Betriebshof- und Werkstattmanagement etc. Entsprechend ist die Granularität eines Fahrauftrages sehr unterschiedlich, er kann von einer kurzen (Rangier-)Bewegung bis zu einer komplexen Folge von Einsetz- / Fahrplan- / Aussetz-Fahrten reichen.

Hinweis:
Die Mission beschreibt einen Teil einer Fahrt zwischen zwei Haltepunkten / Haltestellen und beinhaltet Angaben zu
- dem Fahrgastwechsel (möglich / nicht möglich, d.h. die Türen werden am Ziel geöffnet bzw. nicht geöffnet)
- der Zeitspanne des Haltens (für den potentiellen Fahrgastwechsel / für das Laden des Fahrzeuges / …)
- der Umlaufnummer inklusive Angaben zum vorgegebenen Fahrweg (Wegpunkte, Route) zum Zielpunkt gemäß Fahrwegplanung der ÖV-Leitstelle
plus optional
- den Informationen zur Haltebucht
- der geplanten Fahrzeit zur Umsetzung der Mission gemäß Fahrwegplanung der ÖV-Leitstelle.

Hinweis:
Fahrtänderungen für Service & Wartungsumläufe / -fahrten / -fahrwege / -fahraufträge / -missionen obliegen dem BHMS eigenständig.

Betriebsschutz:
Zugang zur ÖV-Leitstelle (Sicherheitszone) haben nur ausgebildete und (sicherheitstechnisch) geschulte Mitarbeiter, Fahrgäste haben keinen Zugang.

Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Fahrplan / Fahrrouten Erweiterung (Regelbetrieb).

Aktionen:

- Der Disponent der ÖV-Leitstelle leitet dispositive Maßnahmen ein.
- Die ÖV-Leitstelle prüft ob die Maßnahmen ausführbar sind.
  - Anmeldung des Umlaufes mit Umlaufnummer des Fahrzeuges
  - Extraktion der Sequenz von Fahrten mit den jeweiligen Start- und Endpunkten aus dem Umlauf
  - Extraktion der Fahrwege (Routen) der Fahrten → Wegpunkte des Umlaufes
  - Extraktion der Fahraufträge (Fahrgast- Leer-, Rangier- oder Fahrt im Depot) aus dem Umlauf
  - Extraktion der Mission(en) = Teilstück(e) zwischen zwei Haltepunkten / -stellen aus den Fahrten
  - Freigabe der Umlaufnummer und der aktuellen Fahrplandaten.
- Die ÖV-Leitstelle übermittelt (über 3) die aktuellen Fahrplandaten (Fahrten + Fahraufträge und die Missionen) des Umlaufes an die AD-Leitstelle, welche diese zum AD-Bordsystem (über 8) weiterleitet.
  - Das AD-Bordsystem prüft die Daten gegen die hochauflösende Karte und meldet im Problemfall eine Störmeldung (UC-14 → UC-12 Systemüberwachung und ggf. Störmeldung)
- Die ÖV-Leitstelle übermittelt (über 7) die aktuellen Fahrplandaten (Fahrten + Fahraufträge und die Missionen) des Umlaufes an den ÖV-Bordrechner, welcher diese einließt und prüft, (z.B. ob alle notwendigen Durchsagen hinterlegt sind). Das Ergebnis der Prüfung wird an die ÖV-Leitstelle rückgemeldet.

Juristische Anforderungen:

- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
  Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
  Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.1 Generelle Kollisionsvermeidung
  Kollisionen mit anderen Verkehrsteilnehmenden und unbeteiligten Dritten müssen vermieden werden, sofern dies durch
  1. Notbremseingriffe oder
  2. andere Teilnehmende des umgebenden Verkehrs, andere unbeteiligte Dritte oder die Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nicht gefährdende Ausweichmanöver möglich ist. Kann eine Kollision zur Abwendung einer Gefährdung des Lebens der Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nur durch eine Gefährdung des Lebens anderer Teilnehmender des umgebenden Verkehrs oder unbeteiligter Dritter vermieden werden (unvermeidbare alternative Gefährdung von Menschenleben), darf der Schutz der anderen Teilnehmenden des umgebenden Verkehrs und der unbeteiligten Dritten nicht nachrangig gegenüber dem Schutz der Insassen des autonom fahrenden Kraftfahrzeugs erfolgen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.2 Interaktion mit anderen Verkehrsteilnehmenden
  a) Vorausfahrende Verkehrsteilnehmende auf der Fahrbahn werden erkannt. Es wird jederzeit in jedem Geschwindigkeitsbereich und in jeder möglichen Fahrsituation ein angemessener Sicherheitsabstand eingehalten. Der einzuhaltende Sicherheitsabstand bestimmt sich nach § 4 der Straßenverkehrs-Ordnung.
  b) Der Fahrstreifenwechsel vorausfahrender oder nachfolgender Fahrzeuge, der von einem benachbarten Fahrstreifen in den eigenen Fahrstreifen oder aus dem eigenen Fahrstreifen heraus in einen benachbarten Fahrstreifen erfolgt, wird erkannt und bei der Fahraufgabe entsprechend berücksichtigt.
  c) Situationen, welche einen Fahrstreifenwechsel bedingen (beispielsweise anhaltende oder langsame Fahrzeuge auf der Fahrbahn, Ende eines Fahrstreifens), werden erkannt und geeignete Manöver zum Fahrstreifenwechsel werden sicher durchgeführt.
  d) Einsatzfahrzeuge werden erkannt und geeignete Fahrmanöver sicher durchgeführt.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.3 Planung der Fahrpfade und Geschwindigkeiten
  Bei Geschwindigkeitsanpassungen kommt es zu keiner vermeidbaren Beeinträchtigung von Insassen,

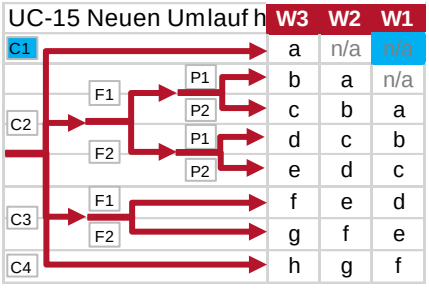
anderen Verkehrsteilnehmenden und unbeteiligten Dritten. Es gelten folgende Anforderungen:
a) Geschwindigkeitsbeschränkungen und Änderungen der Geschwindigkeitsbeschränkung werden erkannt und die Geschwindigkeit wird entsprechend angepaßt.
b) Besondere Anforderungen an die Geschwindigkeit werden erkannt und im Geschwindigkeits- und Fahrtverlauf befolgt (beispielsweise in Bereichen vor Schulen und an Arbeitsstellen an Straßen, an Bushaltestellen, Bahnübergängen, in engen Kurvenradien oder bei Gefällen, in Engstellen, in denen der eigene Fahrstreifen vom Gegenverkehr mitbenutzt werden muß).
c) Zeichen und Weisungen der Polizeibeamten gemäß § 36 der Straßenverkehrs-Ordnung, Wechsellichtzeichen gemäß § 37 der Straßenverkehrs-Ordnung, sonstige Zeichen gemäß der §§ 39 bis 42 der Straßenverkehrs-Ordnung sowie Verkehrseinrichtungen gemäß § 43 der Straßenverkehrs-Ordnung werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
d) Situationen, in denen die Vorfahrt anderen gewährt werden muß (beispielsweise vor Fußgängerüberwegen, in Kreuzungsbereichen oder Einmündungen), werden erkannt und ohne Gefährdung oder Behinderung der Vorfahrtberechtigten bewältigt. Es ist eine berechnete Zeit bis zum Aufprall von mehr als drei Sekunden bezüglich des Vorfahrtberechtigen einzuhalten. Wird von diesen Werten abgewichen, muß dies ausreichend begründet und auf Basis von systematischen Sicherheitsbewertungen nach dem Stand der Technik dokumentiert werden. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO 26262:2018-12 Straßenfahrzeuge – Funktionale Sicherheit erfüllt werden.
e) Bauliche Straßengestaltungen mit Auswirkung auf das Verhaltensrecht (beispielsweise bis zu 5 Meter vom Fahrbahnrand einer vorfahrtberechtigten Straße abgesetzte Radwege nach § 9 Absatz 3 der Straßenverkehrs-Ordnung oder abgesenkte Bordsteine nach § 10 der Straßenverkehrs-Ordnung) werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
f) Arbeitsstellen an Straßen, temporär veränderte Fahrbahnverläufe oder Fahrbahnmarkierungen werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
g) Defizite am Zubehör, insbesondere der Verkehrseinrichtungen (zum Beispiel verschlissene, beschädigte, fehlende oder defekte temporäre oder dauerhafte Fahrbahnmarkierungen und Verkehrszeichen, Phantommarkierungen) und der Straßenausstattung, insbesondere solcher nach vorstehenden Buchstaben a bis f werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Dies gilt insbesondere nach Sturm- und sonstigen Witterungsereignissen.

- AFGBV Anlage 1 Teil 1 Abschnitt 6 Übertragung von Daten an das Kraftfahrzeug
  Die zur selbstständigen Bewältigung der Fahraufgabe im autonomen Betrieb notwendigen Daten und Informationen von externen technischen Einheiten (beispielsweise Backends oder Server eines Anbieters, externe Sensoren, Smartphone) müssen vom Kraftfahrzeug sicher empfangen und verwendet werden können. Daten externer Einheiten können im Kraftfahrzeug zur Ausführung der autonomen Fahrfunktionen verwendet werden. Daten und Informationen können beispielsweise bei bestimmten Anwendungsfällen über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) von einer externen technischen Einheit an das Kraftfahrzeug und vom Kraftfahrzeug an eine technische Einheit übertragen werden. Die Übertragung solcher Daten muß insbesondere den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und nach dem aktuellen Stand der Technik abgesichert sein. Das Absicherungskonzept muß die in einer Bedrohungsanalyse identifizierten Risiken mit wirksamen Maßnahmen adressieren und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten. Zur Datenübertragung sollte eine zentrale sichere elektronische Steuereinheit (SECU) genutzt werden. Die SECU dient als Informationsgateway im Kraftfahrzeug. Die SECU kommuniziert intern an die Kommunikationsbusse des Kraftfahrzeugs und an den physischen On-Board-Diagnose II-Anschluß (OBD II) oder an eine proprietäre Schnittstelle eines Herstellers. Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung sind Teil 5 zu entnehmen. Die Integrität, Authentizität und Verfügbarkeit der Datenübertragung sind sicherzustellen. Die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen oder mit Infrastrukturkomponenten ist zulässig. Sie muß auf der Basis einer Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 insbesondere den Anforderungen an die Informationstechnik nach Teil 5 und damit den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen. Während des Betriebs in einer optionalen Testphase ist die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen und Infrastrukturkomponenten zu testen und gegebenenfalls anzupassen.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert.
  Hinweis:
  Dieses ist gültig für die Planung der Fahrzeugbewegung, die Routenführung über die Wegpunkte / Stützstellen des Umlaufs → Sequenz der Fahrten → Fahrwege → Fahraufträge → Missionen.
- Anders als ursprünglich geplant soll das autonom fahrende Fahrzeug jetzt aufgrund des Hinzufügens eines neuen Umlaufes eine andere Fahrtroute befahren. Da dieses die aktuelle Fahrbewegung nicht unmittelbar (ad hoc) beeinflußt bleibt hier die Sicherheitsrelevanz der Fahrt (ASIL-C) bestehen.

Risikograph:



≙ QM(C)

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzungen durch den gefährlichen Vorfall. (Akzeptiertes Standardrisiko bei Bürotätigkeiten)
✖	
✖	
W1	Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.16 UC-16 Neue Fahrplandaten aufgrund dispositiver Maßnahmen verteilen

Aufgrund eines unvorhersehbaren Ereignisses (Unfall, Stau, Verspätungen im Betriebsablauf, Kurzwende, etc.) müssen ad hoc Änderungen am Sollfahrplan durchgeführt werden. Die Datenaktualisierung des Sollfahrplans erfolgt über das Versenden der aktualisierten / überarbeiteten Version an die FGI-Kanäle, Auskunftsplattform, Web & App-Anwendung, sowie die DFI-Anzeiger an den Haltestellen.

Ferner wird der neue Sollfahrplan an die betroffenen Fahrzeuge übertragen. Dort werden die Informationen im ÖV-Bordrechner gespeichert und an die angeschlossenen Peripheriegeräte (Fahrgastinformationsanzeiger) im Fahrzeug übertragen.

Das Informieren der Fahrgäste wird beschrieben in UC-20 Fahrgäste akustisch informieren.

Hinweis:
Auf dem Betriebshof können eigenständig Umläufe für Service und Wartung durch das BHMS erstellt und angewendet werden. In diesem Fall übernimmt das BHMS die Rolle des Disponenten, welcher das Anfahren von internen Servicestationen (statt öffentlichen Haltestellen) auf dem BHMS organisiert. Somit wird aus dem Informieren der Fahrgäste, die Information an das Personal der Servicestation.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Zuweisung der aktualisierten Fahrplandaten sowie Überwachung der Fahrplanumsetzung auf Einhaltung der Fahrplandaten inklusive Pünktlichkeit. Informieren der Fahrgäste über Abweichungen gegenüber dem Fahrplan inklusive Unterstützung bei der Sicherstellung des reibungslosen Reiseablaufes der Fahrgäste.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung).
BHMS	keine (im Regelbetrieb)	keine (im Regelbetrieb)
AD-Leitstelle	siehe UC-13 / UC-14 / UC-15	siehe UC-13 / UC-14 / UC-15

Hinweis:
Ein Umlauf ist eine Sequenz von Fahrten, vom Ausrücken aus dem Betriebshof bis zum Einrücken in den Betriebshof, d. h. die Menge von Fahrten, die von einem Fahrzeug an einem (Teil des) Betriebstag(s) durchgeführt werden. Die Identifikation erfolgt über den Betriebstag sowie eine Umlaufnummer.

Hinweis:
Die Umlaufnummer dient zur Identifikation des erwarteten „Fahrzeugs“, allerdings im organisatorischen Sinne, nicht im technischen Sinne eines konkreten Fahrzeugs. Wird eine Route von verschiedenen Fahrzeugen (unterschiedliche Fahrzeugnummern) befahren, entspricht diese der Fahrtroutennummer.

Hinweis:
Die Fahrt entspricht der Bewegung eines Fahrzeugs vom Startpunkt bis zum Endpunkt eines Fahrwegs und wird über den Umlauf bzw. Kurs und die Fahrtnummer identifiziert.

Hinweis:
Der Fahrweg ist eine für eine Fahrt genutzte Route. Diese ist definiert durch eine geordnete Folge geplanter Haltepunkte (bei Leerfahrten nur Start- und Zielpunkt) und ggf. Zwischenpunkte, die den Streckenverlauf eindeutig festlegen.

Hinweis:
Der Fahrauftrag definiert als Oberbegriff eine Vorgabe für die Bewegung eines Fahrzeugs. Die Quelle von Fahraufträgen kann vielfältig sein: Fahrplan, dispositive Maßnahme der Leitstelle, Betriebshof- und Werkstattmanagement etc. Entsprechend ist die Granularität eines Fahrauftrages sehr unterschiedlich, er kann von einer kurzen (Rangier-)Bewegung bis zu einer komplexen Folge von Einsetz- / Fahrplan- / Aussetz-Fahrten reichen.

Hinweis:
Die Mission beschreibt einen Teil einer Fahrt zwischen zwei Haltepunkten / Haltestellen und beinhaltet Angaben zu
- dem Fahrgastwechsel (möglich / nicht möglich, d.h. die Türen werden am Ziel geöffnet bzw. nicht geöffnet)
- der Zeitspanne des Haltens (für den potentiellen Fahrgastwechsel / für das Laden des Fahrzeuges / …)
- der Umlaufnummer inklusive Angaben zum vorgegebenen Fahrweg (Wegpunkte, Route) zum Zielpunkt gemäß Fahrwegplanung der ÖV-Leitstelle
plus optional
- den Informationen zur Haltebucht
- der geplanten Fahrzeit zur Umsetzung der Mission gemäß Fahrwegplanung der ÖV-Leitstelle.

Hinweis:
Fahrtänderungen für Service & Wartungsumläufe / -fahrten / -fahrwege / -fahraufträge / -missionen obliegen dem BHMS eigenständig.

Betriebsschutz:
Zugang zum Betriebshof (Sicherheitszone) haben nur ausgebildete und (sicherheitstechnisch) geschulte Mitarbeiter, Fahrgäste haben keinen Zugang.

Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Datenaktualisierung aufgrund eines unvorhersehbaren Ereignisses (Regelbetrieb des planbaren Sonderfalls).

Aktionen:

- Die ÖV-Leitstelle ermittelt die betroffenen Umläufe und die dazugehörigen Fahrzeuge und führt dort eine Datenaktualisierung (UC-13 Fahrtänderung / UC-14 Umlaufänderung / UC-15 Neuen Umlauf hinzufügen) durch.

Juristische Anforderungen:

- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
  Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
  Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.1 Generelle Kollisionsvermeidung
  Kollisionen mit anderen Verkehrsteilnehmenden und unbeteiligten Dritten müssen vermieden werden, sofern dies durch
  1. Notbremseingriffe oder
  2. andere Teilnehmende des umgebenden Verkehrs, andere unbeteiligte Dritte oder die Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nicht gefährdende Ausweichmanöver möglich ist. Kann eine Kollision zur Abwendung einer Gefährdung des Lebens der Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nur durch eine Gefährdung des Lebens anderer Teilnehmender des umgebenden Verkehrs oder unbeteiligter Dritter vermieden werden (unvermeidbare alternative Gefährdung von Menschenleben), darf der Schutz der anderen Teilnehmenden des umgebenden Verkehrs und der unbeteiligten Dritten nicht nachrangig gegenüber dem Schutz der Insassen des autonom fahrenden Kraftfahrzeugs erfolgen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.2 Interaktion mit anderen Verkehrsteilnehmenden
  a) Vorausfahrende Verkehrsteilnehmende auf der Fahrbahn werden erkannt. Es wird jederzeit in jedem Geschwindigkeitsbereich und in jeder möglichen Fahrsituation ein angemessener Sicherheitsabstand eingehalten. Der einzuhaltende Sicherheitsabstand bestimmt sich nach § 4 der Straßenverkehrs-Ordnung.
  b) Der Fahrstreifenwechsel vorausfahrender oder nachfolgender Fahrzeuge, der von einem benachbarten Fahrstreifen in den eigenen Fahrstreifen oder aus dem eigenen Fahrstreifen heraus in einen benachbarten Fahrstreifen erfolgt, wird erkannt und bei der Fahraufgabe entsprechend berücksichtigt.
  c) Situationen, welche einen Fahrstreifenwechsel bedingen (beispielsweise anhaltende oder langsame Fahrzeuge auf der Fahrbahn, Ende eines Fahrstreifens), werden erkannt und geeignete Manöver zum Fahrstreifenwechsel werden sicher durchgeführt.
  d) Einsatzfahrzeuge werden erkannt und geeignete Fahrmanöver sicher durchgeführt.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.3 Planung der Fahrpfade und Geschwindigkeiten
  Bei Geschwindigkeitsanpassungen kommt es zu keiner vermeidbaren Beeinträchtigung von Insassen, anderen Verkehrsteilnehmenden und unbeteiligten Dritten. Es gelten folgende Anforderungen:
  a) Geschwindigkeitsbeschränkungen und Änderungen der Geschwindigkeitsbeschränkung werden erkannt und die Geschwindigkeit wird entsprechend angepaßt.
  b) Besondere Anforderungen an die Geschwindigkeit werden erkannt und im Geschwindigkeits- und Fahrtverlauf befolgt (beispielsweise in Bereichen vor Schulen und an Arbeitsstellen an Straßen, an Bushaltestellen, Bahnübergängen, in engen Kurvenradien oder bei Gefällen, in Engstellen, in denen der eigene Fahrstreifen vom Gegenverkehr mitbenutzt werden muß).
  c) Zeichen und Weisungen der Polizeibeamten gemäß § 36 der Straßenverkehrs-Ordnung, Wechsellichtzeichen gemäß § 37 der Straßenverkehrs-Ordnung, sonstige Zeichen gemäß der §§ 39 bis 42 der Straßenverkehrs-Ordnung sowie Verkehrseinrichtungen gemäß § 43 der Straßenverkehrs-Ordnung werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  d) Situationen, in denen die Vorfahrt anderen gewährt werden muß (beispielsweise vor Fußgängerüberwegen, in Kreuzungsbereichen oder Einmündungen), werden erkannt und ohne Gefährdung oder Behinderung der Vorfahrtberechtigten bewältigt. Es ist eine berechnete Zeit bis zum Aufprall von mehr als drei Sekunden

bezüglich des Vorfahrtberechtigen einzuhalten. Wird von diesen Werten abgewichen, muß dies ausreichend begründet und auf Basis von systematischen Sicherheitsbewertungen nach dem Stand der Technik dokumentiert werden. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO 26262:2018-12 Straßenfahrzeuge – Funktionale Sicherheit erfüllt werden.
e) Bauliche Straßengestaltungen mit Auswirkung auf das Verhaltensrecht (beispielsweise bis zu 5 Meter vom Fahrbahnrand einer vorfahrtberechtigten Straße abgesetzte Radwege nach § 9 Absatz 3 der Straßenverkehrs-Ordnung oder abgesenkte Bordsteine nach § 10 der Straßenverkehrs-Ordnung) werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
f) Arbeitsstellen an Straßen, temporär veränderte Fahrbahnverläufe oder Fahrbahnmarkierungen werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
g) Defizite am Zubehör, insbesondere der Verkehrseinrichtungen (zum Beispiel verschlissene, beschädigte, fehlende oder defekte temporäre oder dauerhafte Fahrbahnmarkierungen und Verkehrszeichen, Phantommarkierungen) und der Straßenausstattung, insbesondere solcher nach vorstehenden Buchstaben a bis f werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Dies gilt insbesondere nach Sturm- und sonstigen Witterungsereignissen.

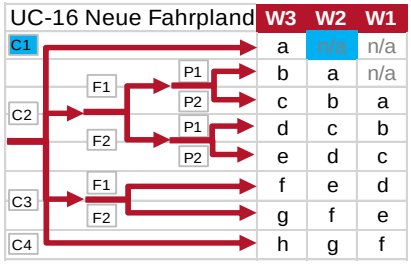
- AFGBV Anlage 1 Teil 1 Abschnitt 6 Übertragung von Daten an das Kraftfahrzeug
  Die zur selbstständigen Bewältigung der Fahraufgabe im autonomen Betrieb notwendigen Daten und Informationen von externen technischen Einheiten (beispielsweise Backends oder Server eines Anbieters, externe Sensoren, Smartphone) müssen vom Kraftfahrzeug sicher empfangen und verwendet werden können. Daten externer Einheiten können im Kraftfahrzeug zur Ausführung der autonomen Fahrfunktionen verwendet werden. Daten und Informationen können beispielsweise bei bestimmten Anwendungsfällen über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) von einer externen technischen Einheit an das Kraftfahrzeug und vom Kraftfahrzeug an eine technische Einheit übertragen werden. Die Übertragung solcher Daten muß insbesondere den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und nach dem aktuellen Stand der Technik abgesichert sein. Das Absicherungskonzept muß die in einer Bedrohungsanalyse identifizierten Risiken mit wirksamen Maßnahmen adressieren und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten. Zur Datenübertragung sollte eine zentrale sichere elektronische Steuereinheit (SECU) genutzt werden. Die SECU dient als Informationsgateway im Kraftfahrzeug. Die SECU kommuniziert intern an die Kommunikationsbusse des Kraftfahrzeugs und an den physischen On-Board-Diagnose II-Anschluß (OBD II) oder an eine proprietäre Schnittstelle eines Herstellers. Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung sind Teil 5 zu entnehmen. Die Integrität, Authentizität und Verfügbarkeit der Datenübertragung sind sicherzustellen. Die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen oder mit Infrastrukturkomponenten ist zulässig. Sie muß auf der Basis einer Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 insbesondere den Anforderungen an die Informationstechnik nach Teil 5 und damit den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen. Während des Betriebs in einer optionalen Testphase ist die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen und Infrastrukturkomponenten zu testen und gegebenenfalls anzupassen.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert.
- Anders als ursprünglich geplant soll das autonom fahrende Fahrzeug, während der Fahrgastwechselzeit, jetzt aufgrund einer Fahrtänderung unmittelbar (ad hoc) die Routenführung (Wegpunkte) ändern, wodurch sich die Fahrplanzeiten verändern. Dadurch kann ein geplanter Zeitpunkt des Haltens zu einem Zeitpunkt des Fahrens werden, welches eine abrupte Türschließung ohne Vorwarnung auslöst.
- Anders als ursprünglich geplant soll das autonom fahrende Fahrzeug, jetzt aufgrund einer Fahrtänderung unmittelbar (ad hoc) abbiegen statt dem Straßenverlauf gerade aus zu folgen. Die momentan gefahrene Geschwindigkeit ist zu hoch für die durch den Straßenverlauf vorgegebene Kurvenführung, d.h. die auftretende Seitenführungskraft (im Zusammenhang mit der Längsführungskraft) kann das Rad des Fahrzeuges, insbesondere Aufgrund von sich ggf. negativ dazu addierenden Wetterbedingungen (Nässe), nicht auf die Straße übertragen (Kammscher Kreis). Die Fahrerassistenzsysteme des Fahrzeugherstellers (OEM), welche das Autonomous Driving System (ADS) des Fahrzeugherstellers (OEM) unterstützen, können aufgrund der Kurzfristigkeit (ad hoc abbiegen) dieses nicht kompensieren, insbesondere weil die Eingriffsmöglichkeit der Technischen Aufsicht (TA) über das AD-Bordsystem (ADBS) die Fahrzeugfunktion des (OEM) im Eingriffsfall übersteuern können muß. Die Reaktionsfähigkeit der Technischen Aufsicht (TA) der AD-Leitstelle, welche über die Fahrplanänderung informiert wird, kann dieses nicht abfangen, weil nicht vorhersehbar ist, wann exakt das AD-Bordsystem dieses im Fahrzeug umsetzt.
  Hinweis:
  Im konventionellen Betrieb des Individualverkehrs kann das Navigationssystem schnell neue Strecken berechnen, aber der Fahrer entscheidet (kontrolliert) wann das Manöver umgesetzt wird. In der autonomen Fahrt wird dieses vom AD-Bordsystem selbständig umgesetzt, weshalb der exakte Zeitpunkt der Umsetzung der Änderung der Fahrtroute nicht für die Technische Aufsicht (TA) der AD-Leitstelle vorhersehbar ist, wodurch ein ggf. notwendiger menschlicher Eingriff zum Abfangen / Übersteuern der autonomen Aktion

nicht gewährleistet ist. Folglich sind Fahrtroutenänderungen so abzusichern, daß nach dem Passieren des Point of Safe Return (PSR), keine abrupte, unbeherrschbare Routenänderung umgesetzt wird, wobei insbesondere die Systemgrenzen (Kammscher Kreis, Elchtest) nicht überschritten werden dürfen. Andernfalls würde die autonome Fahrt, durch die unkontrollierbare Fahrtänderung zu einem nicht geeigneten Zeitpunkt, zu einer unkontrollierbaren Situation → ISO-26262-Band 3: 2018 – Tabelle 3: „C3 Difficult to control or uncontrollable“, was zu einer ASIL-D Bewertung führt.
Hinweis:
Bei der Verifikation der implementierten, automatisierten Schutzmaßnahmen auf dem Testgelände (Kreiselfläche) sind, zum Schutz der Sicherheitsfahrer, Geschwindigkeitsbegrenzung als Sicherheitsauflage (Maßnahme) anzuordnen, welche langsam Schrittweise über den Testablauf erhöht werden können um die Systemgrenze der implementierten Sicherheit iterativ zu ermitteln.

Risikograph (Planung Fahrzeugbewegung):

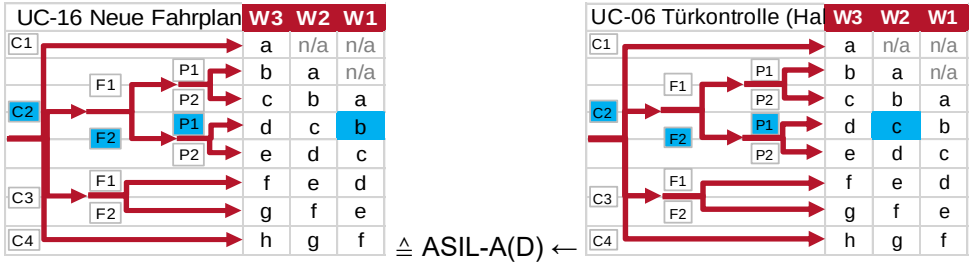


≙ QM(D)

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzungen durch den gefährlichen Vorfall. (Akzeptiertes Standardrisiko bei Bürotätigkeiten)
✖	
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich.

Risikograph (Fahrtänderung der Wegpunkte im Stillstand, v=0km/h):

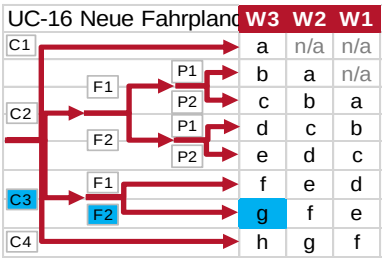


≙ ASIL-A(D) ←

Begründung zur Wahl der Risikoparameter:
VDV-Schrift-161-2 Kap. 3.4.1: Verhinderung der Anfahrt mit geöffneten Türen

C2	Die Betriebserfahrungen haben gezeigt, daß im Versagensfalle nur eine Person betroffen ist
F2	Fahrgäste halten sich im Regelfall häufig in der Nähe der Türen auf
P1	Gefahrenabwehr ist möglich unter der Bedingung, daß der Fahrgast nicht das Fahrzeug verläßt bzw. ein Sturz vermieden werden kann.
W1	Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich. *Hinweis:* *Bewertung ist Abweichend zu VDV-Originaleinstufung, weil hier die Fahrtänderung zu diesem Zeitpunkt kumulativ hinzukommen müßte, welches die Wahrscheinlichkeit reduziert.* *VDV-Originaleinstufung (VDV-Schrift-161-2 Kap. 3.4.1: Verhinderung der Anfahrt mit geöffneten Türen):* *W2 Aufgrund des Einwirkens verschiedenster Bedingungen bis zur unbeabsichtigten Anfahrt wird die Eintrittswahrscheinlichkeit als gering eingestuft.*

Risikograph (Fahrtänderung der Wegpunkte während der Fahrt):



≙ ASIL-D

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen durch den gefährlichen Vorfall
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich
✖	
W3	Eine relativ hohe Auftretenswahrscheinlichkeit und häufige unerwünschte Ereignisse sind wahrscheinlich.

3.2.17 UC-17 Anschlußbeziehungen aktualisieren und darstellen

Aufgrund von Echtzeitdaten, dispositiven Maßnahmen oder anderen Einflüssen müssen die Anschlußbeziehungen an den Haltestellen, in der mobilen Fahrgastinformation und im Fahrzeug aktualisiert werden. Es besteht die Möglichkeit, Anschlüsse trotz Verspätung zu halten. Abbringerfahrzeuge müssen dann auf Zubringerfahrzeuge warten. Der Zubringer wiederum erhält die Information, daß der Abbringer wartet.

Fahrgästen im Abbringerfahrzeug wird die reale aktuelle Verspätung und nicht die prognostizierte Abfahrtzeit angezeigt.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Fahrplandaten der betroffenen Fahrzeuge aktualisieren und über das FGI verteilen. Abweichung in Statistik zur späteren Auswertung sichern.	Fahrplanaktualisierung mit Synchronisation der betroffenen Zu- und Abbringer. Informieren der Fahrgäste.
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung Weiterleitung der geänderten Haltezeiten	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Die Mission beschreibt einen Teil einer Fahrt zwischen zwei Haltepunkten / Haltestellen und beinhaltet Angaben zu
- dem Fahrgastwechsel (möglich / nicht möglich, d.h. die Türen werden am Ziel geöffnet bzw. nicht geöffnet)
- der Zeitspanne des Haltens (für den potentiellen Fahrgastwechsel / für das Laden des Fahrzeuges / …)
- der Umlaufnummer inklusive Angaben zum vorgegebenen Fahrweg (Wegpunkte, Route) zum Zielpunkt gemäß Fahrwegplanung der ÖV-Leitstelle
plus optional
- den Informationen zur Haltebucht
- der geplanten Fahrzeit zur Umsetzung der Mission gemäß Fahrwegplanung der ÖV-Leitstelle.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Fahrzeug ist im Betrieb (Regelbetrieb) und setzt die Missionen der ÖV-Leitstelle *(außerhalb des BHMS)* um.
Es wurden bei Fahrzeugen (Zubringer) Verzögerungen gegenüber den Fahrplandaten bei der Umsetzung erkannt, welche sich noch im Rahmen der Korrigierbarkeit befinden, weshalb die Anschlußfahrzeuge der Fahrfortsetzung (Abbringer) eine verlängerte Haltezeit erhalten.

Aktionen:

- Die ÖV-Leitstelle erkennt die Abweichung zu den Fahrplandaten und ermittelt die beteiligten Fahrzeuge (Zu- und Abbringer).
- Die ÖV-Leitstelle prüft ob Maßnahmen eingeleitet werden können, welche den Anschluß zur potentiellen Fahrtfortsetzung sicherstellen können. Sofern dieses möglich ist werden die Maßnahmen an die betroffenen Fahrzeuge und das FGI übermittelt (über 7 und 3 → 8 plus 1), d.h.
  - ► die Fahrgäste im Zubringer werden über das Warten des Abbringers informiert.
  - ► der Abbringer wird angewiesen auf den Zubringer zu warten, damit verlängert sich die Haltezeit.

  Hinweis:
  Es könnte sinnvoll sein, daß die ÖV-Leitstelle den Bedarf der Maßnahme vorher bei den betroffenen Fahrgästen im Fahrzeug abfragt. (Wie viele Fahrgäste haben eine Verspätung zu ertragen, um sicherzustellen, daß wie viele Mitreisende ihren Anschluß erhalten).
  Hinweis:
  Die Einbindung der AD-Leitstellen (über 3) erfolgt nur für Shuttle / Bus, da S-Bahn und Eisenbahn nicht unter der Kontrolle der AD-Leitstelle stehen. S-Bahn und Eisenbahn sind über deren Leitstellen einzubinden.
- Der ÖV-Bordrechner informiert (über 11) die Fahrgäste in den betroffenen Fahrzeugen (Zu- und Abbringer).
- Das FGI Informiert alle potentiellen Fahrgäste über die aktuellen Fahrplandaten.
  (Verspätung bei Warten, bzw. keine Benachrichtigung bei Weiterfahrt der Abbringer ohne Warten).

- Das AD-Bordsystem setzt die getroffene Maßnahme (Haltezeitverlängerung im Abbringer) um. (Haltezeit = Parameter der Mission)
  Hinweis:
  Sofern es sich um ein Shuttle / Bus handelt, da S-Bahn und Eisenbahn nicht unter der Kontrolle der AD-Leitstelle stehen.
- Die ÖV-Leitstelle speichert die Information zu den getroffenen Maßnahmen in der Statistik.

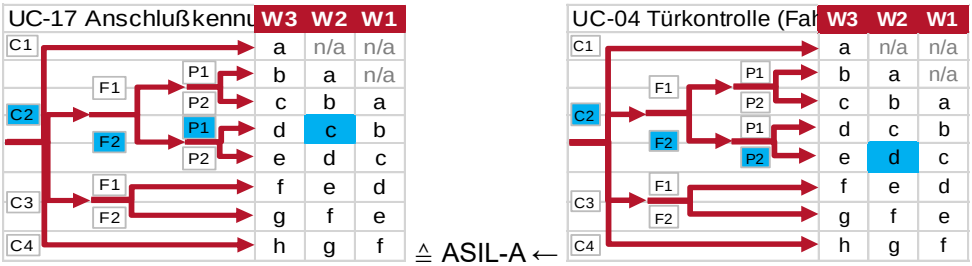
Juristische Anforderungen:

- AFGBV Anlage 1 Teil 1 Abschnitt 1.4 Reaktion auf Umweltbedingungen
  Wetter-, Umwelt- und Straßeninfrastrukturbedingungen (beispielsweise Regen, Sichtbehinderung durch Rauch, Schlaglöcher) werden im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Fahrpfad und Geschwindigkeit sind – bis hin zum Stillstand des Fahrzeugs – so zu wählen, daß die in den Nummern 1.1 bis 1.3 gestellten Anforderungen auch bei geänderten Umweltbedingungen erfüllt werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.2 Technische Vorgaben für das Speichern, Auslesen und Übertragen von Daten. Das System der Datenspeicherung darf nicht flüchtig sein. Die gespeicherten Daten müssen im stromlosen Zustand erhalten bleiben.

Gefahren nach HAZOP:

- Die Verlängerung der Haltezeit verändert die Mission. Dieses kann <u>während</u> der Türschließung (durch den Ablauf der bisherigen Haltezeit) auftreten. Somit kann (nach dem Abschluß der laufenden Türschließung) eine erneute Türöffnung durch die entsprechenden Knöpfe (innen / außen) angefordert werden. Die daraus resultierende Gefahr ist unter UC-06 Türkontrolle bewertet und beschrieben.
  Hinweis:
  Die Zubringer fahren (unverändert) weiter, lediglich die Abbringer erhalten die Anweisung auf die Zubringer zu warten, sofern die ÖV-Leitstelle dieses anordnet.

Risikograph:



VDV-Schrift-161-2 Kap. 3.4.1: Verhinderung der Anfahrt mit geöffneten Türen.

Begründung zur Wahl der Risikoparameter:

C2	Die Betriebserfahrungen haben gezeigt, daß im Versagensfalle nur eine Person betroffen ist.
F2	Fahrgäste halten sich im Regelfall häufig in der Nähe der Türen auf.
P1	Gefahrenabwehr ist möglich unter der Bedingung, daß der Fahrgast nicht das Fahrzeug verläßt bzw. ein Sturz vermieden werden kann.
W2	Aufgrund des Einwirkens verschiedenster Bedingungen bis zur unbeabsichtigten Anfahrt wird die Eintrittswahrscheinlichkeit als gering eingestuft.

3.2.18 UC-18 Zielbeschilderung außen und innen ändern

Die Zielbeschilderungen an den Außenanzeigern sowie im Fahrzeuginneren werden angepaßt.
Gründe hierfür können sein:

- Betriebsaufnahme (Ausrücken aus dem Betriebshof) *(UC-01 → UC-02 → UC-44 → UC-03 → UC-18)*
- Umlaufwechsel
- Umleitung ohne Rückkehr auf den Fahrweg
- Langwende
- Kurzwende
- Linienteilung etc.

Der Vorgang läuft lokal auf dem Fahrzeug.
Im konventionellen Betrieb hat das fahrende Personal die Möglichkeit, die Zielbeschilderung manuell anzupassen.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine	Fahrgastinformation (FGI) korrekt anzeigen. *Hinweis:* *Die Verantwortung der Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung) obliegt der ÖV-Leitstelle, jedoch werden diese Daten nicht über diesen Anwendungsfall (UseCase) initiiert.*
BHMS	keine	keine
AD-Leitstelle	keine	keine

Hinweis:
Zuständigkeit = ÖV-Bordrechner.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Änderung der Außen- und Innenanzeiger der Fahrgastinformation (FGI) (Regelbetrieb).

Aktionen:

- Vorbedingung:
  Der ÖV-Bordrechner trackt den Ablauf / Umsetzung des Fahrplanes und meldet das Einhalten (Pünktlichkeit) sowie Abweichungen (Verspätung / Verfrühung) kontinuierlich an die ÖV-Leitstelle. Dazu werden die GPS Daten der Mission kontinuierlich (über 14) ausgewertet.
- Sobald der ÖV-Bordrechner aus dem Fahrauftrag die Notwendigkeit der Aktualisierung der Zielbeschilderung (Außen- und Innenanzeiger) ableitet, setzt der ÖV-Bordrechner diese Aktualisierung über die zugehörige Fahrgast HMI ÖV Schnittstelle (über 11) um.
  Hinweis:
  Der Fahrauftrag definiert als Oberbegriff eine Vorgabe für die Bewegung eines Fahrzeugs. Die Quelle von Fahraufträgen kann vielfältig sein: Fahrplan, dispositive Maßnahme der Leitstelle, Betriebshof- und Werkstattmanagement etc. Entsprechend ist die Granularität eines Fahrauftrages sehr unterschiedlich, er kann von einer kurzen (Rangier-)Bewegung bis zu einer komplexen Folge von Einsetz- / Fahrplan- / Aussetz-Fahrten reichen.

Juristische Anforderungen:

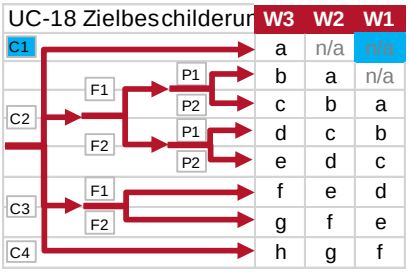
- AFGBV Anlage 1 Teil 5 Anforderungen an die Sicherheit im Bereich der Informationstechnologie
- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.

- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).

Gefahren nach HAZOP:

- Keine
  Der Anwendungsfall (UseCase) gehört zur Fahrgastinformation (FGI), welche keinen Einfluß auf die Sicherheit einer Person ausüben kann.
  Hinweis:
  Im Fehlerfall (nicht korrekte Anzeige) wird der Fahrgast zu einem anderen Ort befördert als der Fahrgast wollte.

Risikograph:



≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzung (Akzeptiertes Standardrisiko bei der allgemein üblichen Nutzung von Verkehrsmitteln)
✖	
✖	
W1	Die angenommene Auswirkung kann unmittelbar oder auch verzögert eintreten, d.h. sobald der Fahrgast die für ihn nichtzutreffende Fahrroute bemerkt. Somit ergibt sich eine Bewertung von W1. Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.19 UC-19 Liniennummer ändern

Ein Fahrzeug wird auf einer anderen Linie eingesetzt. Hierfür muss die Liniennummer am Fahrzeug geändert werden. Dies kann automatisch durch das System oder manuell durch das Personal erfolgen.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine	Fahrgastinformation (FGI) korrekt anzeigen. *Hinweis:* *Die Verantwortung der Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung) obliegt der ÖV-Leitstelle, jedoch werden diese Daten nicht über diesen Anwendungsfall (UseCase) initiiert.*
BHMS	keine	keine
AD-Leitstelle	keine	keine

Hinweis:
Zuständigkeit = ÖV-Bordrechner.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Änderung der Liniennummer ≙ Änderung Außen- und Innenanzeiger der Fahrgastinformation (FGI) (Regelbetrieb).

Aktionen:

- Vorbedingung:
  Der ÖV-Bordrechner trackt den Ablauf / Umsetzung des Fahrplanes und meldet das Einhalten (Pünktlichkeit) sowie Abweichungen (Verspätung / Verfrühung) kontinuierlich an die ÖV-Leitstelle. Dazu werden die GPS Daten der Mission kontinuierlich (über 14) ausgewertet.
- Sobald der ÖV-Bordrechner aus dem Fahrauftrag die Notwendigkeit der Aktualisierung der Liniennummer der Zielbeschilderung (Außen- und Innenanzeiger) ableitet, setzt der ÖV-Bordrechner diese Aktualisierung über die zugehörige Fahrgast HMI ÖV Schnittstelle (über 11) um.
  Hinweis:
  Der Fahrauftrag definiert als Oberbegriff eine Vorgabe für die Bewegung eines Fahrzeugs. Die Quelle von Fahraufträgen kann vielfältig sein: Fahrplan, dispositive Maßnahme der Leitstelle, Betriebshof- und Werkstattmanagement etc. Entsprechend ist die Granularität eines Fahrauftrages sehr unterschiedlich, er kann von einer kurzen (Rangier-)Bewegung bis zu einer komplexen Folge von Einsetz- / Fahrplan- / Aussetz-Fahrten reichen.

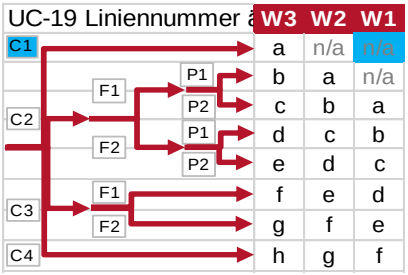
Juristische Anforderungen:

- AFGBV Anlage 1 Teil 5 Anforderungen an die Sicherheit im Bereich der Informationstechnologie
- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.
- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).

Gefahren nach HAZOP:

- Keine
  Der Anwendungsfall (UseCase) gehört zur Fahrgastinformation (FGI), welche keinen Einfluß auf die Sicherheit einer Person ausüben kann.
  Hinweis:
  Im Fehlerfall (nicht korrekte Anzeige) wird der Fahrgast zu einem anderen Ort befördert als der Fahrgast wollte.

Risikograph:



≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzung (Akzeptiertes Standardrisiko bei der allgemein üblichen Nutzung von Verkehrsmitteln)
✖	
✖	
W1	Die angenommene Auswirkung kann unmittelbar oder auch verzögert eintreten, d.h. sobald der Fahrgast die für ihn nichtzutreffende Fahrroute bemerkt. Somit ergibt sich eine Bewertung von W1. Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.20 UC-20 Fahrgäste akustisch informieren

Das Fahrpersonal will die Fahrgäste akustisch über aktuelle Gegebenheiten informieren. Alternativ kann die akustische Information durch die ÖV-Leitstelle an einzelne / ausgewählte Fahrzeuge oder den gesamten Fuhrpark erfolgen. Gründe können allgemeine Meldungen, Echtzeitinformationen wie kurzfristige Störung oder Änderungen im Fahrtablauf, Aktualisierungen der Anschlußbeziehungen oder ähnliches sein.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Die Verantwortung der Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung) obliegt der ÖV-Leitstelle	Korrektheit, Vollständigkeit und Brauchbarkeit der Fahrgastinformation (FGI).
BHMS	keine	keine
AD-Leitstelle	keine	keine

Hinweis:
Zuständigkeit = ÖV-Bordrechner (beim Fahrzeug, nicht Haltestelle).

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Informationsverteilung (Regelbetrieb).

Aktionen:

- ÖV-Leitstelle erstellt akustische Durchsage der aktuellen Fahrgastinformation.
- ÖV-Leitstelle ermittelt die beteiligten Fahrzeuge sowie Haltestellen und sendet die jeweilige Nachricht / Information an
  - den ÖV-Bordrechner im Fahrzeug,
    welcher die Durchsage (über 11), das Fahrgast HMI ÖV, ausgibt.
  - die Haltestelle, sofern diese über eine solche Einrichtung verfügt, welche die Durchsage ausgibt.
    Hinweis:
    Dieses kann auch als Interface zu S-Bahn und Eisenbahn verstanden werden, welches außerhalb des Projektscope liegt.

Juristische Anforderungen:

- AFGBV Anlage 1 Teil 5 Anforderungen an die Sicherheit im Bereich der Informationstechnologie
- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.
- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).

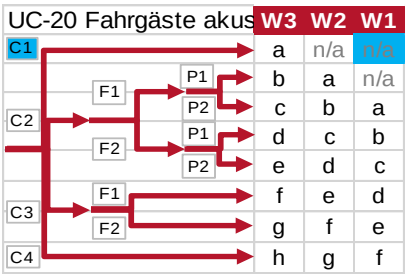
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

Gefahren nach HAZOP:

- Keine
  Der Anwendungsfall (UseCase) gehört zur Fahrgastinformation (FGI), welche keinen Einfluß auf die Sicherheit einer Person ausüben kann, (sofern man die Lautstärke der Ansage auf ein vernünftiges Maß begrenzt).
  Hinweis:
  Im Fehlerfall (nicht korrekte Ansage) wird der Fahrgast zu einem anderen Ort befördert als der Fahrgast wollte.

Risikograph:



≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzung (Akzeptiertes Standardrisiko bei der allgemein üblichen Nutzung von Verkehrsmitteln)
✖	
✖	
W1	Die angenommene Auswirkung kann unmittelbar oder auch verzögert eintreten, d.h. sobald der Fahrgast die für ihn nichtzutreffende Fahrroute bemerkt. Somit ergibt sich eine Bewertung von W1. Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.21 UC-21 Fahrgäste textuell informieren (Tickertext)

Zusätzlich oder auch alternativ zur akustischen Fahrgastinformation können Tickertexte als textuelle Information auf den Innenanzeigen im Fahrzeug und/oder via Haltestellenanzeigen übermittelt werden. Die Eingabe erfolgt in der Regel getrennt für Fahrzeuge und Haltestellen, da auch das Informationsbedürfnis häufig ein anderes ist.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Die Verantwortung der Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung) obliegt der ÖV-Leitstelle	Korrektheit, Vollständigkeit und Brauchbarkeit der Fahrgastinformation (FGI).
BHMS	keine	keine
AD-Leitstelle	keine	keine

Hinweis:
Zuständigkeit = ÖV-Bordrechner (beim Fahrzeug, nicht Haltestelle).

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Informationsverteilung (Regelbetrieb).

Aktionen:

- ÖV-Leitstelle erstellt textuelle Fahrgastinformation.
- ÖV-Leitstelle ermittelt die beteiligten Fahrzeuge sowie Haltestellen und sendet die jeweilige Nachricht / Information an
  - den ÖV-Bordrechner im Fahrzeug,
    welcher die textuelle Information (über 11), das Fahrgast HMI ÖV, z.B. den Innenanzeiger ausgibt.
  - die Haltestelle, sofern diese über eine solche Einrichtung verfügt, welche die textuelle Nachricht anzeigt.
    Hinweis:
    Dieses kann auch als Interface zu S-Bahn und Eisenbahn verstanden werden, welches außerhalb des Projektscope liegt.

Juristische Anforderungen:

- AFGBV Anlage 1 Teil 5 Anforderungen an die Sicherheit im Bereich der Informationstechnologie
- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.
- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).

Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

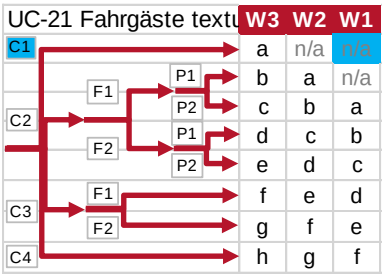
Gefahren nach HAZOP:

- Keine
  Der Anwendungsfall (UseCase) gehört zur Fahrgastinformation (FGI), welche keinen Einfluß auf die Sicherheit einer Person ausüben kann, (sofern man die Anzeige vernünftig lesbar gestaltet, kein

Stroboblitzer).

Hinweis:
Im Fehlerfall (nicht korrekte Anzeige) wird der Fahrgast zu einem anderen Ort befördert als der Fahrgast wollte.

Risikograph:



≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzung (Akzeptiertes Standardrisiko bei der allgemein üblichen Nutzung von Verkehrsmitteln).
✖	
✖	
W1	Die angenommene Auswirkung kann unmittelbar oder auch verzögert eintreten, d.h. sobald der Fahrgast die für ihn nichtzutreffende Fahrroute bemerkt. Somit ergibt sich eine Bewertung von W1. Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.22 UC-22 Problem mit Fahrgast (störendes Verhalten)

In Fahrzeugen des öffentlichen Verkehrs gelten unterschiedliche Verhaltensregeln und Verbote.
Beispiele hierfür sind:

- Rauchverbot ← Nichtraucherschutz
- Während der Fahrt nicht mit dem Fahrpersonal sprechen
- Keine laute Musik
- Gurtpflicht (insofern vorhanden).
- Pflicht zum Tragen einer medizinischen Schutzmaske

Ein Fahrgast verhält sich unkooperativ und verhindert die sichere Weiterfahrt des Fahrzeugs, wenn die Verhaltensregeln (Manieren) und Gebote (Respektvolles Verhalten) nicht eingehalten werden.
Ferner kann der Fahrgast die Weiterfahrt z.B. durch das Blockieren von Türen verhindern.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Sofern der beschwerdeführende Fahrgast den Knopf Kommunikation verwendet wird die ÖV-Leitstelle kontaktiert, welche die Beschwerde entgegennimmt und geeignete Maßnahmen einleitet. *Hinweis:* *Die ÖV-Leitstelle kann das FG-Notfallmanagement und/oder die Technische Aufsicht der AD-Leitstelle mit einbinden, ggf. die Zuständigkeit / Verantwortung übergeben.*	Problemlösung, bis Abgabe / Weiterleitung.
BHMS	keine	keine
AD-Leitstelle	Sofern der beschwerdeführende Fahrgast den Knopf Notfall / Nothalt verwendet wird die AD-Leitstelle kontaktiert, welche die Beschwerde entgegennimmt und geeignete Maßnahmen einleitet. *Hinweis:* *Die AD-Leitstelle kann das FG-Notfallmanagement und/oder die ÖV-Leitstelle mit einbinden, ggf. die Zuständigkeit / Verantwortung übergeben.*	Problemlösung, bis Abgabe / Weiterleitung.

Hinweis:
Dieser UseCase hängt von der Bedienung durch den Fahrgast selbst ab, je nachdem ob dieser den Knopf „Kommunikation“ oder „Notruf“ / „Nothalt“ anwendungsgemäß korrekt verwendet.
Schlechtes respektloses Verhalten ist Grund für eine Beschwerde aber juristisch keine Notlage.
StGB § 34 Rechtfertigender Notstand:
Wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, handelt nicht rechtswidrig, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Dies gilt jedoch nur, soweit die Tat ein angemessenes Mittel ist, die Gefahr abzuwenden.
Somit ist die Fehlbedienung Nothalt zum Erzielen der Möglichkeit zum Aussteigen eines Fahrgastes, veranlaßt z.B. durch Rauchen eines anderen Fahrgastes, im Bereich Automotive angemessen, weil ein Shuttle / Bus kurzfristig anhalten kann, im Gegensatz zur Eisenbahn / U-Bahn / S-Bahn welche erst an einer Station, nicht aber auf der Strecke oder im Tunnel anhalten können (sollen). Außerdem besteht in der Eisenbahn / U-Bahn / S-Bahn, die Möglichkeit den Waggon zu wechseln und so aus der belästigenden Zone des Rauches zu entkommen.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Problemfall (Besondere Situation / Ereignis → planbarer Regelbetrieb).

Aktionen:

- Ein Fahrgast verhält sich unangemessen und/oder respektlos gegenüber anderen Fahrgästen, welche sich dadurch belästigt fühlen.
  - Rauchen trotz Rauchverbot → Verstoß gegen Nichtraucherschutz → Grund zur Beschwerde.
  - Laute Musik → Lärmbelästigung → Grund zur Beschwerde.
  - Verstoß gegen „Die Fahrgäste sind gehalten, sich ausreichenden Halt zu verschaffen und nicht an die Türen anzulehnen“, alternativ Gurtpflicht (sofern gegeben) nicht umgesetzt.
    → Gefährdung bei Fahrt / Unfall → Grund zur Beschwerde.
  - Blockieren der Tür → verhindert Abfahrt → Grund zur Beschwerde wegen Nötigung (Strafrecht).
  - Raub / Überfall → Kriminalität → Notruf.
- Ein anderer Fahrgast meldet das Fehlverhalten durch die Betätigung der
  - Kommunikation → Meldung des Ereignisses als Beschwerde über UC-23 Kommunikation mit Fahrgästen bei außergewöhnlichen Ereignissen.
  - Notruf → Meldung des Ereignisses / des Notfalls
  - Nothalt → Anforderung außerplanmäßiger Halt zum Verlassen des Fahrzeuges → UC-40 Nothalt.
- Die ÖV-Leitstelle nimmt die Meldung, sofern dieser durch die Kommunikation (über 11 → 7) ausgelöst wurde, entgegen und leitet geeignete Maßnahmen der Problemlösung ein. Dieses können sein, z.B.
  - ein Schlichtungsversuch,
  - Androhung von Bußgeld,
  - Aufforderung der Belästigung ausübenden Person, das Fahrzeug zu verlassen. (Verweigerung der weiteren Mitfahrt).
  - Oder
    Bieten der Möglichkeit zum Aussteigen des Fahrgastes, der sich belästigt fühlt (Wahrung der Grundrechte)
    Hinweis:
    Hierzu ist die Technische Aufsicht (TA) der AD-Leitstelle (über 3) einzubeziehen, da nur die Technische Aufsicht (TA) den außerplanmäßigen Halt als UC-28 Eingriffsnotwendigkeit Technische Aufsicht umsetzen kann.
  - Entsenden von Einsatzkräften (eigenes Personal / Polizei)
    Hinweis:
    Im Gegensatz zu Bahnhöfen oder (großen) Betriebshaltestellen gibt es beim autonomen Shuttle / Bus kein ÖPNV-Personal Vorort. Dieses müßte erst entsendet werden, hat jedoch weniger Befugnisse als die Polizei, weshalb die offiziellen Einsatzkräfte der Polizei hier angemessen sind.

  Hinweis:
  Die ÖV-Leitstelle kann auch (über 3) die Technische Aufsicht (TA) der AD-Leitstelle und damit das FG-Notfallmanagement (über 2 bzw. 20) mit einbinden.
- Die AD-Leitstelle nimmt den Notruf / Nothalt (über 16 → 8) entgegen, welcher automatisiert aufgezeichnet wird in Bild und Ton gemäß AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher (Abschnitt 13) und leitet geeignete Maßnahmen der Problemlösung ein. Diese können die, wie zuvor bei der ÖV-Leitstelle genannten möglichen Maßnahmen sein, allerdings hat die Technische Aufsicht (TA) der AD-Leitstelle mehr Handlungsmöglichkeiten als die ÖV-Leitstelle durch den direkten Zugriff auf das Fahrzeug → UC-28 Eingriffsnotwendigkeit Technische Aufsicht.
  Hinweis:
  Die Primäraufgabe der Technischen Aufsicht (TA) der AD-Leitstelle ist die Überwachung der autonomen Fahrt, weshalb die Technische Aufsicht (TA) der AD-Leitstelle, die Möglichkeit hat die Behandlung von Beschwerden an das FG-Notfallmanagement (über 20) einzubinden / abzugeben. Die ÖV-Leitstelle kann (über 3) optional zusätzlich eingebunden werden (3er Konferenzschaltung).
  Hinweis:
  Das Fahrgast-Notfallmanagement ist verantwortlich für die Kommunikation und -Betreuung in Notfall-Situationen. Dieses umfaßt Notfälle allgemeiner Art (z.B. ein medizinischer Notfall oder Kriminalität) als auch spezifische Notfallbehandlungen im Zusammenhang mit dem AD-Betrieb (z.B. ein Unfall oder eine Fahrzeugstörung). Die Kommunikation erfolgt entweder direkt und/oder indirekt über den Operator der Technischen Aufsicht (TA) der AD-Leitstelle zum Fahrzeug. Außerdem sind die Angehörigenbetreuung und ggf. Notfallseelsorge beim Fahrgast-Notfallmanagement angesiedelt.

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den

Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie in der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik, Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik über einen Abschluß verfügt als
  - Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert),
  - Bachelor, Master oder
  - staatlich geprüfter Techniker.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 2
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie eine entsprechende Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen hat.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 3
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muß, und
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 4
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihr anvertrauten Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes zuverlässig ist.
  Zur Beurteilung der Zuverlässigkeit im Sinne des Satzes 2 Nummer 4 sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde, eine Auskunft aus dem Fahrerlaubnisregister sowie eine Auskunft über Eintragungen aus dem Fahreignungsregister vorzulegen. Sofern in dem Fahrerlaubnisregister mehr als drei Punkte eingetragen sind, ist die Zuverlässigkeit nicht gegeben. § 8 Absatz 3 gilt bezüglich Satz 3 entsprechend.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 2
  Die als Technische Aufsicht eingesetzte natürliche Person darf sich mit Zustimmung des Halters zur Erfüllung ihrer Pflichten weiterer geeigneter natürlicher Personen bedienen, die über mindestens drei Jahre Berufserfahrung im Bereich des Verkehrs- oder Kraftfahrzeugwesens verfügen. Die eingesetzten natürlichen Personen müssen wiederkehrend, mindestens jedoch jährlich beim Hersteller in Bezug auf den Umgang mit dem Kraftfahrzeug sowie wesentliche Veränderungen am Kraftfahrzeug oder der autonomen Fahrfunktion geschult werden. Die Schulung ist mit einer praktischen Prüfung einschließlich der Bewältigung simulierter Betriebsstörungen abzuschließen. Der erfolgreiche Abschluß der Schulung von eingesetzten natürlichen Personen ist von der Technischen Aufsicht zu dokumentieren. Sollen die eingesetzten natürlichen Personen Fahrten im manuellen Fahrbetrieb übernehmen oder Fahrmanöver freigeben, müssen diese Personen eine gültige Fahrerlaubnis besitzen. Die Klasse der Fahrerlaubnis muß der des Fahrzeugs mit autonomer Fahrfunktion entsprechen.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 3
  Befindet sich das Kraftfahrzeug mit autonomer Fahrfunktion im risikominimalen Zustand im Sinne des § 1d Absatz 4 des Straßenverkehrsgesetzes, hat die als Technische Aufsicht eingesetzte natürliche Person eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durchzuführen, bevor sie dessen Beendigung veranlassen darf. Das Ergebnis der Untersuchung ist zu dokumentieren. Wurde der risikominimale Zustand durch einen Defekt am Kraftfahrzeug ausgelöst, muß nach Erreichen des risikominimalen Zustands die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage 1 Nummer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
  Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist ungeachtet der Sätze 1 und 3 das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen. In diesen Fällen erfolgt die Untersuchung der Technischen Aufsicht gemäß Satz 1 im Nachgang des Abtransports auf Grundlage der gespeicherten Fahrdaten.

- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
  Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
  Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse
  - 1) Keine Datenspeicherung bei autonomer Fahrt im festgelegten Betriebsbereich

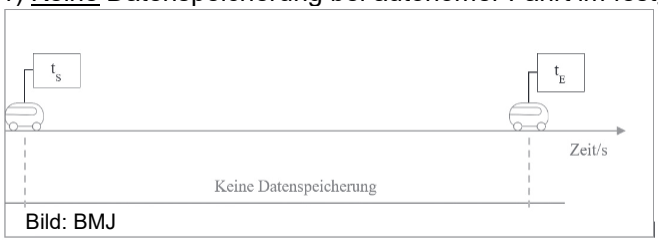


Bild: BMJ

  - 2) Datenspeicherung bei autonomer Fahrt im festgelegten Betriebsbereich mit Ereignis (bspw. Unfall)

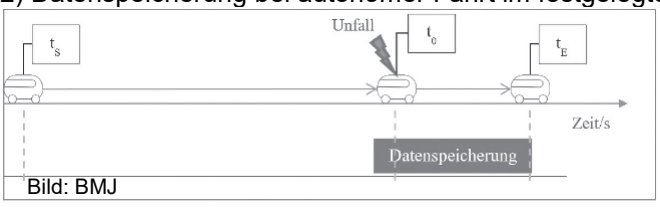


Bild: BMJ

  - 3) Datenspeicherung bei autonomer Fahrt im festgelegten Betriebsbereich mit Ereignis und anschließender Überführung des Kraftfahrzeuges in den risikominimalen Zustand

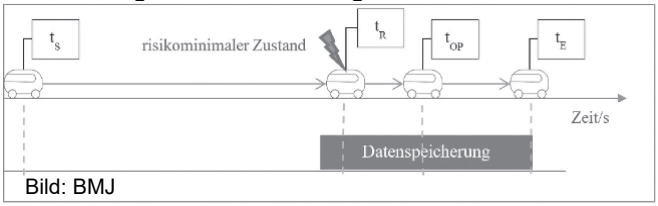


Bild: BMJ

  - Legende:
    - t_S Zeitpunkt – Beginn der Fahrt (Starten des Kraftfahrzeuges)
    - t_R Zeitpunkt – Auslösung des risikominimalen Zustands
    - t_0 Zeitpunkt – Unfallereignis
    - t_{0P} Zeitpunkt – Anforderung oder Eingabe der Technischen Aufsicht
    - t_E Zeitpunkt – Ende der Fahrt

- AFGBV Anlage 1 Teil 3 Abschnitt 13.2 Technische Vorgaben für das Speichern, Auslesen und Übertragen von Daten
  Das System der Datenspeicherung darf nicht flüchtig sein. Die gespeicherten Daten müssen im stromlosen Zustand erhalten bleiben.
  Ergänzende technische Anforderungen für den Datenspeicher
- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.
- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).
- AFGBV Anlage 1 Teil 1 Abschnitt 7.1 Betriebshandbuch
  Zweck des Betriebshandbuchs ist es, mittels detaillierter Vorgaben den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten und der Technischen Aufsicht die richtige Reaktion auf Fehlerfälle zu ermöglichen.
  Hinweis:
  AFGBV Anlage 3 Dokumentationspflichten des Herstellers Kapitel 2 spezifiziert die Anforderungen.

Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.
- BOStrab §3 Absatz 2
  Einrichtungen in Betriebsanlagen und Fahrzeugen, die für die Benutzung oder Betätigung durch Fahrgäste bestimmt sind, müssen gut erkennbar und leicht erreichbar sein. Ihre Handhabung muß sich sinnfällig erkennen lassen; Fehlbedienungen dürfen zu keiner Betriebsgefährdung führen.
  Hinweis:
  Einrichtungen (welche für die Nutzung durch Fahrgäste vorgesehen sind) müssen
  gut erkennbar, (d.h. der Verwendungszweck muß eindeutig und leicht verständlich / logisch)
  und leicht erreichbar (behindertengerecht und für Kinder geeignet) sein.
- BOStrab §4 Absatz 4
  Durch betriebliche Vorkehrungen ist dafür zu sorgen, daß Betriebsstörungen zügig beseitigt werden, bei Unfällen und gefährlichen Ereignissen unverzüglich Hilfe geleistet wird und insbesondere bei Brandfällen die Möglichkeit zur Selbst- oder Fremdrettung von Personen oder eine Kombination von beidem in Abhängigkeit von den lokalen Verhältnissen besteht.
- BOStrab §7 Absatz 2
  Der Unternehmer ist verpflichtet, bei der Auswahl, Aus- und Fortbildung, Verwendung und Beaufsichtigung der Betriebsbediensteten die Sorgfalt anzuwenden, die eine sichere und ordnungsgemäße Beförderung von Personen erfordert.
- BOStrab §23 Absatz 1
  Für die Verständigung von Betriebsbediensteten mit Betriebsstellen müssen im betriebsnotwendigen Umfang nachrichtentechnische Anlagen vorhanden sein. Besonders wichtige Meldungen an zentrale Betriebsstellen sollen vorrangig übermittelt werden können.
- BOStrab §23 Absatz 3
  Bei Fahrbetrieb ohne Fahrzeugführer müssen nachrichtentechnische Anlagen vorhanden sein, die eine vorrangige Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle ermöglichen.
- BOStrab §43 Absatz 6
  Türen müssen in geschlossener Stellung festgehalten sein. Sie müssen jedoch von Fahrgästen im Notfall geöffnet werden können.
- BOStrab §46 Absatz 4
  Fahrzeuge müssen Einrichtungen für eine Sprechverbindung zwischen Fahrzeugführer und einer Betriebsstelle haben. Notfall-Informationen müssen vorrangig durchgegeben werden können.

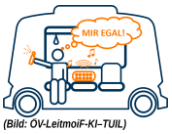
- BOStrab §46 Absatz 5
  Personenfahrzeuge eines Zuges, die nicht mit Betriebsbediensteten besetzt sind, müssen ständig verfügbare Einrichtungen für eine Notfall-Sprechverbindung zwischen Fahrgästen und dem Fahrzeugführer haben. ➔ Die AD-Leitstelle ist der Fahrzeugführer im automatisierten *(Remote-Sicherheitsfahrer bei ≤ SAE 3)* / autonomen *(≥ SAE4)* Betrieb.
  Hinweis: Im konventionellen Betrieb befindet sich der Sicherheitsfahrer im Fahrzeug.
- BOStrab §46 Absatz 6
  Bei Fahrbetrieb ohne Fahrzeugführer müssen Personenfahrzeuge Einrichtungen für eine Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle haben. Absatz 4 Satz 2 gilt entsprechend.
- BOStrab §52 Absatz 3
  Betriebsanlagen oder Fahrzeuge, die ganz oder teilweise selbsttätig arbeiten oder fernbedient werden, müssen im Rahmen der betrieblichen Erfordernisse von Betriebsbediensteten auf einwandfreie Funktion überwacht werden.
- BOStrab §54 Absatz 3
  Personenzüge dürfen nur so beschleunigt und nur so gebremst werden, daß Fahrgäste nicht mehr als unvermeidbar gefährdet werden.

Einbindung juristischer Vorgaben auf straßengebundenen Verkehrssysteme.

- StGB § 34 Rechtfertigender Notstand
  Wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, handelt nicht rechtswidrig, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Dies gilt jedoch nur, soweit die Tat ein angemessenes Mittel ist, die Gefahr abzuwenden.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.



(Bild: ÖV-LeitmotiF-KI-TUIL)

- Die potentiellen Gefahren entsprechen den typischen Gefahren der Teilnahme am Straßenverkehr mit Interaktion zu anderen Menschen, welche jedoch sehr vielschichtig und stark unterschiedlich in ihrer Gefährdung sein können, abhängig von der Art des Problems / der (Verhaltens-)Störung, weshalb deren Sicherheitsrelevanz von QM bis ASIL-D (schwer beherrschbar) oder darüber hinaus nicht beherrschbar, (z.B. Terroranschlag) reicht.
  - ► Die Sicherheitsrelevanz des Regelprozesses für die Kommunikation wird bewertet als Szenario *(best case)*.
  - ► Die Sicherheitsrelevanz des Regelprozesses für den Notruf / Nothalt wird bewertet als Szenario *(worse case)*.
    Hinweis: Hier nicht worst case, es kann schlimmere Ereignisse / Vorfälle geben.

Risikograph (worse case ≙ Notfall):

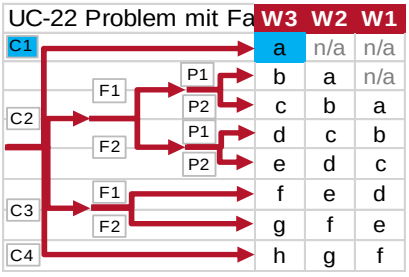
UC-22 Problem mit Fa			W3	W2	W1
C1			a	n/a	n/a
	F1	P1	b	a	n/a
		P2	c	b	a
C2		P1	d	c	b
	F2	P2	e	d	c
	F1		f	e	d
C3	F2		g	f	e
C4			h	g	f

≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C4	Die Range der Ereignisse reicht von C1 (best case) bis C4 (worse case) ■ C1 Geringe Verletzung ■ C2 schwere irreversible Verletzung einer oder mehrerer Personen inkl. Tod einer einzigen Person ■ C3 Tod mehrerer Personen ■ C4 Tod vieler Personen *(es gibt keine quantitative Angabe von „viele“ versus „mehrere“)* *Hinweis:* *C4 ergibt sich z.B. bei einem Amoktäter.*
✖	
✖	
W1	Die Range der Ereignisse reicht von W1 (best case) bis W3 (worse case), aber die Wahrscheinlichkeit (W) des Auftretens verhält sich reziprok zur Auswirkung (C). *Hinweis:* *Notfall = worse case, wegen der Schwere, deshalb selten, also W1.*

Risikograph (best case):



≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Die Range der Ereignisse reicht von C1 (best case) bis C4 (worse case) ■ C1 Geringe Verletzung ■ C2 schwere irreversible Verletzung einer oder mehrerer Personen inkl. Tod einer einzigen Person ■ C3 Tod mehrerer Personen ■ C4 Tod vieler Personen *(es gibt keine quantitative Angabe von „viele“ versus „mehrere“)*
✖	
✖	
W3	Die Range der Ereignisse reicht von W1 (best case) bis W3 (worse case), aber die Wahrscheinlichkeit (W) des Auftretens verhält sich reziprok zur Auswirkung (C) *Hinweis:* *best case Szenario, somit geringe Schwere C1, deshalb häufiger, also W3.*

3.2.23 UC-23 Kommunikation mit Fahrgästen bei außergewöhnlichen Ereignissen

Im Verlauf einer (Regel-)Fahrt tritt ein außergewöhnliches und unvorhersehbares Ereignis (Unfall, Schaden am Fahrzeug, schwerwiegende Störung, …) oder ein Notfall ein.

Im automatisierten Betrieb können die Ereignisse bzw. Notfälle von einem Fahrgast, der Fahrzeugperipherie, den Mitarbeiterinnen bzw. Mitarbeitern der AD-Leitstelle oder der ÖV-Leitstelle erkannt werden. Im nachfolgenden Schritt wird eine Kommunikation zwischen Fahrgastnotfallmanagement und den Fahrgästen aufgebaut, bevor Maßnahmen festgelegt werden.

Standardablauf

I. Eine außergewöhnliche Situation oder ein Notfall tritt ein

II. Ein Fahrgast, die Fahrzeugperipherie oder ein Mitarbeiter / eine Mitarbeiterin der AD- oder ÖV-Leitstelle erkennt eine außergewöhnliche Situation und meldet dies dem FG-Notfallmanagement.
Hinweis:
Die Fahrzeugperipherie erkennt keine außergewöhnliche Situation, sondern eine Störung.
Die ÖV-Leitstelle erkennt eine Fahrplanabweichung, auch eine potentielle, durch die Meldung von Stau oder Straßensperrung.
Beides ist kein Notfall, sondern erfordert eine logistische Anpassung / dispositive Maßnahme.
Ausnahme: Eine polizeiliche Suchmeldung für eine erkrankte, zu quarantänisierende Person wird durch die Auswertung der statistischen Daten, mittels persönlichem Fahrschein / Bahncard, im Rahmen einer Fahndungsunterstützung, als aktueller Mitfahrer in einem Fahrzeug identifiziert, dann kann auch die ÖV-Leitstelle einen Notfall auslösen und die Quarantäne für das Fahrzeug anordnen, sowie die Einsatzkräfte dorthin beordern.
Hinweis:
Es gibt keine direkte Verbindung zwischen Fahrgast und FG-Notfallmanagement.
Die Verbindung über den Knopf Kommunikation läuft über das Fahrgast HMI ÖV (über 11) zum ÖV-Bordrechner und anschließend (über 7) zur ÖV-Leitstelle. Sofern erforderlich, im Falle einer Fehlbedienung, (d.h. Meldung eines Notfalls über die Kommunikationstaste statt dem Notruf), erfolgt sowohl (über 3) die Einbindung der Technischen Aufsicht (TA) der AD-Leitstelle, als ggf. auch (über 2 bzw. 20), sofern zweckmäßig, die Einbindung des FG-Notfallmanagements.
Die Verbindung Notruf / Nothalt läuft über das Fahrgast HMI AD (über 16) zum AD-Bordsystem und von dort (über 8) zur AD-Leitstelle, welche die Kommunikation in Bild und Ton aufzeichnet (Beweisführung). Die Technische Aufsicht (TA) der AD-Leitstelle kann (über 20) das FG-Notfallmanagement und optional (über 3) die ÖV-Leitstelle einbinden.

III. Das FG-Notfallmanagement baut eine bidirektionale Kommunikation mit den Fahrgästen auf bzw. entscheidet über das weitere Vorgehen.
Hinweis:
Das hängt von den Prozessen des ÖPNV selbst und deren Konferenzschaltungsmöglichkeiten der Leitstellen ab.
Erst wenn die Technische Aufsicht (TA) der AD-Leitstelle bei Notruf / Nothalt die Zuständigkeit abgegeben hat bzw., wenn die ÖV-Leitstelle bei Kommunikation die Zuständigkeit abgegeben / übertragen hat, ist das FG-Notfallmanagement zuständig.

IV. Das FG-Notfallmanagement entscheidet, ob ein Nothalt durchgeführt werden muß.
Hinweis:
Sofern ein Fahrgast einen außerplanmäßigen Halt angefordert hat um der Belästigung eines anderen Fahrgasts zu entgehen, darf (StGB §239 Freiheitsberaubung) dieses nicht verweigert werden, somit liegt die Entscheidung beim Fahrgast.
Hinweis:
Eine Freiheitsberaubung gemäß StGB §239 Absatz 1 „auf andere Weise“ liegt auch dann vor, wenn einem Anderen die Fortbewegungsfreiheit, sei es auch nur vorübergehend, die Möglichkeit genommen wird, einen Raum zu verlassen. Dazu zählt auch das Hindern eines Fahrzeuginsassen am Verlassen des Wagens, welches durch schnelles Fahren mit einem Fahrzeug begangen werden kann, sofern der Fahrzeugführer, entgegen der ausdrücklichen Aufforderung eines Fahrzeuginsassen, den eindeutigen und unmißverständlichen Wunsch zum Ausdruck bringt, das Fahrzeug unter den gegebenen Umständen verlassen zu wollen, nicht nachkommt (Widerrufs eines ursprünglich erteilten Einverständnisses in die Beförderung mit dem Fahrzeug)
Quelle: BGH, Urt. v. 20.1.2005 - 4 StR 366/04 - NStZ 2005, 507.
Hinweis:
Sofern ein belästigender Fahrgast die Aufforderung der Unterlassung verweigert, sind Ordnungskräfte zur Wiederherstellung der Ordnung zu entsenden. Da Shuttle / Bus im Straßenverkehr fahren und nicht von einem Bahnhof oder mit einer von ÖPNV-Mitarbeitern besetzten Haltestelle abhängig sind, können (aufgrund der Befugnisse) Einsatzkräfte der Polizei effizient eingreifen. In beiden Fällen ist kein Nothalt zwingend erforderlich, es reicht ein normales Anhalten unter Wahrung der gesetzlich beschränkten negativen Beschleunigung von $a = -2{,}4 m/s^2$ gefordert für stehende oder nicht angegurtete Fahrzeuginsassen.
Hinweis:
Sofern ein Fahrgast während der Fahrt die geschlossenen Türen gewaltsam aufbricht, wird ein Nothalt über das Minimum Risk Manoeuvre (MRM) des Fahrzeuges (OEM) bzw. das AD-Bordsystem eingeleitet.

V. Das Fahrzeug wird bei Bedarf evakuiert.

VI. Weitere (Notfall-) Maßnahmen werden eingeleitet.

Zur besseren Verdeutlichung und Lesbarkeit wird der Use Case in die folgenden drei Teile zerlegt:

A. Meldung von außergewöhnlichen Ereignissen

B. Kommunikation mit Fahrgästen bei außergewöhnlichen Ereignissen

C. Festlegung von Maßnahmen bei außergewöhnlichen Ereignissen

Hinweis:
Ende der Originalbeschreibung, reale Beschreibung siehe Aktionen, teilweise auch die folgenden Hinweise.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Sofern der (außergewöhnliches) Ereignis erkennende Fahrgast den Knopf Kommunikation verwendet, wird die ÖV-Leitstelle kontaktiert, welche die Meldung / Rückfrage entgegennimmt und geeignete Maßnahmen einleitet. *Hinweis:* *Die ÖV-Leitstelle kann sowohl die Technische Aufsicht (TA) der AD-Leitstelle und damit das FG-Notfallmanagement mit einbinden, als auch die Zuständigkeit / Verantwortung übergeben.*	Problemlösung, bis Abgabe / Weiterleitung.
BHMS	keine	keine
AD-Leitstelle	Sofern der (außergewöhnliches) Ereignis erkennende Fahrgast den Knopf Notfall / Nothalt verwendet wird die AD-Leitstelle kontaktiert, welche die Meldung entgegennimmt und geeignete Maßnahmen einleitet. *Hinweis:* *Die AD-Leitstelle kann sowohl das FG-Notfallmanagement und/oder die ÖV-Leitstelle mit einbinden, als auch die Zuständigkeit / Verantwortung übergeben.*	Problemlösung, bis Abgabe / Weiterleitung.

Hinweis:
Dieser UseCase hängt von der Bedienung durch den Fahrgast selbst ab, je nachdem ob dieser den Knopf „Kommunikation“ oder „Notruf“ / „Nothalt“ anwendungsgemäß korrekt verwendet.

Hinweis:
Der Kommunikationsknopf ist gedacht für den Fahrgast um Rückfragen und Meldungen abzugeben, welche im konventionellen Betrieb durch den Fahrer umgesetzt würden, dazu zählen

- *Rückfrage, z.B. Fährt dieses Fahrzeug nach …*
- *Meldung Fundsache (Buch, Tablet, Regenschirm, Portemonnaie, …)*
- *Beschwerde z.B. Verschmutzung, unangemessenes Benehmen Mitreisender, …*

Der Notruf ist gedacht für den Fahrgast um Notlagen zu melden, welche im konventionellen Betrieb durch den Fahrer behandelt würden, dazu zählen

- *Meldung medizinischer Notlage, z.B. einem Fahrgast ist übel, schwindelig, … oder auch ein anderer Fahrgast ist zusammengesackt*
- *Bedrohung durch Mitreisende (Nötigung, Raub, Kriminalität, Taschendiebstahl, …)*

Der Nothalt ist gedacht für den Fahrgast um ein umgehendes Anhalten anzufordern, welche im konventionellen Betrieb durch den Fahrer umgesetzt würde, dazu zählen

- *Fahrgast befindet sich im Fahrzeug, aber der Hund an der Leine ist noch außerhalb und die Türen wurden geschlossen bevor das Tier zusteigen konnte → Vermeidung zum Schutze des Tierwohls, d.h. ein Mitschleifen verhindern.*
- *Kinderwagen wurde bereits in das Fahrzeug gewuchtet, aber die Türen haben sich geschlossen bevor die Begleitperson zusteigen konnte.*

Hinweis:
Die Möglichkeit der Fehlbedienung durch den Fahrgast, insbesondere bei „Notruf“ und „Nothalt“ ist durch geeignete Maßnahmen abzufangen.

Hinweis:
Sollte die ÖV-Leitstelle, beim Kommunikationsablauf, Kamerabilder aus dem Fahrzeug zur Situationsanalyse benötigen, so ist dieses beschrieben in UC-24 Fundsachen und Sauberkeit im Fahrzeug.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Ereignisfall (Besondere Situation / Ereignis → planbarer Regelbetrieb).

Aktionen:

- Ein Fahrgast bemerkt ein außergewöhnliches Ereignis und meldet dieses über die
  - Kommunikation → Meldung des Ereignisses (Rückfrage / Meldung / Beschwerde).
  - Notruf → Meldung des Ereignisses / des Notfalls / der Notlage

(Bild: ÖV-LeitmoiF-KI-TUIL)

  - Nothalt → Anforderung außerplanmäßiger Halt zum Verlassen des Fahrzeuges → UC-40 Nothalt.
- Sofern die Meldung über die Kommunikation (über 11 → 7) erfolgt, nimmt die ÖV-Leitstelle diese entgegen und leitet geeignete Maßnahmen der Problemlösung ein. Diese können sein, z.B.
  - Beantwortung der Fragen zum Fahrplan, Unterstützung bei der Reiseroute, ….
  - Meldung von Verschmutzung / Fundsache → UC-24 Fundsachen und Sauberkeit im Fahrzeug.
  - Beschwerde → UC-22 Problem mit Fahrgast (störendes Verhalten).
- Die AD-Leitstelle nimmt den Notruf / Nothalt (über 16 → 8) entgegen, welcher automatisiert aufgezeichnet wird in Bild und Ton gemäß AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher (Abschnitt 13), und leitet geeignete Maßnahmen der Problemlösung ein.
  - Beantwortung der Frage(n), sofern bekannt, ggf. Weiterleitung (über 3) an ÖV-Leitstelle bei Fragen zum Fahrplan oder Servicewunsch bzgl. Unterstützung bei der Reiseroute bei Fehlbedienung.
  - Geeignete Maßnahmen zur Behebung / Minderung einer Notlage (Notruf) sind abhängig von der Notlage selbst, d.h. bei Kriminalität (Meldung Taschendiebstahl, Bedrohung, Raub) werden die Zivilstreitkräfte der Polizei (110), bei einem medizinischen Notfall der Rettungsdienst oder die Feuerwehr (112) bzw. der ärztliche Bereitschaftsdienst (116117) informiert. Sofern die Notlage nicht die autonome Fahrt betrifft, kann die Bearbeitung (über 20) an das Fahrgast-Notfallmanagement weitergeleitet / übergeben bzw. diese mit eingebunden werden. (Dort ist auch die psychologische Betreuung und/oder die Ersthelfer angesiedelt).
    Hinweis:
    Psychologische Betreuung durch geschultes Personal ist hilfreich bei randalierenden ggf. betrunkenen Fahrgästen und notwendig bei Amoklauf. Bei letzterem oder medizinischem Notfall gehört ggf. auch die Angehörigenbetreuung der im Fahrzeug befindlichen Fahrgäste dazu.
  - Bei der Anforderung eines Nothalts wird automatisch ein Minimum Risk Manoeuvre (MRM) umgesetzt, welches eine Untersuchung des Vorfalles durch die Technische Aufsicht (TA) der AD-Leitstelle mit der Dokumentation des Ergebnisses (Nachweispflicht) zur Folge hat. Sofern eine Weiterfahrt zulässig ist, darf ausschließlich die Technische Aufsicht (TA) der AD-Leitstelle die Beendigung des Minimum Risk Manoeuvres (MRM) veranlassen.
    Der Nothalt ist eine Erweiterung des Notfalles, welcher neben der Behandlung des Notfalles (s.o.) ein automatisiertes Anhalten des Fahrzeuges über ein Minimum Risk Manoeuvre (MRM) umsetzt. Das Minimum Risk Manoeuvre (MRM) führt in Abhängigkeit der Situationsparameter einen sofortigen Halt oder einen Halt an geeigneter Stelle durch.
    Hinweis:
    Bei einem Minimum Risk Manoeuvre (MRM) ist unabhängig von der Kategorie (A bis E) der Warnblinker zu aktivieren und die technische Aufsicht (TA) der AD-Leitstelle ist verpflichtet unverzüglich Kontakt mit den Insassen des Kraftfahrzeugs herzustellen.
    Sofern kein Notfall vorliegen sollte (z.B. bei Fehlbedienung) kann die Technische Aufsicht (TA) der AD-Leitstelle dieses direkt behandeln (sinnvoll bei kurz zu beantwortenden Fragen) oder Weiterleiten (sinnvoll, wenn die Behandlung / Problemlösung von der Überwachung der Fahrt ablenkt). In beiden Fällen ist der Vorfall zu untersuchen und das Ergebnis zu dokumentieren, bevor das Minimum Risk Manoeuvre (MRM) durch die Technische Aufsicht (TA) der AD-Leitstelle aufgehoben werden darf.

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie

informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie in der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik, Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik über einen Abschluß verfügt als
  - Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert),
  - Bachelor, Master oder
  - staatlich geprüfter Techniker.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 2
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie eine entsprechende Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen hat.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 3
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muß, und
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 4
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihr anvertrauten Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes zuverlässig ist.
  Zur Beurteilung der Zuverlässigkeit im Sinne des Satzes 2 Nummer 4 sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde, eine Auskunft aus dem Fahrerlaubnisregister sowie eine Auskunft über Eintragungen aus dem Fahreignungsregister vorzulegen. Sofern in dem Fahrerlaubnisregister mehr als drei Punkte eingetragen sind, ist die Zuverlässigkeit nicht gegeben. § 8 Absatz 3 gilt bezüglich Satz 3 entsprechend.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 2
  Die als Technische Aufsicht eingesetzte natürliche Person darf sich mit Zustimmung des Halters zur Erfüllung ihrer Pflichten weiterer geeigneter natürlicher Personen bedienen, die über mindestens drei Jahre Berufserfahrung im Bereich des Verkehrs- oder Kraftfahrzeugwesens verfügen. Die eingesetzten natürlichen Personen müssen wiederkehrend, mindestens jedoch jährlich beim Hersteller in Bezug auf den Umgang mit dem Kraftfahrzeug sowie wesentliche Veränderungen am Kraftfahrzeug oder der autonomen Fahrfunktion geschult werden. Die Schulung ist mit einer praktischen Prüfung einschließlich der Bewältigung simulierter Betriebsstörungen abzuschließen. Der erfolgreiche Abschluß der Schulung von eingesetzten natürlichen Personen ist von der Technischen Aufsicht zu dokumentieren. Sollen die eingesetzten natürlichen Personen Fahrten im manuellen Fahrbetrieb übernehmen oder Fahrmanöver freigeben, müssen diese Personen eine gültige Fahrerlaubnis besitzen. Die Klasse der Fahrerlaubnis muß der des Fahrzeugs mit autonomer Fahrfunktion entsprechen.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 3
  Befindet sich das Kraftfahrzeug mit autonomer Fahrfunktion im risikominimalen Zustand im Sinne des § 1d Absatz 4 des Straßenverkehrsgesetzes, hat die als Technische Aufsicht eingesetzte natürliche Person eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durchzuführen, bevor sie dessen Beendigung veranlassen darf. Das Ergebnis der Untersuchung ist zu dokumentieren. Wurde der risikominimale Zustand durch einen Defekt am Kraftfahrzeug ausgelöst, muß nach Erreichen des risikominimalen Zustands die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage 1 Nummer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
  Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist ungeachtet der Sätze 1 und 3 das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen. In diesen Fällen erfolgt die Untersuchung der Technischen Aufsicht gemäß Satz 1 im Nachgang des Abtransports auf Grundlage der gespeicherten Fahrdaten.

- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
  Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
  Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse
  - 1) Keine Datenspeicherung bei autonomer Fahrt im festgelegten Betriebsbereich

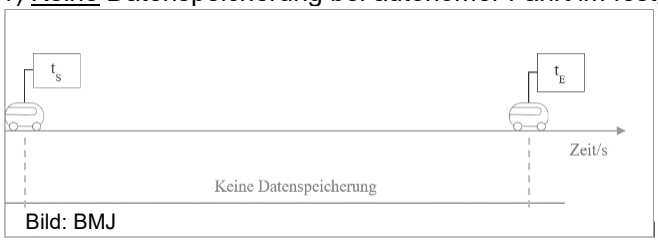


Bild: BMJ

  - 2) Datenspeicherung bei autonomer Fahrt im festgelegten Betriebsbereich mit Ereignis (bspw. Unfall)

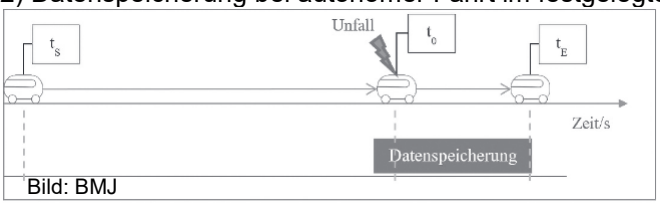


Bild: BMJ

  - 3) Datenspeicherung bei autonomer Fahrt im festgelegten Betriebsbereich mit Ereignis und anschließender Überführung des Kraftfahrzeuges in den risikominimalen Zustand

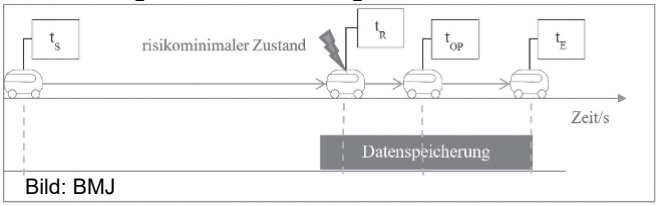


Bild: BMJ

  - Legende:
    - t_S Zeitpunkt – Beginn der Fahrt (Starten des Kraftfahrzeuges)
    - t_R Zeitpunkt – Auslösung des risikominimalen Zustands
    - t_0 Zeitpunkt – Unfallereignis
    - t_{0P} Zeitpunkt – Anforderung oder Eingabe der Technischen Aufsicht
    - t_E Zeitpunkt – Ende der Fahrt

- AFGBV Anlage 1 Teil 3 Abschnitt 13.2 Technische Vorgaben für das Speichern, Auslesen und Übertragen von Daten
  Das System der Datenspeicherung darf nicht flüchtig sein. Die gespeicherten Daten müssen im stromlosen Zustand erhalten bleiben.
  Ergänzende technische Anforderungen für den Datenspeicher
- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.
- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).
- AFGBV Anlage 1 Teil 1 Abschnitt 7.1 Betriebshandbuch
  Zweck des Betriebshandbuchs ist es, mittels detaillierter Vorgaben den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten und der Technischen Aufsicht die richtige Reaktion auf Fehlerfälle zu ermöglichen.
  Hinweis:
  AFGBV Anlage 3 Dokumentationspflichten des Herstellers Kapitel 2 spezifiziert die Anforderungen.

Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.
- BOStrab §3 Absatz 2
  Einrichtungen in Betriebsanlagen und Fahrzeugen, die für die Benutzung oder Betätigung durch Fahrgäste bestimmt sind, müssen gut erkennbar und leicht erreichbar sein. Ihre Handhabung muß sich sinnfällig erkennen lassen; Fehlbedienungen dürfen zu keiner Betriebsgefährdung führen.
  Hinweis:
  Einrichtungen (welche für die Nutzung durch Fahrgäste vorgesehen sind) müssen
  gut erkennbar, (d.h. der Verwendungszweck muß eindeutig und leicht verständlich / logisch)
  und leicht erreichbar (behindertengerecht und für Kinder geeignet) sein.
- BOStrab §4 Absatz 4
  Durch betriebliche Vorkehrungen ist dafür zu sorgen, daß Betriebsstörungen zügig beseitigt werden, bei Unfällen und gefährlichen Ereignissen unverzüglich Hilfe geleistet wird und insbesondere bei Brandfällen die Möglichkeit zur Selbst- oder Fremdrettung von Personen oder eine Kombination von beidem in Abhängigkeit von den lokalen Verhältnissen besteht.
- BOStrab §7 Absatz 2
  Der Unternehmer ist verpflichtet, bei der Auswahl, Aus- und Fortbildung, Verwendung und Beaufsichtigung der Betriebsbediensteten die Sorgfalt anzuwenden, die eine sichere und ordnungsgemäße Beförderung von Personen erfordert.
- BOStrab §23 Absatz 1
  Für die Verständigung von Betriebsbediensteten mit Betriebsstellen müssen im betriebsnotwendigen Umfang nachrichtentechnische Anlagen vorhanden sein. Besonders wichtige Meldungen an zentrale Betriebsstellen sollen vorrangig übermittelt werden können.
- BOStrab §23 Absatz 3
  Bei Fahrbetrieb ohne Fahrzeugführer müssen nachrichtentechnische Anlagen vorhanden sein, die eine vorrangige Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle ermöglichen.
- BOStrab §43 Absatz 6
  Türen müssen in geschlossener Stellung festgehalten sein. Sie müssen jedoch von Fahrgästen im Notfall geöffnet werden können.
- BOStrab §46 Absatz 4
  Fahrzeuge müssen Einrichtungen für eine Sprechverbindung zwischen Fahrzeugführer und einer Betriebsstelle haben. Notfall-Informationen müssen vorrangig durchgegeben werden können.

- BOStrab §46 Absatz 5
  Personenfahrzeuge eines Zuges, die nicht mit Betriebsbediensteten besetzt sind, müssen ständig verfügbare Einrichtungen für eine Notfall-Sprechverbindung zwischen Fahrgästen und dem Fahrzeugführer haben. ➔ Die AD-Leitstelle ist der Fahrzeugführer im automatisierten *(Remote-Sicherheitsfahrer bei ≤ SAE 3)* / autonomen *(≥ SAE4)* Betrieb.
  Hinweis: Im konventionellen Betrieb befindet sich der Sicherheitsfahrer im Fahrzeug.
- BOStrab §46 Absatz 6
  Bei Fahrbetrieb ohne Fahrzeugführer müssen Personenfahrzeuge Einrichtungen für eine Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle haben. Absatz 4 Satz 2 gilt entsprechend.
- BOStrab §52 Absatz 3
  Betriebsanlagen oder Fahrzeuge, die ganz oder teilweise selbsttätig arbeiten oder fernbedient werden, müssen im Rahmen der betrieblichen Erfordernisse von Betriebsbediensteten auf einwandfreie Funktion überwacht werden.
- BOStrab §54 Absatz 3
  Personenzüge dürfen nur so beschleunigt und nur so gebremst werden, daß Fahrgäste nicht mehr als unvermeidbar gefährdet werden.

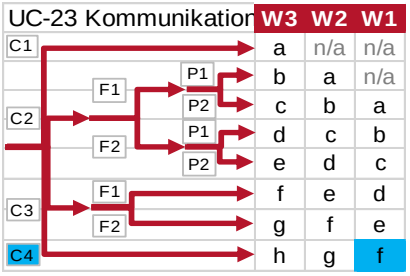
Einbindung juristischer Vorgaben auf straßengebundenen Verkehrssysteme.

- StGB § 34 Rechtfertigender Notstand
  Wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, handelt nicht rechtswidrig, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Dies gilt jedoch nur, soweit die Tat ein angemessenes Mittel ist, die Gefahr abzuwenden.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.
- Die potentiellen Gefahren entsprechen den typischen Gefahren der Teilnahme am Straßenverkehr inklusive der Interaktion mit anderen Menschen, welche jedoch sehr vielschichtig und stark unterschiedlich in ihrer Gefährdung sein können, abhängig von der Art der Interaktion, des Verhaltens bzw. des Problems / der (Verhaltens-)Störung, weshalb deren Sicherheitsrelevanz von QM bis ASIL-D (schwer beherrschbar) oder darüber hinaus nicht beherrschbar, (z.B. Terroranschlag) reicht, aber Vorfälle schwerer Art treten glücklicherweise (gemäß der Statistik) nur selten (reziprok) auf.
  - ► Die Sicherheitsrelevanz des Regelprozesses für die Kommunikation wird bewertet als Szenario (best case)
  - ► Die Sicherheitsrelevanz des Regelprozesses für den Notruf / Nothalt wird bewertet als Szenario (worse case).

Risikograph (worse case):

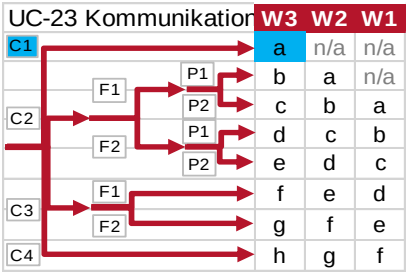


≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C4	Die Range der Ereignisse reicht von C1 (best case) bis C4 (worse case) ■ C1 Geringe Verletzung ■ C2 schwere irreversible Verletzung einer oder mehrerer Personen inkl. Tod einer einzigen Person ■ C3 Tod mehrerer Personen ■ C4 Tod vieler Personen *(es gibt keine quantitative Angabe von „viele“ versus „mehrere“)*
✖	
✖	
W1	Die Range der Ereignisse reicht von W1 (best case) bis W3 (worse case), aber die Wahrscheinlichkeit (W) des Auftretens verhält sich reziprok zur Auswirkung (C)

Risikograph (best case):



≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Die Range der Ereignisse reicht von C1 (best case) bis C4 (worse case) ■ C1 Geringe Verletzung ■ C2 schwere irreversible Verletzung einer oder mehrerer Personen inkl. Tod einer einzigen Person ■ C3 Tod mehrerer Personen ■ C4 Tod vieler Personen *(es gibt keine quantitative Angabe von „viele“ versus „mehrere“)*
✖	
✖	
W3	Die Range der Ereignisse reicht von W1 (best case) bis W3 (worse case), aber die Wahrscheinlichkeit (W) des Auftretens verhält sich reziprok zur Auswirkung (C)

3.2.24 UC-24 Fundsachen und Sauberkeit im Fahrzeug

Verschmutzungen im oder am Fahrzeug können beispielweise durch Wettereinflüsse (Winter: Streusalz oder Streusplitt) entstehen. Ferner können Verschmutzungen beabsichtigt (z.B. durch Beschmieren) oder unbeabsichtigt (z.B. Verschüttetes oder Erbrochenes) durch Fahrgäste verursacht werden. Abhängig von der Art und vom Umfang der Verschmutzung werden unterschiedliche Maßnahmen ergriffen. Die Spanne reicht von der Reinigung durch das Fahrpersonal (im konventionellen Betrieb) bei kleineren Verschmutzungen bis zum Austausch des Fahrzeuges.

Als Fundsachen werden persönliche Gegenstände wie beispielsweise Mobiltelefone, Portemonnaies, Regenschirme oder Rücksäcke bezeichnet, welche von einem Fahrgast in einem Fahrzeug oder an einer Haltestelle unbeabsichtigt zurückgelassen werden.

Der Fahrgast meldet eine Verschmutzung im / am Fahrzeug oder eine Fundsache im Fahrzeug.
In der ÖV-Leitstelle wird die Meldung geprüft und ggf. via Kameraüberwachung verifiziert.
Ferner kann das Leitstellenpersonal die Fahrgäste kontaktieren. Auf Basis der Informationen wird entschieden, ob ausgetauscht werden muss (Bereitstellung Ersatzfahrzeug) oder ein mobiles Serviceteam die Verschmutzung beseitigt bzw. die Fundsache sicherstellt. In diesem Fall ggf. Weiter mit Use Cases Dispositive Maßnahmen.

I. Fundsache bzw. Verschmutzung wird durch Fahrgast gemeldet

II. Leitstellenpersonal prüft Meldung ggf. via Kameraüberwachung (AD-Leitstelle)

III. Ggf. Rücksprache der Leitstelle mit dem Fahrgast

Leitstellenpersonal legt Maßnahmen fest.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Meldung entgegennehmen und geeignete Maßnahmen zur Lösung/Behebung einleiten.	Problemlösung
BHMS	keine *Hinweis:* *In dem betrachteten Fall erfolgt die Meldung von Fundsachen oder Beschwerde wegen Verschmutzung über die spezifische App des ÖPNV-Unternehmens.*	keine
AD-Leitstelle	Sofern die ÖV-Leitstelle Kamerabilder aus dem Fahrzeug anfordert, stellt die Technische Aufsicht der AD-Leitstelle die Verbindung her und übermittelt diese.	keine

Hinweis:
Die Behandlung von Fundsachen und Reinigung erfolgt im BHMS mit UC-07 Fahrzeug abrüsten.
Die Behandlung von Fundsachen und Reinigung über die Kommunikation des Fahrzeuges erfolgt mit UC-23 Kommunikation mit Fahrgästen bei außergewöhnlichen Ereignissen.
UC-24 beschreibt die Behandlung von Fundsachen und Reinigung via App
plus beschreibt den Erweiterten Ablauf von UC-23, wenn die ÖV-Leitstelle Kamerabilder zur Verifikation der Situation benötigt.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Für die App gilt zusätzlich, daß die Richtlinien der BDSG, DSGVO, der IT-Sicherheit und des Virenschutzes eingehalten werden.

Situation:
Besondere Situation / Ereignis (Sonderfall → planbarer Regelbetrieb).

Aktionen:

- Ein Fahrgast bemerkt ein außergewöhnliches Ereignis (Fundsache / Verschmutzung) und meldet dieses über die spezifische App des ÖPNV-Unternehmens.
- Die ÖV-Leitstelle nimmt die Meldung über die App entgegen und leitet geeignete Maßnahmen nach der Überprüfung der Meldung ein.
  - Die ÖV-Leitstelle fordert eine Videoverbindung (über 3) bei der AD-Leitstelle an.
  - Die Technische Aufsicht der AD-Leitstelle informiert (Datenschutz) die Fahrgäste im Fahrzeug über die Kameraübertragung und aktiviert diese (über 15) mittels dem Operator HMI AD.

- ► Das AD-Bordsystem übermittelt das Videosignal (UM0.15.3 CamaraImage) vom Operator HMI AD (über 8) an die AD-Leitstelle, welche es (über 3) an die ÖV-Leitstelle weiterleitet.
  Hinweis:
  Die Kameraaufzeichnung wird gemäß AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse zum Zwecke des Nachweises bzw. der Beweissicherung aufgezeichnet unter Wahrung der Anforderungen der Datensicherheit. Gleichzeitig sind die gesetzlichen Bestimmungen des Datenschutzes, insbesondere die Datensparsamkeit einzuhalten. Folglich dürfen Gespräche zwischen dem Fahrgast mit der ÖV-Leitstelle nicht bzw. nur in begründeten Fällen, möglichst anonymisiert, aufgezeichnet / dokumentiert werden. Deshalb, (nur die Technische Aufsicht (TA) der AD-Leitstelle kann die Innenraumkamera weg vom Fahrgast, auf die Verschmutzung ausrichten) erfolgt dieser Ablauf (Sonderfall) nicht über den üblichen Weg (über 14 zum ÖV-Bordrechner und dann über 7 zur ÖV-Leitstelle).

- Sofern sinnvoll und gewünscht, kann die ÖV-Leitstelle zusätzlich eine Sprechverbindung / Durchsage zum Fahrzeug herstellen (über 7) und (über 11) ausgeben.

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie in der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik, Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik über einen Abschluß verfügt als
  - ► Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert),
  - ► Bachelor, Master oder
  - ► staatlich geprüfter Techniker.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 2
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie eine entsprechende Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen hat.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 3
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muß, und
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 4
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihr anvertrauten Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes zuverlässig ist.
  Zur Beurteilung der Zuverlässigkeit im Sinne des Satzes 2 Nummer 4 sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde, eine Auskunft aus dem Fahrerlaubnisregister sowie eine Auskunft über Eintragungen aus dem Fahreignungsregister vorzulegen. Sofern in dem Fahrerlaubnisregister mehr als drei Punkte eingetragen sind, ist die Zuverlässigkeit nicht gegeben. § 8 Absatz 3 gilt bezüglich Satz 3 entsprechend.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 2
  Die als Technische Aufsicht eingesetzte natürliche Person darf sich mit Zustimmung des Halters zur Erfüllung ihrer Pflichten weiterer geeigneter natürlicher Personen bedienen, die über mindestens drei Jahre Berufserfahrung im Bereich des Verkehrs- oder Kraftfahrzeugwesens verfügen. Die eingesetzten natürlichen Personen müssen wiederkehrend, mindestens jedoch jährlich beim Hersteller in Bezug auf den Umgang mit dem Kraftfahrzeug sowie wesentliche Veränderungen am Kraftfahrzeug oder der autonomen Fahrfunktion geschult werden. Die Schulung ist mit einer praktischen Prüfung einschließlich der Bewältigung simulierter Betriebsstörungen abzuschließen. Der erfolgreiche Abschluß der Schulung von eingesetzten natürlichen Personen ist von der Technischen Aufsicht zu dokumentieren. Sollen die eingesetzten natürlichen Personen

Fahrten im manuellen Fahrbetrieb übernehmen oder Fahrmanöver freigeben, müssen diese Personen eine gültige Fahrerlaubnis besitzen. Die Klasse der Fahrerlaubnis muß der des Fahrzeugs mit autonomer Fahrfunktion entsprechen.

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 3
  Befindet sich das Kraftfahrzeug mit autonomer Fahrfunktion im risikominimalen Zustand im Sinne des § 1d Absatz 4 des Straßenverkehrsgesetzes, hat die als Technische Aufsicht eingesetzte natürliche Person eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durchzuführen, bevor sie dessen Beendigung veranlassen darf. Das Ergebnis der Untersuchung ist zu dokumentieren. Wurde der risikominimale Zustand durch einen Defekt am Kraftfahrzeug ausgelöst, muß nach Erreichen des risikominimalen Zustands die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage 1 Nummer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
  Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist ungeachtet der Sätze 1 und 3 das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen. In diesen Fällen erfolgt die Untersuchung der Technischen Aufsicht gemäß Satz 1 im Nachgang des Abtransports auf Grundlage der gespeicherten Fahrdaten.
- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
  Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
  Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.
- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.
- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).

- AFGBV Anlage 1 Teil 1 Abschnitt 7.1 Betriebshandbuch
  Zweck des Betriebshandbuchs ist es, mittels detaillierter Vorgaben den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten und der Technischen Aufsicht die richtige Reaktion auf Fehlerfälle zu ermöglichen.
  Hinweis:
  AFGBV Anlage 3 Dokumentationspflichten des Herstellers Kapitel 2 spezifiziert die Anforderungen.
- BOKraft §11 Fundsachen
  Nach Beendigung jeder Fahrt haben Fahrzeugführer oder Schaffner festzustellen, ob Gegenstände zurückgeblieben sind. Fundsachen sind unverzüglich an die dafür vorgesehene Einrichtung des Betriebs oder an die von der Genehmigungsbehörde benannte Stelle abzuliefern, wenn sie nicht sofort zurückgegeben werden können. § 978 des Bürgerlichen Gesetzbuchs bleibt unberührt.

Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.
- BOStrab §46 Absatz 6
  Bei Fahrbetrieb ohne Fahrzeugführer müssen Personenfahrzeuge Einrichtungen für eine Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle haben. Absatz 4 Satz 2 gilt entsprechend.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betrachtung dieses UseCases auf typische Fundsachen und Verschmutzungen reduziert. Daraus resultieren, abgesehen von nicht erkennbarem Inhalt bei Fundsachen und einer Rutschgefahr bei Verschüttetem, keine nennenswerten Gefahren, welche nicht durch die etablierten Betriebsprozesse und daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert wurden. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.

(Bild: ÖV-LeitmoiF-KI-TUIL)

Risikograph:

UC-24 Fundsachen un			W3	W2	W1
C1			a	n/a	n/a
C2	F1	P1	b	a	n/a
		P2	c	b	a
	F2	P1	d	c	b
		P2	e	d	c
C3	F1		f	e	d
	F2		g	f	e
C4			h	g	f

≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzungen durch den gefährlichen Vorfall
✖	
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich

3.2.25 UC-25 Waschvorgang

Das BHMS prüft vorab, ob die Waschstraße verfügbar ist. Sollte dies nicht der Fall sein, wird das Fahrzeug auf einem Abstellpunkt abgestellt (s. UC Parken). Ist die Waschstraße verfügbar, fährt das Fahrzeug zu dieser (s. UC Depot-Fahrt). Sobald das Fahrzeug in die Waschstraße einfährt, wird der Missionsstatus auf "verarbeitend“ gesetzt. Ist die Durchfahrt durch die Waschstraße abgeschlossen, wird der Missionsstatus auf "beendet" gesetzt.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine	keine
BHMS	Fahrzeug Service (Reinigung, erkannte Mängel, z.B. Beschmierungen dokumentieren und zur späteren Instandsetzung einplanen) Prüfung Verfügbarkeit Waschstraße	Fahrzeugzustand (Einsatzbereitschaft)
AD-Leitstelle	Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Dieser UseCase findet ausschließlich auf einem Betriebshof statt.

Hinweis:
Fahrtänderungen für Service & Wartungsumläufe / -fahrten / -fahrwege / -fahraufträge / -missionen obliegen dem BHMS eigenständig.

Betriebsschutz:
Zugang zum Betriebshof (Sicherheitszone) haben nur ausgebildete und (sicherheitstechnisch) geschulte Mitarbeiter, Fahrgäste haben keinen Zugang.

Situation:
Service & Wartungsumlauf (Regelbetrieb).

Aktionen:

- Das BHMS plant und setzt alle Tätigkeiten bzgl. Fahrzeugpflege (Service & Wartung) eigenständig um, wozu auch der Waschvorgang gehört.
  - Das BHMS bestimmt welches Fahrzeug wann gewaschen werden soll.
  - Das BHMS prüft vor dem Entsenden des Fahrzeuges zur Waschstraße, ob diese verfügbar ist.
    - Sofern die Waschstraße frei ist,
      wird das Fahrzeug autonom über UC-44 Fahrt im Depot zur Station bewegt.
    - Sofern die Waschstraße belegt (Warteschlange voll) ist,
      wird das Fahrzeug autonom über UC-44 Fahrt im Depot zum Abstellpunkt UC-43 Parken bewegt.
  - Das BHMS erhält während der Durchfahrt / Umrundung durch die Waschstraße automatisierte Meldung.
    Hinweis:
    Es gibt Waschstraßen der Kategorie Durchfahrt, bekannt vom PKW und
    es gibt Waschstraßen wo das Fahrzeug steht und sich die Waschanlage um das Fahrzeug bewegt.
    - Die Anlage der Waschstraße schiebt das Fahrzeug automatisiert durch die Waschstraße bzw. die Waschanlage reinigt das Fahrzeug, wobei dieses ggf. mehrfach umrundet wird.
    - Das AD-Bordsystem überwacht über UM0.19.8 Control (S19.A = CAN) dabei das Drehen der Fahrzeugräder und damit deren Geschwindigkeit, sofern es sich um eine Waschstraße der Kategorie Durchfahrt handeln sollte.
    - Das AD-Bordsystem gleicht die Bewegung mit der hochauflösenden Karte ab und übermittelt die Fahrzeugposition (über 14) an den ÖV-Bordrechner sowie (über 8) an die AD-Leitstelle sofern es sich um eine Waschstraße der Kategorie Durchfahrt handeln sollte.
    - Der ÖV-Bordrechner berichtet (informiert) den Fortschritt mittels der logischen Ortung über GPS den zurückgelegten Weg der Durchfahrt (über 6) an das BHMS sofern es sich um eine Waschstraße der Kategorie Durchfahrt handeln sollte.
  - Sobald das Fahrzeug den Waschvorgang abgeschlossen hat,
    wird das Fahrzeug zur nächsten Station oder zu einem Abstellplatz bewegt, gemäß dem Service & Wartungsumlauf des BHMS, d.h. UC-25 → UC-44 → nächste Station / UC-43.

Juristische Anforderungen:

- AFGBV §5 Absatz 5
  Die Hersteller und die Halter von Kraftfahrzeugen mit autonomer Fahrfunktion sind verpflichtet
  ► das Kraftfahrt-Bundesamt bei der Durchführung der Marktüberwachungstätigkeiten zu unterstützen und
  ► dem Kraftfahrt-Bundesamt auf Verlangen die für die Marktüberwachung erforderlichen Unterlagen und Informationen sowie andere technische Spezifikationen unentgeltlich bereitzustellen, wobei die Hersteller auf Verlangen auch einen Zugang zu Software und Algorithmen ermöglichen müssen.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 1
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen die Fahrzeugsysteme für die aktive und passive Sicherheit des Kraftfahrzeugs mit autonomer Fahrfunktion regelmäßig überprüft werden.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.
- AFGBV §13 Anforderungen an den Halter Absatz 3
  Der Halter muß sicherstellen, daß Anweisungen zur ordnungsgemäßen Durchführung der Wartungsarbeiten, der Gesamtprüfungen, weiterer Untersuchungen und Fahrten im manuellen Fahrbetrieb vorliegen und daß diese Anweisungen befolgt werden. Die Anweisungen sind zu dokumentieren.
- AFGBV §13 Anforderungen an den Halter Absatz 4
  Berichte über die Durchführung von Wartungsarbeiten, von Gesamtprüfungen und von weiteren Untersuchungen müssen durch den Halter oder die verantwortliche Person unverzüglich schriftlich oder elektronisch erstellt werden. Die Berichte sind zu unterzeichnen. Die Berichte sind zu dokumentieren und vom Halter oder von der für die Technische Aufsicht verantwortlichen Person sechs Monate lang aufzubewahren und nach Ablauf dieser Frist unverzüglich, bei elektronischer Speicherung automatisiert, zu löschen.
- AFGBV §13 Anforderungen an den Halter Absatz 5
  Die Anforderungen zur Dokumentenverwaltung für die Anweisungen nach Absatz 3 und der Berichte nach Absatz 4 müssen dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik wird vermutet, wenn die Vorgaben der ISO 9001:2015 Qualitätsmanagementsysteme – Grundlagen und Begriffe erfüllt werden. Darüber hinaus muß die Dokumentenverwaltung den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 genügen.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.
- AFGBV Anlage 1 Teil 1 Abschnitt 7.1 Betriebshandbuch
  Zweck des Betriebshandbuchs ist es, mittels detaillierter Vorgaben den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten und der Technischen Aufsicht die richtige Reaktion auf Fehlerfälle zu ermöglichen.
  Hinweis:
  AFGBV Anlage 3 Dokumentationspflichten des Herstellers Kapitel 2 spezifiziert die Anforderungen.
- AFGBV Anlage 1 Teil 1 Abschnitt 8 Sensorik
  Zur technischen Umsetzung der autonomen Fahrfunktion muß eine Sensorik verwendet werden, die alle für die sichere Erfüllung der Fahraufgabe erforderlichen Gegenstände, Daten oder Personen im Umfeld des Kraftfahrzeugs erfaßt und hinsichtlich der Verarbeitung personenbezogener Daten die Vorgaben der Verordnung (EU) 2016/679, des Bundesdatenschutzgesetzes und spezialgesetzlicher datenschutzrechtlicher Vorschriften beachtet. Zur Erfüllung des in Satz 1 genannten Zwecks und unter Einhaltung der genannten Vorgaben kann die Sensorik durch externe Systeme unterstützt werden. Beeinflussen Wetter-, Umwelt- und Infrastrukturbedingungen die Leistungsfähigkeit der Sensorik, werden von der technischen Ausrüstung des

Kraftfahrzeugs mit autonomer Fahrfunktion Maßnahmen eingeleitet, um die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken auszugleichen. Die Sensorik ist in das Sicherheitskonzept des Kraftfahrzeugs mit autonomer Fahrfunktion nach Nummer 7.2 und in die permanente Systemüberwachung nach Nummer 5 einzubinden.

- AFGBV Anlage 1 Teil 1 Abschnitt 9 Alterung und Abnutzung des Systems
  Das Kraftfahrzeug muß die funktionalen Anforderungen auch bei Alterung und Abnutzung der relevanten Systemkomponenten erfüllen. Beeinflussen Alterungserscheinungen die Leistungsfähigkeit, beispielsweise der Sensorik, gleicht die technische Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken durch geeignete Maßnahmen aus.

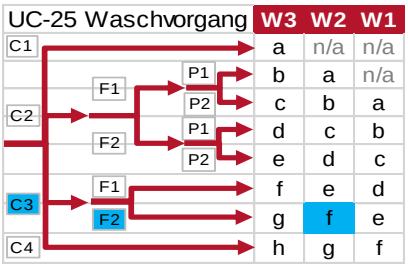
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.
- Zum Waschvorgang gehört auch die sorgfältige und ordnungsgemäße Reinigung der Sensorik sowie die Überprüfung der Leistungsfähigkeit, besonders hinsichtlich Abnutzung durch Verschmutzung.
  - Gegenstände, Daten oder Personen im Umfeld des Kraftfahrzeugs werden nicht korrekt erfaßt. (bounding box ≙ Hüllkörper).
    Hinweis:
    LIDAR-Systeme können Objekte als rechteckige Quader (bounding box ≙ Hüllkörper) erkennen bzw. abbilden. Diese Hüllkörper können sowohl Objekte aus der Umgebung, z.B. parkendes Auto, Wartehaus der Haltestellen oder auch Personen / Tiere sein.
  - Gegenstände, Daten oder Personen im Umfeld des Kraftfahrzeugs werden anders erkannt als sie es sind, z.B. werden bewegliche Objekte (Vulnerable Road User (VRU) ≙ verwundbarer Verkehrsteilnehmer) als feststehende Objekte erkannt oder umgekehrt.
    Hinweis:
    Durch eine dichte Ölverschmutzung wird ein hoher Anteil vom Laserstrahl direkt reflektiert, weshalb ein bewegliches Objekt dauerhaft mit minimalem Abstand erkannt wird, wobei hier viele Punkte der Wolke direkt als Fehler erkannt werden können, jedoch gibt es weitere Punkte, welche erst nach einer gewissen Zeit in abgeschwächter Form zurück reflektiert werden. Dabei kann es vorkommen das Reflektionen von späteren Aussendungen früher empfangen werden, aber nicht als später emittierte erkannt werden, weil sich die Verschmutzung während der Fahrt geringfügig durch den veränderten Luftdruck durch die Geschwindigkeit oder Kurvenfahrt verformt.
    Hinweis:
    KI-gestützte Algorithmen können dieses durch Lernen erkennen und auch anteilig kompensieren, welches über Simulationen im Windkanal trainiert werden kann.
  - Bewegungen von Objekten werden Reverse / Umgekehrt / Rückwärts erkannt, z.B. ein sich näherndes Objekt wird als sich aus der Gefahrenzone heraus- statt hineinbewegend erkannt.
    Hinweis:
    Dieses kann insbesondere dann auftreten, wenn der Laserstrahl durch Verschmutzung (Regen- Öltropfen) auf dem Sensor oder Verschmutzung in der Umwelt (Regen, Schnee oder Nebel), welche den Strahl beugen und zerstreuen können, so abgeschwächt wird, daß nur ein, ggf. zeitlich verzögerter, Strahl zum Sensor zurückreflektiert wird.
    Es kann auch auftreten, wenn reflektiertes Licht von anderen LiDAR-Systemen empfangen, aber nicht als Fremdpunkt erkannt wird, was bei uncodierten Systemen vorkommen kann.
    Hinweis:
    Verschmutzungen von Regentropfen kleben bei langsamen Geschwindigkeiten von z.B. 30km/h, lösen sich jedoch bei höheren Geschwindigkeiten z.B. 80km/h durch den Luftdruck. Verschmutzungen von Öl haben eine höhere Haftung / Klebkraft. Die Werte sind vom Sensor und der Montage abhängig, weshalb diese Werte durch Tests am Fahrzeug zu ermitteln sind.

Risikograph:



≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen durch den gefährlichen Vorfall. *Hinweis:* *ISO-26262-03:2018 Clause 7.4.3.1 Sicherheitsanforderungen müssen dem Automotive Safety Integrity Level (ASIL) der Funktion und dem zugehörigen Sicherheitsziel entsprechen.* *Der Waschvorgang reinigt die Sensorik, eine nicht ordnungsgemäße Reinigung der Sensorik kann dazu führen, daß Hüllboxen von Gegenständen oder Personen im Umfeld des Kraftfahrzeugs nicht korrekt erfaßt werden, welches einen Unfall auslösen kann.* *Hinweis (Gegen-)Maßnahme:* *Am Ausgang zur Waschstraße ist das momentane gegen das bekannte Umgebungsbild zu vergleichen, sofern dieses relevante Abweichungen aufweisen sollte, z.B. durch einen Ölfilm der beim Waschen nicht abgewaschen wurde, dann ist manuell nachzuarbeiten.*
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.26 UC-26 Lademanagement

Dieser Use Case behandelt den Prozeß des Ladens der Fahrzeuge; die Feststellung einer Ladenotwendigkeit ist nicht Teil dieser Beschreibung.

- Variante 1 Laden im Depot und Fahrzeug im Depot.
- Variante 2 Laden im Depot und Fahrzeug außerhalb vom Depot.
- Variante 3 Laden außerhalb vom Depot.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	■ Keine (Fahrzeug innerhalb vom Depot) ■ Dispositive Maßnahmen zur Problemlösung treffen (Fahrzeug außerhalb vom Depot)	Problemlösung, sofern Fahrzeug außerhalb des BHMS.
BHMS	Fahrzeug Service	Fahrzeugzustand (Einsatzbereitschaft)
AD-Leitstelle	Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Das Betriebshofmanagementsystem (BHMS) umfaßt das Planungs- und Steuerungssystem für alle Vorgänge auf dem Betriebshof, z.B. Abstellen, Rangieren, Kuppeln, Waschen, Tanken / Laden, etc. von Bussen und Shuttles.

Hinweis:
Fahrtänderungen für Service & Wartungsumläufe / -fahrten / -fahrwege / -fahraufträge / -missionen obliegen dem BHMS eigenständig.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Aufladen der Battery Electric Vehicles (BEV) / Batterieelektrische Fahrzeuge (Regelbetrieb / Sonderfall).

Aktionen (Regelbetrieb ≙ Variante 1 Laden im Depot und Fahrzeug im Depot):

- Das BHMS plant den Ladevorgang.
  Zum geplanten Zeitpunkt, zu dem sich das Fahrzeug zur Ladestation begeben soll wird geprüft, ob diese verfügbar ist.
- Sofern Platz in der Warteschlange der Station vorhanden ist, begibt sich das Fahrzeug (über UC-44 Fahrt im Depot) zur Ladestation. Andernfalls wird (über UC-43 Parken) ein zwischenzeitliches Parken umgesetzt.
- In beiden Fällen (Fahrt zur Ladestation / Parkplatz + Laden / Parken) wird eine Mission vom BHMS erstellt.
- Das AD-Bordsystem prüft die FZ-Mission gegen die hochauflösende Karte und meldet das Ergebnis der Prüfung (über 14) an den ÖV-Bordrechner und (über 8) an die AD-Leitstelle.
  Hinweis:
  Die Mission beschreibt einen Teil einer Fahrt zwischen zwei Haltepunkten / Haltestellen über eine Menge an Wegpunkten. Es wird unterschieden zwischen einer ÖV-Mission und einer FZ-Mission. Die ÖV-Mission bezeichnet das Missions-Artefakt, welches eine Mission zwischen der ÖV-Leistelle bzw. dem BHMS und der AD-Leitstelle (d.h. Schnittstelle 3 bzw. 4) darstellt, während die FZ-Mission ein Missions-Artefakt bezeichnet, welches eine Mission zwischen der AD-Leistelle und dem AD-Bordsystem (d.h. Schnittstelle 8) darstellt.
- Die AD-Leitstelle überwacht die Fahrt (über UC-44 Fahrt im Depot).
  Hinweis:
  In diesem Use Case wird nur der positive Ast, die Umsetzung der Fahrt zur Ladestation beschrieben.
  Der negative Fall (alle Ladestationen besetzt) wäre die Fahrt zum Parkplatz und später die Fahrt zur Ladestation.
- Sobald das Fahrzeug die Ladestation erreicht hat, meldet es sich beim Lademanagementsystem (LMS) an.
- Die Station des Lademanagementsystems (LMS) des BHMS nimmt die Anmeldung entgegen und erteilt die Freigabe.
  Hinweis:
  Sollte es keine Freigabe vom LMS geben, wartet das Fahrzeug stehend in der Warteposition bis die Freigabe erteilt wird.
- Abhängig von der Konstruktion des Fahrzeugs wird der Ladestecker eingesteckt oder der Pantograph ausgefahren, beim induktiven Laden wird dieses aktiviert.
  Hinweis:
  Pantographen gibt es in der Form vom Fahrzeug hochgefahren oder von der Stromversorgung heruntergefahren, weshalb hier ausgefahren und eingefahren verwendet wird.

- Sobald der Ladevorgang abgeschlossen ist, wird der Ladevorgang beendet, d.h. abhängig von der Konstruktion wird das Ladekabel entfernt, der Pantograph eingefahren oder das induktive Laden abgeschaltet.
- Das Fahrzeug verläßt (über UC-44 Fahrt im Depot) die Station und begibt sich zur nächsten Station oder zum Parkplatz (UC-43 Parken).

Aktionen (Sonderfall ≙ Variante 2 / 3 Fahrzeug außerhalb vom Depot und Laden im Depot / außerhalb):

- Das AD-Bordsystem erkennt (über 17), daß der Batterieladestand niedrig ist.
  Hinweis: Der ÖV-Bordrechner kann dieses ebenfalls eigenständig (über 12) erkennen.
- Das AD-Bordsystem informiert (über 14) den ÖV-Bordrechner und (über 8) die AD-Leitstelle.
- Der ÖV-Bordrechner meldet dieses an die ÖV-Leitstelle.
- Die ÖV-Leitstelle prüft
  - ob der Ladestand ausreichend ist, um den Umlauf inklusive Rückkehr zum Depot zu beenden.
    Hinweis: Sollte dieses möglich sein, sind keine Maßnahmen erforderlich.
  - Sollte dieses nicht möglich sein, prüft die ÖV-Leitstelle, ob die Endhaltestelle der aktuellen Linie inklusive Rückkehr zum Depot zu erreichen ist.
    Hinweis:
    Ein Umlauf ist eine Sequenz von Fahrten, vom Ausrücken aus dem Betriebshof bis zum Einrücken in den Betriebshof, d. h. die Menge von Fahrten, die von einem Fahrzeug an einem (Teil des) Betriebstag(s) durchgeführt werden. Die Identifikation erfolgt über den Betriebstag sowie eine Umlaufnummer.
    Hinweis:
    Ein Umlauf kann eine / mehrere Linien abfahren. Eine Linie kann auch durch eine Linienteilung in zwei neue Umläufe geteilt werden. Dadurch kann der Fahrweg entsprechend verkürzt werden, so daß eine Rückkehr zum Depot sichergestellt wird.
    Hinweis:
    Eine Linienteilung gehört zu den Basismaßnahmen der ÖV-Störungsbehandlung.
  - Sollte auch dieses nicht möglich sein, prüft die ÖV-Leitstelle, ob die nächste Haltestelle erreicht werden kann.
- Die ÖV-Leitstelle trifft dispositive Maßnahmen der Problemlösung, inklusive Ersatzfahrzeug aussenden und Fahrgäste über die Änderungen informieren.
  Hinweis:
  Mit dem Ersatzfahrzeug kann auch ein Mitarbeiter des ÖPNV-Unternehmens zum Ort der Fahrgastübergabe fahren. Dieser begleitet dann das batterieschwache Fahrzeug zu einer Ladestation außerhalb des BHMS um dort den Ladestecker einzustecken und nach dem Laden wieder zu entfernen.

Juristische Anforderungen:

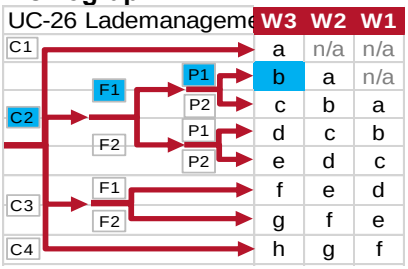
- AFGBV §5 Absatz 5
  Die Hersteller und die Halter von Kraftfahrzeugen mit autonomer Fahrfunktion sind verpflichtet
  ► das Kraftfahrt-Bundesamt bei der Durchführung der Marktüberwachungstätigkeiten zu unterstützen und
  ► dem Kraftfahrt-Bundesamt auf Verlangen die für die Marktüberwachung erforderlichen Unterlagen und Informationen sowie andere technische Spezifikationen unentgeltlich bereitzustellen, wobei die Hersteller auf Verlangen auch einen Zugang zu Software und Algorithmen ermöglichen müssen.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.
- AFGBV Anlage 1 Teil 1 Abschnitt 7.1 Betriebshandbuch
  Zweck des Betriebshandbuchs ist es, mittels detaillierter Vorgaben den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten und der Technischen Aufsicht die richtige Reaktion auf Fehlerfälle zu ermöglichen.
  Hinweis:
  AFGBV Anlage 3 Dokumentationspflichten des Herstellers Kapitel 2 spezifiziert die Anforderungen.
- AFGBV Anlage 1 Teil 1 Abschnitt 9 Alterung und Abnutzung des Systems
  Das Kraftfahrzeug muß die funktionalen Anforderungen auch bei Alterung und Abnutzung der relevanten Systemkomponenten erfüllen. Beeinflussen Alterungserscheinungen die Leistungsfähigkeit, beispielsweise der Sensorik, gleicht die technische Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken durch geeignete Maßnahmen aus.

  Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.
- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dieses gilt insbesondere für den Zugang zum Hochvoltbereich, wo nur geschultes Personal für die Umsetzung der Tätigkeiten eingesetzt werden darf.
  Hinweis:
  Dieses gilt insbesondere beim Laden über den Pantographen, wo ein unkontrolliertes Wegfahren / Wegrollen durch geeignete Sperren zu verhindern ist.
  Hinweis:
  Die Betriebsprozesse beinhalten die vom ÖPNV-Unternehmen bereits eingesetzten Schutzmaßnahmen, dazu zählt z.B. die Installation von FI-Schutzschaltern und /oder der Einsatz von Arbeitskleidung nach E DIN EN 50286 VDE 0682-301:2021-09 (CENELEC).

Risikograph:



≙ ASIL-A

Begründung zur Wahl der Risikoparameter:

C2	C2 Schwere irreversible Verletzung einer oder mehrerer Personen inkl. Tod einer einzigen Person durch den gefährlichen Vorfall (Pantograph Fehlbedienung). *Hinweis:* *C1 Geringe Verletzungen durch den gefährlichen Vorfall (Ladstecker).*
F1	seltener bis öfterer Aufenthalt im gefährlichen Bereich. *Hinweis:* *Die Gefahr tritt im wesentlichen nur beim Ein- und Ausschalten, jedoch nicht während des Ladevorganges auf.*
P1	Möglichkeit der Vermeidung unter bestimmten Bedingungen, *z.B. Arbeitsvorschrift (AV)*.
W3	Eine relativ hohe Auftretenswahrscheinlichkeit und häufige unerwünschte Ereignisse sind wahrscheinlich. *Hinweis: hohe Auftretenswahrscheinlichkeit des Ladens, aber wenig unerwünscht Ereignisse sind zu erwarten.*

3.2.27 UC-27 Ersatzfahrzeug bereitstellen

Das Fahrzeug ist nicht mehr einsatzfähig und gibt eine Schadensmeldung an die ÖV-Leitstelle weiter. Durch die Fahrzeugnummer bzw. Umlauf-Nr. kann die ÖV-Leitstelle auf Anforderungen an den neuen Umlauf schließen, der Standort als weitere Information hilft bei der Auswahl des Fahrzeuges aus einer Fahrzeugliste. Dargestellt in dem Swimlane-Diagramm ist zwischen der ÖV-Leitstelle und dem Betriebshof eine 1:1-Beziehung, diese kann auch als 1:n-Beziehung ausgelegt sein, wenn mehrere Betriebshöfe existieren und angefragt werden. Das jeweilige BHMS stellt die Umlaufanforderungen der Fahrzeugverfügbarkeit entgegen und trifft eine Fahrzeugauswahl. Die Leitstelle erhält gegebenenfalls eine Liste an möglichen Ersatzfahrzeugen und trifft die Fahrzeugauswahl. Nach Umlaufgenerierung werden die Umlaufinformationen dem Fahrzeug über das BHMS (Verhinderung Zustandsinkonsistenz) zur Verfügung gestellt. Das Fahrzeug meldet sich auf dem Umlauf an und beginnt die Fahrt zum vorgegebenen Einsatzort.

Hinweis:
Der betrachtete Use Case basiert auf der bisherigen Betrachtung im Projekt ÖV-LeitmotiF-KI.
Diese hat sich zwischenzeitlich verändert, wobei die Versorgung der Fahrgäste im Notfall bei einem Liegenbleiber, ggf. im Winter ohne funktionierende Heizung im Fahrzeug und auch die rechtzeitige Einplanung und Bereitstellung von Ersatzfahrzeugen für Notfälle aus der Betrachtung herausgenommen und durch dispositive Maßnahmen, welche in anderen Use Cases hinreichend beschrieben sind, ersetzt wurde. Dieses FSK ist jedoch Teil der Blaupause für ÖPNV-Unternehmen, für welche der hier beschriebene Ablauf der Fahrgastversorgung relevant ist, weshalb diese Beschreibung erhalten bleibt um den diskriminierungsfreien Zugang der Markteilnehmer, insbesondere der ÖPNV-Unternehmen zu wahren. Die projektspezifischen Änderungen sind zu finden im Dokument 20230330_Deliverable_MS1_UseCases_v3.docx oder Nachfolger.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Der ÖV-Disponent entscheidet über die Fortsetzung und das Entsenden eines Ersatzfahrzeuges. Die ÖV-Leitstelle informiert über das FGI die wartenden, potentiellen Fahrgäste.	Kapazitätsplanung inkl. Ausfalleinsatzplanung Fahrplan Aktualisierung Fahrgastinformation (Verspätung/Ersatzverkehr)
BHMS	Prüfung der Einsatzbereitschaft. (Verifikation der Umsetzung der Maßnahmen von Wartung und Pflege) vor dem Aufrüsten sowie Absolvieren der (erweiterten) Abfahrkontrolle.	Vorhaltung von einsatzfähigen Ersatzfahrzeugen gemäß Planung der ÖV-Leitstelle.
AD-Leitstelle	Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, (sofern notwendig), ggf. Wiederherstellung der Leichtigkeit des Straßenverkehrs, damit dieser nicht durch das ausgefallene Fahrzeug beeinträchtigt wird, sofern dieses ohne Gefährdung von Leib und Leben möglich ist. Türöffnung, sofern Fahrgäste das Fahrzeug verlassen möchten.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Fahrtänderungen für Service & Wartungsumläufe / -fahrten / -fahrwege / -fahraufträge / -missionen obliegen dem BHMS eigenständig.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Ereignisfall (Besondere Situation / Ereignis → planbarer Regelbetrieb).

Aktionen:

- Das AD-Bordsystem überwacht den Fahrzeugsystemzustand (über 17) kontinuierlich und wertet diesen zur Störungserkennung aus.
- Sofern eine schwerwiegende Störung erkannt wird, welche die Sicherheit der Fortbewegung gefährdet, führt das Fahrzeug (ADO) ein Minimum Risk Manoeuvre (MRM) aus, um in den sicheren Zustand zurückzukehren zusätzlich wird die automatische Datenspeicherung mit der Überführung in den sicheren Zustand gestartet, *gemäß AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse Fall 3.*

- Das AD-Bordsystem meldet dieses (über 14) informativ an den ÖV-Bordrechner und (über 8) an die AD-Leitstelle zur Bearbeitung.
- Die Technische Aufsicht (TA) der AD-Leitstelle baut eine vorrangige Sprechverbindung mit Video zu den Fahrgästen auf,
  - ► um sie über das Minimum Risk Manoeuvre (MRM) zu informieren und um sich nach dem Befinden der Fahrgäste zu erkundigen.
  - ► Sofern eine Notlage (z.B. bei Unfall) das Ereignis ausgelöst hat, leistet die Technische Aufsicht (TA) der AD-Leitstelle unverzüglich Hilfe (Ersthelfer),
    - ► ggf. mit dem Hinzurufen von Einsatzkräften,
    - ► ggf. Einbindung des FG-Notfallmanagement und
    - ► ggf. auch unter Einbeziehung (Konferenzschaltung) der ÖV-Leitstelle.
  - ► Sofern ein technischer Defekt vorliegt wird die Auslösung und die Notwendigkeit des risikominimalen Zustands untersucht, wobei auch untersucht wird, ob die Fahraufgabe durch die Technische Aufsicht (TA) der AD-Leitstelle manuell übernommen werden muß, bis der auslösende Defekt nachhaltig beseitigt worden ist. Das Ergebnis der Untersuchung wird dokumentiert.
  - ► Sofern die Fahraufgabe aufgrund der Störungsursache gemäß der Richtlinie (VA / AV) des ÖPNV-Unternehmens nicht manuell übernommen werden darf, ist ein Ersatzfahrzeug zu stellen.
    Hinweis:
    Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen.
    - ► Die AD-Leitstelle informiert (über 3) den Disponenten der ÖV-Leitstelle, welcher die Fahrgäste über das Ersatzfahrzeug und das voraussichtliche Eintreffen zum Umsteigen informiert.
    - ► Die Fahrtfortsetzung wird durch die Technische Aufsicht untersagt (gesperrt) per Rückmeldung (über 8) an das AD-Bordsystem.
- Das AD-Bordsystem meldet die Sperrung der Fahrtfortsetzung (über 14) an den ÖV-Bordrechner, welcher (über 7) die ÖV-Leitstelle (redundant) informiert, jedoch weitere Informationen aus der Fahrplanung ergänzt.
  Hinweis:
  Der Disponent wurde bereits informiert, jetzt meldet das System den Status, welcher auf der Benutzeroberfläche (GUI) angezeigt wird.
- Die ÖV-Leitstelle kann durch die Fahrzeugnummer und/oder die Umlauf-Nr. die betroffene Fahrt und den Fahrauftrag herleiten. Zusätzlich ist der Standort des ausgefallenen Fahrzeuges bekannt, welches den ÖV-Disponenten bei der Auswahl geeigneter Maßnahmen unterstützt.
  - ► Einstellung der Fahrt,
    weil z.B. der Ausfall kurz vor Umlaufende eingetreten ist, jedoch hängt dieses von den Fahrgästen im Fahrzeug und der Nähe eines Betriebshofes mit Ersatzfahrzeugen ab.
    Hinweis:
    Sofern Fahrgäste von dem Einstellen der Fahrt betroffen sind, werden diese versorgt, welches von der Position des Ausfalls und z.B. der nächsten regulären Haltestelle / Halteposition abhängt und ob diese vom Fahrgast eigenständig erreicht werden kann.
  - ► Aussendung eines Ersatzfahrzeuges,
    hierbei spielt der Standort des BHMS (1:n-Beziehung) durch die potentielle Fahrtzeit zum Einsatzort (Ausfallort) eine entscheidende Rolle um die Wartezeit der Fahrgäste zu minimieren.
    Hinweis:
    Im Interesse der Fahrgäste ist eine möglichst geringe Ausfallzeit (Verspätung).
    Hinweis:
    Die ÖV-Leitstelle hat eine Übersicht (Kapazitätsplan) der Fahrzeuge (im Einsatz sowie in der Reserve im Betriebshof und im Service), woraus ein geeignetes Ersatzfahrzeug vom ÖV-Disponenten ausgewählt (sofern möglich / vorhanden) werden kann. Andernfalls wird eine alternative Fahrgastversorgung durch Drittanbieter angeboten.
- Das BHMS meldet das (Ersatz-)Fahrzeug auf dem Umlauf an, sofern dieses der ÖV-Disponent veranlaßt hat.
  - ► Sofern Fahrgäste von dem Ausfall des Fahrzeuges direkt betroffenen sind, begibt sich das Ersatzfahrzeug zum Ausfallort um die vorhandenen Fahrgäste aufzunehmen.
  - ► Andernfalls begibt sich das Ersatzfahrzeug zur nächsten Haltestelle / Haltepunkt um den Umlauf des ausgefallenen Fahrzeugs zu übernehmen und die potentiellen Fahrgäste aufzunehmen.
- Die ÖV-Leitstelle informiert über das FGI die wartenden, potentiellen Fahrgäste auf dem Umlauf über die Verspätung.

Juristische Anforderungen:

- AFGBV §5 Absatz 5
  Die Hersteller und die Halter von Kraftfahrzeugen mit autonomer Fahrfunktion sind verpflichtet
  ► das Kraftfahrt-Bundesamt bei der Durchführung der Marktüberwachungstätigkeiten zu unterstützen und
  ► dem Kraftfahrt-Bundesamt auf Verlangen die für die Marktüberwachung erforderlichen Unterlagen und Informationen sowie andere technische Spezifikationen unentgeltlich bereitzustellen, wobei die Hersteller auf Verlangen auch einen Zugang zu Software und Algorithmen ermöglichen müssen.
- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des

Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.

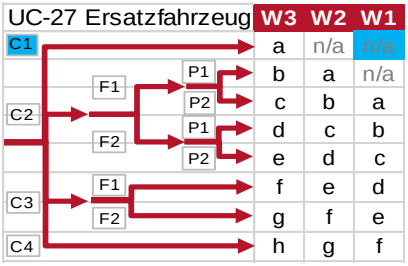
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.
- Die spezifischen Gefahren der verbundenen Use Cases (UC-01 Fahrzeug aufrüsten, UC-02 Umlaufanmeldung/-zuweisung, UC-44 Fahrt im Depot und UC-03 Leerfahrt) sind in den jeweiligen Use Cases beschrieben.

Risikograph:



≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzungen durch den gefährlichen Vorfall. (Akzeptiertes Standardrisiko bei Bürotätigkeiten, hier dispositive Maßnahme)
✖	
✖	
W1	Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.28 UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA)

In einer Verkehrsszene tritt ein Fehler / äußerer/interner Einfluß auf, welcher den reibungslosen Betrieb des Flottenbetriebs stört, sodaß Hilfe von der Technischen Aufsicht (TA) wünschenswert/notwendig ist.
Beispiele hierfür sind Fehlverhalten von Fahrgästen, falschparkende, regelkonform auftretende Hindernisse, andere Verkehrsteilnehmende und False-E-Stops.

Die Störung wird über die Kommunikationsinfrastruktur an die AD-Leitstelle übermittelt. Zu den Maßnahmen, die entweder automatisiert (z.B. als Sofortmaßnahme) oder manuell durch die Technische Aufsicht (TA) eingeleitet werden können, zählen beispielsweise "Risikominimalen Zustand einnehmen", "Geschwindigkeit reduzieren" oder "Fahrt zu bestimmtem Haltepunkt".

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine *Hinweis:* *Sofern (durch die Eingriffsnotwendigkeit der Technischen Aufsicht) festgestellt wird, daß ein Entsenden eines Ersatzfahrzeug erforderlich sein sollte, entscheidet der ÖV-Disponent über die Einleitung der dispositiven Maßnahmen **über die zugehörigen Use Cases**. Dazu gehört das Entsenden eines Ersatzfahrzeuges oder auch das Einstellen des Umlaufes.* *Die ÖV-Leitstelle informiert über das FGI die wartenden, potentiellen Fahrgäste.*	keine
BHMS	keine *Hinweis:* *Sofern bei der Fahrzeugpflege ein Defekt (durch die Eingriffsnotwendigkeit der Technischen Aufsicht) festgestellt werden sollte, insbesondere wenn dieser die Einsatzfähigkeit des Fahrzeuges verhindert, hat das BHMS Maßnahmen der Instandsetzung **über die zugehörigen Use Cases**, einzuleiten, welche die Einsatzfähigkeit des Fahrzeuges wiederherstellt.*	keine
AD-Leitstelle	Fahrzeugüberwachung und Konfiguration der Fahrbereitschaft zur Aufrechterhaltung der Betriebsfortsetzung, sofern möglich. Andernfalls Bergung veranlassen.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Die Eingriffsnotwendigkeit Technische Aufsicht (TA) kann sowohl im Regelbetrieb der Fahrgastbeförderung, als auch innerhalb des BHMS bei der Fahrzeugpflege (Service & Wartung) auftreten.

Hinweis:
Das Operator-HMI (AD) übernimmt die Freigabe sowie Steuerung von Fahrfunktionen inklusive Konfliktbehandlung durch den Operator im Fahrzeug im autonomen Fahrbetrieb.

Hinweis:
Das Fahrzeug-Interface stellt lesenden Zugriff auf technische Zustandsdaten des Fahrzeugs (z.B. Batterie-Ladezustand) zur Verfügung.

Hinweis:
Das Verkehrsinfrastruktur-Interface umfaßt die Kommunikation mit ansteuerbaren Verkehrs-Infrastruktur-Elementen auf der Strecke und im Betriebshof (LSA, Poller, Schranke, etc.)

Hinweis:
Das Umwelt-IF (AD) umfaßt die Sensorik zur Umwelterfassung und -kommunikation für das automatisierte Fahren. Hierzu zählen Kameras, Radar, LiDAR, AD-Infrastruktur, C2I-Kommunikation und C2C-Kommunikation. Die Aktorik umfaßt sämtliche Einrichtungen, die zur Durchführung des automatisierten Fahrens benötigt werden (Lenkung, Antrieb, Bremse), sowie Türsteuerung, Blinker, Warnleuchten, Hupe, etc.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Ereignisfall (Besondere Situation / Ereignis → planbarer Regelbetrieb).

Aktionen:

- Das AD-Bordsystem überwacht kontinuierlich die autonome Fahrt über die Sensorik und die Peripherie des Fahrzeuges und sendet technische Informationen (über 8) an die AD-Leitstelle.

- Das AD-Bordsystem erkennt eine Störung → UC-12 Systemüberwachung und ggf. Störmeldung.
  Hinweis:
  Das AD-Bordsystem meldet Störungen (über 14) informativ an den ÖV-Bordrechner und (über 8) zur Bearbeitung an die AD-Leitstelle. Der ÖV-Bordrechner verarbeitet die Störungsinformation und meldet, sofern sich das Fahrzeug außerhalb des Betriebshofes befindet und gewünscht, diese (über 7) an die ÖV Leitstelle zur weiteren Bearbeitung. Sollte sich das Fahrzeug im Betriebshof befinden, so erfolgt die Meldung (über 6) an das BHMS.
- Die Systemüberwachung des AD-Bordsystems leitet stabilisierende Maßnahmen der Fehlerkorrektur, Stabilisierung, Robustheit ein und überprüft ob die Maßnahmen hinreichend wirksam sind.
  - Sofern die Maßnahmen hinreichend sind, erfolgt ein Ereigniseintrag.
    Hinweis: hinreichend bedeutet, daß die Maßnahmen die Störung kompensieren können.
  - Sofern die Maßnahmen unzureichend sind, erfolgt (über 8) eine Warnmeldung (z.B. Meldung: Lenkung ist schwergängig, Unterstützungsleistung ist häufig aktiv) an die AD-Leitstelle.
    Hinweis: unzureichend bedeutet, daß die Maßnahmen die Störung nur teilweise, jedoch ausreichend, kompensieren können (Warnlampe Gelb).
    Hinweis:
    Abhängig von der Art der Störung kann das AD-Bordsystem durch das Aktivieren des Warnblinkers die Umgebung warnen. Folglich kann ein Eingriff der Technischen Aufsicht (TA) der AD-Leitstelle notwendig werden, um den Warnblinker wieder zu deaktivieren oder das Fahrzeug manuell zu übernehmen.
  - Sofern die Maßnahmen ungenügend sind, wird das Minimum Risk Manoeuvre (MRM) ausgeführt und das AD-Bordsystem meldet (über 8) die Systemstörung an die AD-Leitstelle sowie (über 14) an den ÖV-Bordrechner.
    Hinweis: ungenügend bedeutet, daß die Maßnahmen die Störung nicht ausreichend kompensieren können ≙ Warnlampe Rot.
    Hinweis: Bei einem Minimum Risk Manoeuvre (MRM) ist unabhängig der Kategorie (A bis E) der Warnblinker zu aktivieren.
    - Die Technische Aufsicht (TA) der AD-Leitstelle analysiert die Ursache / Auslösung des Minimum Risk Manoeuvre (MRM) und ergreift geeignete Maßnahmen, um die Störung zu beheben, damit der reibungslose Betrieb wiederaufgenommen / fortgeführt werden kann, sofern dieses nicht möglich sein sollte, werden Maßnahmen ergriffen, welche das Schadenspotential bestmöglich reduzieren. Dazu kann die AD-Leitstelle weitere Daten vom Fahrzeug über das AD-Bordsystem anfordern, z.B.
      - Daten auslesen (über 17) vom Fahrzeug-Interface.
      - Daten auslesen (über 18) vom Verkehrs-Infrastruktur-Interface.
      - Daten lesen und schreiben (über 19) vom Umwelt-Interface AD.
        Hinweis (Randbedingung):
        Die Außenumgebung vor dem Fahrzeug wird (über UM0.19.2 CameraImage) übertragen.
      - Der Fahrgastraum kann (über 15) durch das Operator HMI AD eingesehen werden, hierbei sind die Datenschutzvorschriften nach Artikel 35 der Verordnung (EU) 2016/679, insbesondere den Anforderungen an die Informationstechnik nach Teil 5 und damit den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 einzuhalten. Die Fahrgäste sind vor der Einsicht über das Aktivieren der Kamera dbzgl. anzusprechen (Umsetzung der Informationspflicht).
        Hinweis (Randbedingung):
        Die Innenraunumgebung kann (über UM0.15.3 CamaraImage) eingesehen werden.
      - Das AD-Bordsystem kann auf Basis von Statistikdaten, KI gestützt, Vorschläge zur Behebung der Störung der AD-Leitstelle unterbreiten. ← UC-31 Entscheidungshilfe (Fahrtfortsetzung).
    - Sofern das Minimum Risk Manoeuvre (MRM) durch einen Defekt am Kraftfahrzeug ausgelöst wurde, muß die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage I Ziffer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
    - Die Technische Aufsicht (TA) der AD-Leitstelle informiert (über 3) die ÖV-Leitstelle falls ein Fahrzeugausfall vorliegen oder eine Außerbetriebnahme sinnvoll sein sollte → UC-27 Ersatzfahrzeug bereitstellen.

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und

Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.

- AFGBV §12 Anforderungen an den Hersteller Absatz 1 Punkt 2
  Der Hersteller eines Kraftfahrzeugs mit autonomer Fahrfunktion hat
  ein Sicherheitskonzept zur funktionalen Sicherheit nach Anlage I Nummer 7.2 zu erstellen, und dabei
  a) auf Basis dieses Sicherheitskonzeptes eine Gefährdungsanalyse nach Anlage I Ziffer 7.2.1 durchzuführen,
  b) das Sicherheitskonzept nach Anlage III Ziffer 3 zu dokumentieren,
  c) die Sicherheit der autonomen Fahrfunktion entsprechend dieses Sicherheitskonzepts zu überprüfen und die Sicherheit gegenüber dem Kraftfahrt-Bundesamt nach den Anforderungen nach Anlage I Ziffer 10 nachzuweisen.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 3
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihnen anvertrauten Aufgaben zuverlässig sind; zur Beurteilung ihrer Zuverlässigkeit sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde sowie, bei Einsatz für die Durchführung von Fahrten im manuellen Betrieb, eine Auskunft aus dem Fahrerlaubnisregister vorzulegen; § 8 Absatz 3 gilt entsprechend.
- AFGBV §13 Anforderungen an den Halter Absatz 5
  Die Anforderungen zur Dokumentenverwaltung für die Anweisungen nach Absatz 3 und der Berichte nach Absatz 4 müssen dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik wird vermutet, wenn die Vorgaben der ISO 9001:2015 Qualitätsmanagementsysteme – Grundlagen und Begriffe erfüllt werden. Darüber hinaus muß die Dokumentenverwaltung den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 genügen.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach §1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie in der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik, Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik über einen Abschluß verfügt als
  - ► Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert),
  - ► Bachelor, Master oder
  - ► staatlich geprüfter Techniker.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 2
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie eine entsprechende Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen hat.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 3
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muß, und
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 4
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihr anvertrauten Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes zuverlässig ist.
  Zur Beurteilung der Zuverlässigkeit im Sinne des Satzes 2 Nummer 4 sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde, eine Auskunft aus dem Fahrerlaubnisregister sowie eine Auskunft über Eintragungen aus dem Fahreignungsregister vorzulegen. Sofern in dem Fahrerlaubnisregister mehr als drei Punkte eingetragen sind, ist die Zuverlässigkeit nicht gegeben. § 8 Absatz 3 gilt bezüglich Satz 3 entsprechend.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 2
  Die als Technische Aufsicht eingesetzte natürliche Person darf sich mit Zustimmung des Halters zur Erfüllung ihrer Pflichten weiterer geeigneter natürlicher Personen bedienen, die über mindestens drei Jahre

Berufserfahrung im Bereich des Verkehrs- oder Kraftfahrzeugwesens verfügen. Die eingesetzten natürlichen Personen müssen wiederkehrend, mindestens jedoch jährlich beim Hersteller in Bezug auf den Umgang mit dem Kraftfahrzeug sowie wesentliche Veränderungen am Kraftfahrzeug oder der autonomen Fahrfunktion geschult werden. Die Schulung ist mit einer praktischen Prüfung einschließlich der Bewältigung simulierter Betriebsstörungen abzuschließen. Der erfolgreiche Abschluß der Schulung von eingesetzten natürlichen Personen ist von der Technischen Aufsicht zu dokumentieren. Sollen die eingesetzten natürlichen Personen Fahrten im manuellen Fahrbetrieb übernehmen oder Fahrmanöver freigeben, müssen diese Personen eine gültige Fahrerlaubnis besitzen. Die Klasse der Fahrerlaubnis muß der des Fahrzeugs mit autonomer Fahrfunktion entsprechen.

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 3
  Befindet sich das Kraftfahrzeug mit autonomer Fahrfunktion im risikominimalen Zustand im Sinne des § 1d Absatz 4 des Straßenverkehrsgesetzes, hat die als Technische Aufsicht eingesetzte natürliche Person eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durchzuführen, bevor sie dessen Beendigung veranlassen darf. Das Ergebnis der Untersuchung ist zu dokumentieren. Wurde der risikominimale Zustand durch einen Defekt am Kraftfahrzeug ausgelöst, muß nach Erreichen des risikominimalen Zustands die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage 1 Nummer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
  Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist ungeachtet der Sätze 1 und 3 das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen. In diesen Fällen erfolgt die Untersuchung der Technischen Aufsicht gemäß Satz 1 im Nachgang des Abtransports auf Grundlage der gespeicherten Fahrdaten.
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV §15 Datenspeicherung Absatz 2
  Die gespeicherten Daten dürfen nur durch das Kraftfahrt-Bundesamt und die zuständige Behörde und nur zum Zweck der Nachprüfung der Erfüllung der Voraussetzungen der Genehmigung und der mit der Genehmigung verbundenen Überwachungspflichten erhoben, gespeichert und verwendet werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 2 Risikominimaler Zustand
  Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur Ausübung der Fahraufgabe gilt: Das Kraftfahrzeug kann nur auf Veranlassung der Technischen Aufsicht den risikominimalen Zustand verlassen.
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse
  siehe Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV Anlage 1 Teil 1 Abschnitt 3 Notfahrfunktion
  Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit einer Notfahrfunktion ausgestattet sein. Muß sich das Kraftfahrzeug im Falle eines Defekts am Kraftfahrzeug in den risikominimalen Zustand versetzen, muß dies mit der Notfahrfunktion erfolgen. Fahrten mit der Notfahrfunktion dürfen nur bei Schrittgeschwindigkeit und aktivierter Warnblinkanlage erfolgen. Der Übergang der autonomen Fahrfunktion aus der normalen Fahrt in die Fahrt mit der Notfahrfunktion ist von dieser Geschwindigkeitsbegrenzung ausgenommen, sofern ein Abbremsen erforderlich ist.
- AFGBV Anlage 1 Teil 1 Abschnitt 4 Manueller Fahrbetrieb
  Im manuellen Fahrbetrieb erfüllt eine fahrzeugführende Person die Fahraufgabe. Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit Vorrichtungen ausgestattet sein, die es einer fahrzeugführenden Person ermöglichen, die Fahraufgabe wahrzunehmen. Ist die Steuerung im manuellen Fahrbetrieb auf Geschwindigkeiten nicht höher als Schrittgeschwindigkeit begrenzt, ist es nicht erforderlich, daß die fahrzeugführende Person sich innerhalb des Kraftfahrzeugs mit autonomer Fahrfunktion aufhält. Die

Steuerung kann in diesem Fall über eine im Nahfeld des Kraftfahrzeugs befindliche Fernsteuerung ausgeführt werden. Die maximale Distanz, über die eine Fernsteuerung möglich ist, beträgt 6 Meter, gemessen in gerader Verbindung. Die Einhaltung der maximalen Distanz ist vom Hersteller durch geeignete technische Mittel sicher zu stellen. Soll das Kraftfahrzeug mit autonomer Fahrfunktion im manuellen Fahrbetrieb mit Geschwindigkeiten höher als Schrittgeschwindigkeit gesteuert werden, muß es mit einem Sitzplatz für die fahrzeugführende Person ausgestattet sein. Der Sitzplatz ist entsprechend der geltenden Vorschriften zu gestalten.

- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.1 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur dynamischen Ausübung der Fahraufgabe gilt:
  a) Zur dauerhaften Überwachung der technischen Ausrüstung werden nicht personenbezogene technische Daten im Kraftfahrzeug erhoben und gespeichert.
  b) Eine Beeinträchtigung der technischen Ausrüstung ist der Technischen Aufsicht unverzüglich anzuzeigen.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.2 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und mit konventionellen Vorrichtungen zur Ausübung der Fahraufgabe gilt:
  Die autonome Fahrfunktion darf nicht erneut aktivierbar sein, solange eine Beeinträchtigung der technischen Ausrüstung besteht.

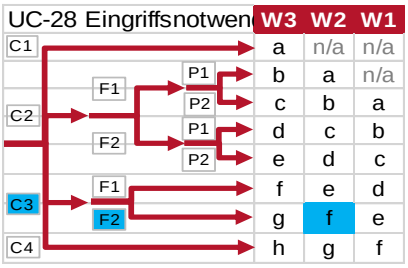
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.
- Die angemessene Sicherheit der Fahrgäste während der Fahrt obliegt zum großen Anteil den Systemen der autonomen Fahrt des Fahrzeugherstellers (OEM) oder dem Hersteller des AD-Tuning-Kits, welche im Gefahrenfall ein Minimum Risk Manoeuvre (MRM) umsetzen, weshalb der verbleibende Anteil einer Störungsmeldung als informativ QM (C) betrachtet werden kann, **aber hier meldet das Fahrzeug (OEM), daß seine Systemgrenze der Handlungsfähigkeit überschritten wurde, weshalb das Fahrzeug (OEM) Unterstützung durch einen Operator anfordert.**
  ISO-26262-03:2018 Clause 7.4.3.1 Sicherheitsanforderungen müssen dem Automotive Safety Integrity Level (ASIL) der Funktion und dem zugehörigen Sicherheitsziel entsprechen.
  Hinweis Fahrt = ASIL-C.
  Hinweis:
  Dieser Use Case betrachtet den Fall nach der sicheren Fehlererkennung, welcher mit Hilfe der Leitworte aufgedeckt / erkannt werden soll. Je nach Art der Störung kann jedes Leitwort dafür angewendet worden sein.

Risikograph:



≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall.
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.29 UC-29 Temporäre Sensorbeeinträchtigung

Im AD-Fahrzeug tritt eine temporäre Sensorbeeinträchtigung der Fahrzeugsensorik (z.B. durch äußere Einflüsse, Umwelteinflüsse wie Regen, Nebel, Nacht (Dunkelheit), Gegenlicht oder Schnee) auf. Im AD-Fahrzeug wird diese automatisiert identifiziert, z.B. durch den Abgleich von extern vorhandenen Informationen durch die Infrastruktursensorik der AD-Infrastruktur oder durch interne, im AD-Fahrzeug vorliegende, Datenströme.
Sofern eine Gegenmaßnahme (z.B. ein Notstopp) durch das AD-Fahrzeug ausgeführt werden muß, wird dies sofort durchgeführt. In jedem Fall kommuniziert das AD-Fahrzeug den auftretenden Sensorfehler über die Kommunikationsinfrastruktur an die AD-Leitstelle. In der AD-Leitstelle wird die Warnung visualisiert. Die technische Aufsicht kann nun den Sachverhalt prüfen und passende Maßnahmen einleiten (z.B. Warten, bis sich die Umweltbedingung geändert hat, andere Flotten-Fahrzeuge warnen oder dispositive Maßnahmen einleiten, wie bspw. das Fahrzeug auf andere Routen schicken, den Zeitplan des Fahrzeugs und anderer Fahrzeuge ändern oder ggf. ein Service-Team zum Fahrzeug schicken).

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine	keine
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung und Konfiguration der Fahrbereitschaft zur Aufrechterhaltung der Betriebsfortsetzung, sofern möglich. Andernfalls Bergung veranlassen.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Das Operator-HMI (AD) übernimmt die Freigabe sowie Steuerung von Fahrfunktionen inklusive Konfliktbehandlung durch den Operator im Fahrzeug im autonomen Fahrbetrieb.

Hinweis:
Das Fahrzeug-Interface stellt lesenden Zugriff auf technische Zustandsdaten des Fahrzeugs (z.B. Batterie-Ladezustand) zur Verfügung.

Hinweis:
Das Verkehrsinfrastruktur-Interface umfaßt die Kommunikation mit ansteuerbaren Verkehrs-Infrastruktur-Elementen auf der Strecke und im Betriebshof (LSA, Poller, Schranke, etc.)

Hinweis:
Das Umwelt-IF (AD) umfaßt die Sensorik zur Umwelterfassung und -kommunikation für das automatisierte Fahren. Hierzu zählen Kameras, Radar, LiDAR, AD-Infrastruktur, C2I-Kommunikation und C2C-Kommunikation. Die Aktorik umfaßt sämtliche Einrichtungen, die zur Durchführung des automatisierten Fahrens benötigt werden (Lenkung, Antrieb, Bremse), sowie Türsteuerung, Blinker, Warnleuchten, Hupe, etc.

Hinweis:
Die Eingriffsnotwendigkeit der Technischen Aufsicht (TA) kann sowohl im Regelbetrieb der Fahrgastbeförderung, als auch innerhalb des BHMS bei der Fahrzeugpflege (Service & Wartung) auftreten.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Ereignisfall (Besondere Situation / Ereignis → planbarer Regelbetrieb).

Aktionen:

- Das AD-Bordsystem überwacht kontinuierlich die autonome Fahrt über die Sensorik und die Peripherie des Fahrzeuges und sendet technische Informationen (über 8) an die AD-Leitstelle.
- Das AD-Bordsystem erkennt eine Störung → UC-12 Systemüberwachung und ggf. Störmeldung.
  Hinweis:
  Das AD-Bordsystem meldet Störungen (über 14) informativ an den ÖV-Bordrechner und (über 8) zur Bearbeitung an die AD-Leitstelle. Der ÖV-Bordrechner verarbeitet die Störungsinformation und meldet, sofern sich das Fahrzeug außerhalb des Betriebshofes befindet und gewünscht, dieses (über 7) an die ÖV Leitstelle zur weiteren Bearbeitung. Sollte sich das Fahrzeug im Betriebshof befinden, so erfolgt die Meldung (über 6) an das BHMS.

- Die Systemüberwachung des AD-Bordsystems leitet stabilisierende Maßnahmen der Fehlerkorrektur, Stabilisierung, Robustheit ein und überprüft ob die Maßnahmen hinreichend wirksam sind.
  - ► Sofern die Maßnahmen hinreichend sind, erfolgt ein Ereigniseintrag.
    Hinweis: hinreichend bedeutet, daß die Maßnahmen die Störung kompensieren können.
  - ► Sofern die Maßnahmen unzureichend sind, erfolgt (über 8) eine Warnmeldung (z.B. Meldung: Lenkung ist schwergängig, Unterstützungsleistung ist häufig aktiv) an die AD-Leitstelle.
    Hinweis: unzureichend bedeutet, daß die Maßnahmen die Störung nur teilweise, jedoch ausreichend, kompensieren können.
    (Warnlampe Gelb)
    Hinweis:
    Abhängig von der Art der Störung kann das AD-Bordsystem durch das Aktivieren des Warnblinkers die Umgebung warnen.
    Folglich kann ein Eingriff der Technischen Aufsicht (TA) der AD-Leitstelle notwendig werden, um den Warnblinker wieder zu deaktivieren oder das Fahrzeug manuell zu übernehmen.
    Hinweis:
    Eine temporäre Sensorbeeinträchtigung kann ausgelöst werden durch einen Wasserschwall, welcher beim Durchfahren eines anderen Fahrzeuges durch eine Pfütze hervorgeht, weshalb die Umgebungssensoren kurzzeitig gestört werden.
    Eine temporäre Sensorbeeinträchtigung kann ausgelöst werden durch eine undichte Lenkung, in welche Wasser eindringen kann, welches zu einer Schwergängigkeit führt → temporär „behebbar" durch Erhöhung der Unterstützungsleistung (Servolenkung).
  - ► Sofern die Maßnahmen ungenügend sind, wird das Minimum Risk Manoeuvre (MRM) ausgeführt und das AD-Bordsystem meldet (über 8) die Systemstörung an die AD-Leitstelle sowie (über 14) an den ÖV-Bordrechner.
    Hinweis: ungenügend bedeutet, daß die Maßnahmen die Störung nicht ausreichend kompensieren können ≙ Warnlampe Rot.
    Hinweis:
    Bei einem Minimum Risk Manoeuvre (MRM) ist unabhängig der Kategorie (A bis E) der Warnblinker zu aktivieren und die Technische Aufsicht (TA) der AD-Leitstelle ist verpflichtet unverzüglich Kontakt mit den Insassen des Kraftfahrzeugs herzustellen.
    - ► Die Technische Aufsicht (TA) der AD-Leitstelle analysiert die Situation und entscheidet über die Eingriffsnotwendigkeit → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).
      Hinweis:
      Sofern die Sensorbeeinträchtigung (irrelevant ob temporär) dazu führen kann, daß Hüllboxen von Gegenständen oder Personen im Umfeld des Kraftfahrzeugs nicht korrekt erfaßt werden, welches einen schweren Unfall zur Folge haben könnte, ist in diesem Fall ein automatisiertes Minimum Risk Manoeuvre (MRM) zwingend umzusetzen.
      Hinweis:
      Die ordnungsgemäße Reinigung der (umgebungserfassenden) Sensorik ist ein wesentlicher Bestandteil zur Vermeidung von Fahrtunterbrechungen (Liegenbleiber) aufgrund von verschmutzungsbedingten (temporären) Sensorbeeinträchtigungen. → Im Rahmen der Betriebsprozesse können solche potentiellen Gefahren leicht ermittelt und durch daraus resultierende Arbeitsvorschriften des ÖPNV-Unternehmens (regelmäßige, an die Witterungsbedingungen angepaßte Reinigung) auf ein verbleibendes Maß eines akzeptablen Restrisikos reduziert werden.

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 3
  Befindet sich das Kraftfahrzeug mit autonomer Fahrfunktion im risikominimalen Zustand im Sinne des § 1d Absatz 4 des Straßenverkehrsgesetzes, hat die als Technische Aufsicht eingesetzte natürliche Person eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durchzuführen, bevor sie dessen Beendigung veranlassen darf. Das Ergebnis der Untersuchung ist zu dokumentieren. Wurde der risikominimale Zustand durch einen Defekt am Kraftfahrzeug ausgelöst, muß nach Erreichen des risikominimalen Zustands die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage 1 Nummer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
  Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist ungeachtet der Sätze 1 und 3 das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen. In diesen Fällen erfolgt die Untersuchung der Technischen Aufsicht gemäß Satz 1 im Nachgang des Abtransports auf Grundlage der gespeicherten Fahrdaten.
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.

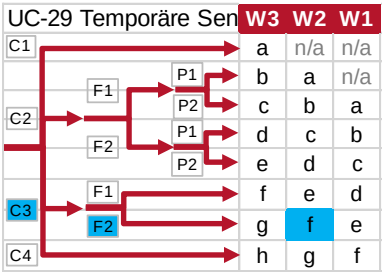
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.
- Dieser UseCase beschreibt eine Maßnahme (Sicherheitsfunktion) der Systemüberwachung, welche bei dem Erkennen einer Störung, hier der Sensorik, automatisch aktiviert wird, wodurch das Schadenspotential einer potentiellen Gefährdung im Rahmen der technischen Sicherheitssysteme auf ein verbleibendes, akzeptiertes Risiko, ggf. durch ein Minimum Risk Manoeuvre (MRM), begrenzt wird.
- Sofern die Sensorbeeinträchtigung (irrelevant ob temporär) dazu führen kann, daß Hüllboxen von Gegenständen oder Personen im Umfeld des Kraftfahrzeugs nicht korrekt erfaßt werden, welches einen schweren Unfall zur Folge haben könnte, ist in diesem Fall ein automatisiertes Minimum Risk Manoeuvre (MRM) zwingend umzusetzen.

Risikograph:



≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall.
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.30 UC-30 Fehler in der Selbstpositionierung

Im AD-Fahrzeug tritt ein dauerhafter Lokalisierungsfehler in einer Fahrsituation auf. Der Fehler wird automatisiert detektiert und eine entsprechende Meldung über die Kommunikationsinfrastruktur an die AD-Leitstelle geschickt. Das AD-Fahrzeug signalisiert den Insassen und seinem Verkehrsumfeld den Fehlerfall.

Sobald die Situation aufgelöst ist, setzt das AD-Fahrzeug seinen Weg fort.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine	keine
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung und Konfiguration der Fahrbereitschaft zur Aufrechterhaltung der Betriebsfortsetzung, sofern möglich. Andernfalls Bergung veranlassen.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Das Operator-HMI (AD) übernimmt die Freigabe sowie Steuerung von Fahrfunktionen inklusive Konfliktbehandlung durch den Operator im Fahrzeug im autonomen Fahrbetrieb.

Hinweis:
Das Fahrzeug-Interface stellt lesenden Zugriff auf technische Zustandsdaten des Fahrzeugs (z.B. Batterie-Ladezustand) zur Verfügung.

Hinweis:
Das Verkehrsinfrastruktur-Interface umfaßt die Kommunikation mit ansteuerbaren Verkehrs-Infrastruktur-Elementen auf der Strecke und im Betriebshof (LSA, Poller, Schranke, etc.)

Hinweis:
Das Umwelt-IF (AD) umfaßt die Sensorik zur Umwelterfassung und -kommunikation für das automatisierte Fahren. Hierzu zählen Kameras, Radar, LiDAR, AD-Infrastruktur, C2I-Kommunikation und C2C-Kommunikation. Die Aktorik umfaßt sämtliche Einrichtungen, die zur Durchführung des automatisierten Fahrens benötigt werden (Lenkung, Antrieb, Bremse), sowie Türsteuerung, Blinker, Warnleuchten, Hupe, etc.

Hinweis:
Die Eingriffsnotwendigkeit der Technischen Aufsicht (TA) kann sowohl im Regelbetrieb der Fahrgastbeförderung, als auch innerhalb des BHMS bei der Fahrzeugpflege (Service & Wartung) auftreten.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Ereignisfall (Besondere Situation / Ereignis → planbarer Regelbetrieb).

Aktionen:

- Das AD-Bordsystem überwacht kontinuierlich die autonome Fahrt über die Sensorik und die Peripherie des Fahrzeuges und sendet technische Informationen (über 8) an die AD-Leitstelle.
- Das AD-Bordsystem erkennt eine Störung → UC-12 Systemüberwachung und ggf. Störmeldung.
  Hinweis:
  Das AD-Bordsystem meldet Störungen (über 14) informativ an den ÖV-Bordrechner und (über 8) zur Bearbeitung an die AD-Leitstelle. Der ÖV-Bordrechner verarbeitet die Störungsinformation und meldet, sofern sich das Fahrzeug außerhalb des Betriebshofes befindet und gewünscht, dieses (über 7) an die ÖV Leitstelle zur weiteren Bearbeitung. Sollte sich das Fahrzeug im Betriebshof befinden, so erfolgt die Meldung (über 6) an das BHMS.

- Die Systemüberwachung des AD-Bordsystems leitet stabilisierende Maßnahmen der Fehlerkorrektur, Stabilisierung, Robustheit ein und überprüft ob die Maßnahmen hinreichend wirksam sind.
  - Sofern die Maßnahmen hinreichend sind, erfolgt ein Ereigniseintrag.
    Hinweis: hinreichend bedeutet, daß die Maßnahmen die Störung kompensieren können.
  - Sofern die Maßnahmen unzureichend sind, erfolgt (über 8) eine Warnmeldung (z.B. Meldung: Fehler in der Selbstpositionierung) an die AD-Leitstelle.
    Hinweis: unzureichend bedeutet, daß die Maßnahmen die Störung nur teilweise, jedoch ausreichend, kompensieren können.
    (Warnlampe Gelb)
    Hinweis:
    Abhängig von der Art der Störung kann das AD-Bordsystem durch das Aktivieren des Warnblinkers die Umgebung warnen.
    Folglich kann ein Eingriff der Technischen Aufsicht (TA) der AD-Leitstelle notwendig werden, um den Warnblinker wieder zu deaktivieren oder das Fahrzeug manuell zu übernehmen.
    Hinweis:
    Ein Fehler in der Selbstpositionierung bedeutet, das Fahrzeug fährt gemäß den spezifizierten Regelungsparametern korrekt auf der Straße, aber nicht korrekt zur hochauflösenden Straße. Dieser kann auftreten, wenn in einer Baustelle nach den gelben statt weißen Linien zu fahren ist.
    - Die Technische Aufsicht (TA) der AD-Leitstelle analysiert die Situation und entscheidet über die Eingriffsnotwendigkeit → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).
      Hinweis:
      Da die Abweichung / Störung ausreichend kompensiert werden kann ist kein Minimum Risk Manoeuvre (MRM) erforderlich.
      Hinweis:
      Abhängig von der Art der Störung kann das AD-Bordsystem durch das Aktivieren des Warnblinkers die Umgebung warnen.
      Folglich kann ein Eingriff der Technischen Aufsicht (TA) der AD-Leitstelle notwendig werden, um den Warnblinker wieder zu deaktivieren, (z.B. beim Fahren nach gelben statt weißen Linien) und/oder das Fahrzeug manuell zu übernehmen.
    - Die AD-Leitstelle leitet weitere Maßnahmen zur Erhöhung der Fahrzeugsicherheit ein, damit die Aufrechterhaltung des sicheren Zustandes, trotz der Störung, gewährleistet wird.
      Hinweis:
      Dieses kann z.B. eine Änderung im Toleranzbereich der Sensorwerte sein.
      Dieses kann z.B. eine Änderung der Unterstützungsleistung oder Dämpfung sein.
      Dieses kann z.B. eine Reduzierung der maximal erlaubten Geschwindigkeit sein.
  - Sofern die Maßnahmen ungenügend sind, wird das Minimum Risk Manoeuvre (MRM) ausgeführt und das AD-Bordsystem meldet (über 8) die Systemstörung an die AD-Leitstelle sowie (über 14) an den ÖV-Bordrechner.
    Hinweis: ungenügend bedeutet, daß die Maßnahmen die Störung nicht ausreichend kompensieren können ⚠ Warnlampe Rot.
    Hinweis: Bei einem Minimum Risk Manoeuvre (MRM) ist unabhängig der Kategorie (A bis E) der Warnblinker zu aktivieren und die Technische Aufsicht (TA) der AD-Leitstelle ist verpflichtet unverzüglich Kontakt mit den Insassen des Kraftfahrzeugs herzustellen.
    - Die Technische Aufsicht (TA) der AD-Leitstelle analysiert die Situation und entscheidet über die Eingriffsnotwendigkeit → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.
- AFGBV §12 Anforderungen an den Hersteller Absatz 1 Punkt 2
  Der Hersteller eines Kraftfahrzeugs mit autonomer Fahrfunktion hat
  ein Sicherheitskonzept zur funktionalen Sicherheit nach Anlage I Nummer 7.2 zu erstellen, und dabei
  a) auf Basis dieses Sicherheitskonzeptes eine Gefährdungsanalyse nach Anlage I Ziffer 7.2.1 durchzuführen,
  b) das Sicherheitskonzept nach Anlage III Ziffer 3 zu dokumentieren,
  c) die Sicherheit der autonomen Fahrfunktion entsprechend dieses Sicherheitskonzepts zu überprüfen und die Sicherheit gegenüber dem Kraftfahrt-Bundesamt nach den Anforderungen nach Anlage I Ziffer 10 nachzuweisen.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 3
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihnen

anvertrauten Aufgaben zuverlässig sind; zur Beurteilung ihrer Zuverlässigkeit sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde sowie, bei Einsatz für die Durchführung von Fahrten im manuellen Betrieb, eine Auskunft aus dem Fahrerlaubnisregister vorzulegen; § 8 Absatz 3 gilt entsprechend.

- AFGBV §13 Anforderungen an den Halter Absatz 5
  Die Anforderungen zur Dokumentenverwaltung für die Anweisungen nach Absatz 3 und der Berichte nach Absatz 4 müssen dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik wird vermutet, wenn die Vorgaben der ISO 9001:2015 Qualitätsmanagementsysteme – Grundlagen und Begriffe erfüllt werden. Darüber hinaus muß die Dokumentenverwaltung den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 genügen.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach §1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie in der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik, Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik über einen Abschluß verfügt als
  - Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert),
  - Bachelor, Master oder
  - staatlich geprüfter Techniker.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 2
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie eine entsprechende Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen hat.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 3
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muß, und
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 4
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihr anvertrauten Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes zuverlässig ist.
  Zur Beurteilung der Zuverlässigkeit im Sinne des Satzes 2 Nummer 4 sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde, eine Auskunft aus dem Fahrerlaubnisregister sowie eine Auskunft über Eintragungen aus dem Fahreignungsregister vorzulegen. Sofern in dem Fahrerlaubnisregister mehr als drei Punkte eingetragen sind, ist die Zuverlässigkeit nicht gegeben. § 8 Absatz 3 gilt bezüglich Satz 3 entsprechend.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 2
  Die als Technische Aufsicht eingesetzte natürliche Person darf sich mit Zustimmung des Halters zur Erfüllung ihrer Pflichten weiterer geeigneter natürlicher Personen bedienen, die über mindestens drei Jahre Berufserfahrung im Bereich des Verkehrs- oder Kraftfahrzeugwesens verfügen. Die eingesetzten natürlichen Personen müssen wiederkehrend, mindestens jedoch jährlich beim Hersteller in Bezug auf den Umgang mit dem Kraftfahrzeug sowie wesentliche Veränderungen am Kraftfahrzeug oder der autonomen Fahrfunktion geschult werden. Die Schulung ist mit einer praktischen Prüfung einschließlich der Bewältigung simulierter Betriebsstörungen abzuschließen. Der erfolgreiche Abschluß der Schulung von eingesetzten natürlichen Personen ist von der Technischen Aufsicht zu dokumentieren. Sollen die eingesetzten natürlichen Personen Fahrten im manuellen Fahrbetrieb übernehmen oder Fahrmanöver freigeben, müssen diese Personen eine gültige Fahrerlaubnis besitzen. Die Klasse der Fahrerlaubnis muß der des Fahrzeugs mit autonomer Fahrfunktion entsprechen.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 3
  Befindet sich das Kraftfahrzeug mit autonomer Fahrfunktion im risikominimalen Zustand im Sinne des § 1d Absatz 4 des Straßenverkehrsgesetzes, hat die als Technische Aufsicht eingesetzte natürliche Person eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durchzuführen, bevor sie dessen Beendigung veranlassen darf. Das Ergebnis der Untersuchung ist zu dokumentieren. Wurde der risikominimale Zustand durch einen Defekt am Kraftfahrzeug ausgelöst, muß nach Erreichen des

risikominimalen Zustands die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage 1 Nummer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist ungeachtet der Sätze 1 und 3 das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen. In diesen Fällen erfolgt die Untersuchung der Technischen Aufsicht gemäß Satz 1 im Nachgang des Abtransports auf Grundlage der gespeicherten Fahrdaten.

- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV §15 Datenspeicherung Absatz 2
  Die gespeicherten Daten dürfen nur durch das Kraftfahrt-Bundesamt und die zuständige Behörde und nur zum Zweck der Nachprüfung der Erfüllung der Voraussetzungen der Genehmigung und der mit der Genehmigung verbundenen Überwachungspflichten erhoben, gespeichert und verwendet werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 2 Risikominimaler Zustand
  Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur Ausübung der Fahraufgabe gilt: Das Kraftfahrzeug kann nur auf Veranlassung der Technischen Aufsicht den risikominimalen Zustand verlassen.
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse
  siehe Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.

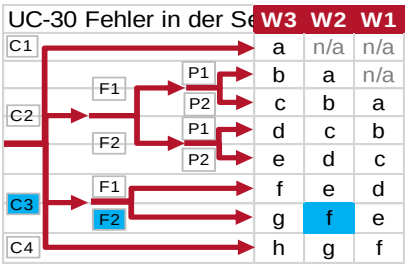
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.

Risikograph:



≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall.
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.31 UC-31 Entscheidungshilfe (Fahrtfortsetzung)

Ein autonomes Fahrzeug wurde nach dem Erkennen eines anomalen Verhaltens / Störung über ein automatisches Minimum Risk Manoeuvre (MRM) durch das AD-Bordsystem in den sicheren Zustand zurück überführt.

Die als Technische Aufsicht eingesetzte natürliche Person führt eine Analyse / Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durch, welches zu dem Ergebnis kommt, daß die Störung

- durch geeignete Maßnahmen behoben werden und damit auch das Minimum Risk Manoeuvre (MRM) beendet werden kann. Eine Fortsetzung der Fahrt ist, ggf. mit Randbedingungen (Einschränkungen) möglich.
- durch einen Defekt am Kraftfahrzeug ausgelöst wurde, weshalb die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage I Ziffer 4 manuell übernommen wird, bis der auslösende Defekt nachhaltig beseitigt worden ist.

Das Ergebnis der Untersuchung wird dokumentiert.

Hinweis:
Die AD-Leitstelle kann, sofern sich das Fahrzeug außerhalb des BHMS befindet, der ÖV-Leitstelle das Entsenden eines Ersatzfahrzeuges vorschlagen. Sollte sich das Fahrzeug auf dem Betriebshof befinden, kann das Fahrzeug durch die Technische Aufsicht (TA) für den Regelbetrieb gesperrt (Ausrückungsverbot) werden.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine *Hinweis:* *Sofern (durch die Eingriffsnotwendigkeit der Technischen Aufsicht) festgestellt wird, daß ein Entsenden eines Ersatzfahrzeug erforderlich sein sollte, entscheidet der ÖV-Disponent über die Einleitung der dispositiven Maßnahmen **über die zugehörigen Use Cases**. Dazu gehört das Entsenden eines Ersatzfahrzeuges oder auch das Einstellen des Umlaufes.* *Die ÖV-Leitstelle informiert über das FGI die wartenden, potentiellen Fahrgäste.*	keine
BHMS	keine *Hinweis:* *Sofern bei der Fahrzeugpflege ein Defekt (durch die Eingriffsnotwendigkeit der Technischen Aufsicht) festgestellt werden sollte, insbesondere wenn dieser die Einsatzfähigkeit des Fahrzeuges verhindert, dann hat das BHMS Maßnahmen der Instandsetzung **über die zugehörigen Servicestationen** einzuleiten, welche die Einsatzfähigkeit des Fahrzeuges wiederherstellen.*	keine
AD-Leitstelle	Fahrzeugüberwachung und Konfiguration der Fahrbereitschaft zur Aufrechterhaltung der Betriebsfortsetzung, sofern möglich. Andernfalls Bergung veranlassen.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Die Eingriffsnotwendigkeit der Technischen Aufsicht (TA) kann sowohl im Regelbetrieb der Fahrgastbeförderung, als auch innerhalb des BHMS bei der Fahrzeugpflege (Service & Wartung) auftreten.

Hinweis:
Das Operator-HMI (AD) übernimmt die Freigabe sowie Steuerung von Fahrfunktionen inklusive Konfliktbehandlung durch den Operator im Fahrzeug im autonomen Fahrbetrieb.

Hinweis:
Das Fahrzeug-Interface stellt lesenden Zugriff auf technische Zustandsdaten des Fahrzeugs (z.B. Batterie-Ladezustand) zur Verfügung.

Hinweis:
Das Verkehrsinfrastruktur-Interface umfaßt die Kommunikation mit ansteuerbaren Verkehrs-Infrastruktur-Elementen auf der Strecke und im Betriebshof (LSA, Poller, Schranke, etc.)

Hinweis:
Das Umwelt-IF (AD) umfaßt die Sensorik zur Umwelterfassung und -kommunikation für das automatisierte Fahren. Hierzu zählen Kameras, Radar, LiDAR, AD-Infrastruktur, C2I-Kommunikation und C2C-Kommunikation. Die Aktorik umfaßt sämtliche Einrichtungen, die zur Durchführung des automatisierten Fahrens benötigt werden (Lenkung, Antrieb, Bremse), sowie Türsteuerung, Blinker, Warnleuchten, Hupe, etc.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Ereignisfall (Besondere Situation / Ereignis → planbarer Regelbetrieb).

Aktionen:

- Das AD-Bordsystem erkennt eine Störung → UC-12 Systemüberwachung und ggf. Störmeldung, welche das AD-Bordsystem nur ungenügend kompensieren kann, somit wird ein Minimum Risk Manoeuvre (MRM) ausgeführt um das Fahrzeug in den sicheren Zustand zu überführen.
  Hinweis: ungenügend bedeutet, daß die Maßnahmen die Störung nicht ausreichend kompensieren können ≙ Warnlampe Rot.
  Hinweis: Bei einem Minimum Risk Manoeuvre (MRM) ist unabhängig der Kategorie (A bis E) der Warnblinker zu aktivieren.
  Hinweis:
  Das AD-Bordsystem meldet Störungen (über 14) informativ an den ÖV-Bordrechner und (über 8) zur Bearbeitung an die AD-Leitstelle. Der ÖV-Bordrechner verarbeitet die Störungsinformation und meldet, sofern sich das Fahrzeug außerhalb des Betriebshofes befindet und gewünscht, dieses (über 7) an die ÖV Leitstelle zur weiteren Bearbeitung. Sollte sich das Fahrzeug im Betriebshof befinden, so erfolgt die Meldung (über 6) an das BHMS.
- Die Technische Aufsicht (TA) der AD-Leitstelle analysiert die Ursache / Auslösung des Minimum Risk Manoeuvres (MRM) und ergreift geeignete Maßnahmen um die Störung zu beheben damit der reibungslose Betrieb wiederaufgenommen / fortgeführt werden kann. Sofern dieses nicht möglich sein sollte werden Maßnahmen ergriffen, welche das Schadenspotential bestmöglich reduzieren. Dazu kann die AD-Leitstelle weitere Daten vom Fahrzeug über das AD-Bordsystem anfordern, z.B.
  - Daten auslesen (über 17) vom Fahrzeug-Interface.
  - Daten auslesen (über 18) vom Verkehrs-Infrastruktur-Interface.
  - Daten lesen und schreiben (über 19) vom Umwelt-Interface AD.
    Hinweis (Randbedingung):
    Die Außenumgebung vor dem Fahrzeug wird (über UM0.19.2 CameraImage) übertragen.
  - Der Fahrgastraum kann (über 15) durch das Operator HMI AD eingesehen werden, hierbei sind die Datenschutzvorschriften nach Artikel 35 der Verordnung (EU) 2016/679, insbesondere die Anforderungen an die Informationstechnik nach Teil 5 und damit den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 einzuhalten. Die Fahrgäste sind vor der Einsicht über das Aktivieren der Kamera dbzgl. anzusprechen (Umsetzung der Informationspflicht).
    Hinweis (Randbedingung):
    Die Innenraumumgebung kann (über UM0.15.3 CamaraImage) eingesehen werden.
  - Das AD-Bordsystem kann auf Basis von Statistikdaten, KI gestützt, Vorschläge zur Behebung der Störung der AD-Leitstelle unterbreiten. ← UC-31 Entscheidungshilfe (Fahrtfortsetzung).
- Sofern das Minimum Risk Manoeuvre (MRM) durch einen Defekt am Kraftfahrzeug ausgelöst wurde, muß die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage I Ziffer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
- Die Technische Aufsicht (TA) der AD-Leitstelle informiert (über 3) die ÖV-Leitstelle falls ein Fahrzeugausfall vorliegen oder eine Außerbetriebnahme sinnvoll sein sollte → UC-27 Ersatzfahrzeug bereitstellen.

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.
- AFGBV §12 Anforderungen an den Hersteller Absatz 1 Punkt 2
  Der Hersteller eines Kraftfahrzeugs mit autonomer Fahrfunktion hat
  ein Sicherheitskonzept zur funktionalen Sicherheit nach Anlage I Nummer 7.2 zu erstellen, und dabei
  a) auf Basis dieses Sicherheitskonzeptes eine Gefährdungsanalyse nach Anlage I Ziffer 7.2.1 durchzuführen,
  b) das Sicherheitskonzept nach Anlage III Ziffer 3 zu dokumentieren,
  c) die Sicherheit der autonomen Fahrfunktion entsprechend dieses Sicherheitskonzepts zu überprüfen und die Sicherheit gegenüber dem Kraftfahrt-Bundesamt nach den Anforderungen nach Anlage I Ziffer 10 nachzuweisen.

- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 3
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihnen anvertrauten Aufgaben zuverlässig sind; zur Beurteilung ihrer Zuverlässigkeit sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde sowie, bei Einsatz für die Durchführung von Fahrten im manuellen Betrieb, eine Auskunft aus dem Fahrerlaubnisregister vorzulegen; § 8 Absatz 3 gilt entsprechend.
- AFGBV §13 Anforderungen an den Halter Absatz 5
  Die Anforderungen zur Dokumentenverwaltung für die Anweisungen nach Absatz 3 und der Berichte nach Absatz 4 müssen dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik wird vermutet, wenn die Vorgaben der ISO 9001:2015 Qualitätsmanagementsysteme – Grundlagen und Begriffe erfüllt werden. Darüber hinaus muß die Dokumentenverwaltung den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 genügen.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach §1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie in der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik, Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik über einen Abschluß verfügt als
  - ► Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert),
  - ► Bachelor, Master oder
  - ► staatlich geprüfter Techniker.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 2
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie eine entsprechende Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen hat.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 3
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muß, und
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 4
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihr anvertrauten Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes zuverlässig ist.
  Zur Beurteilung der Zuverlässigkeit im Sinne des Satzes 2 Nummer 4 sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde, eine Auskunft aus dem Fahrerlaubnisregister sowie eine Auskunft über Eintragungen aus dem Fahreignungsregister vorzulegen. Sofern in dem Fahrerlaubnisregister mehr als drei Punkte eingetragen sind, ist die Zuverlässigkeit nicht gegeben. § 8 Absatz 3 gilt bezüglich Satz 3 entsprechend.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 2
  Die als Technische Aufsicht eingesetzte natürliche Person darf sich mit Zustimmung des Halters zur Erfüllung ihrer Pflichten weiterer geeigneter natürlicher Personen bedienen, die über mindestens drei Jahre Berufserfahrung im Bereich des Verkehrs- oder Kraftfahrzeugwesens verfügen. Die eingesetzten natürlichen Personen müssen wiederkehrend, mindestens jedoch jährlich beim Hersteller in Bezug auf den Umgang mit dem Kraftfahrzeug sowie wesentliche Veränderungen am Kraftfahrzeug oder der autonomen Fahrfunktion geschult werden. Die Schulung ist mit einer praktischen Prüfung einschließlich der Bewältigung simulierter Betriebsstörungen abzuschließen. Der erfolgreiche Abschluß der Schulung von eingesetzten natürlichen Personen ist von der Technischen Aufsicht zu dokumentieren. Sollen die eingesetzten natürlichen Personen Fahrten im manuellen Fahrbetrieb übernehmen oder Fahrmanöver freigeben, müssen diese Personen eine gültige Fahrerlaubnis besitzen. Die Klasse der Fahrerlaubnis muß der des Fahrzeugs mit autonomer Fahrfunktion entsprechen.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 3
  Befindet sich das Kraftfahrzeug mit autonomer Fahrfunktion im risikominimalen Zustand im Sinne des § 1d

Absatz 4 des Straßenverkehrsgesetzes, hat die als Technische Aufsicht eingesetzte natürliche Person eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durchzuführen, bevor sie dessen Beendigung veranlassen darf. Das Ergebnis der Untersuchung ist zu dokumentieren. Wurde der risikominimale Zustand durch einen Defekt am Kraftfahrzeug ausgelöst, muß nach Erreichen des risikominimalen Zustands die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage 1 Nummer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist ungeachtet der Sätze 1 und 3 das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen. In diesen Fällen erfolgt die Untersuchung der Technischen Aufsicht gemäß Satz 1 im Nachgang des Abtransports auf Grundlage der gespeicherten Fahrdaten.

- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV §15 Datenspeicherung Absatz 2
  Die gespeicherten Daten dürfen nur durch das Kraftfahrt-Bundesamt und die zuständige Behörde und nur zum Zweck der Nachprüfung der Erfüllung der Voraussetzungen der Genehmigung und der mit der Genehmigung verbundenen Überwachungspflichten erhoben, gespeichert und verwendet werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 2 Risikominimaler Zustand
  Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur Ausübung der Fahraufgabe gilt: Das Kraftfahrzeug kann nur auf Veranlassung der Technischen Aufsicht den risikominimalen Zustand verlassen.
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse
  siehe Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.

Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

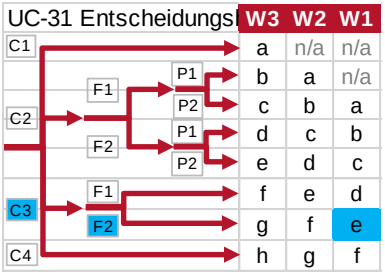
Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.

- Die angemessene Sicherheit der Fahrgäste während der Fahrt obliegt zum großen Anteil den Systemen der autonomen Fahrt des Fahrzeugherstellers (OEM) oder dem Hersteller des AD-Tuning-Kits, welche im Gefahrenfall ein Minimum Risk Manoeuvre (MRM) umsetzen, weshalb der verbleibende Anteil einer Störungsmeldung als informativ QM (C) betrachtet werden kann, **aber hier meldet das Fahrzeug (OEM), daß seine Systemgrenze der Handlungsfähigkeit überschritten wurde, weshalb das Fahrzeug (OEM) Unterstützung durch einen Operator anfordert.**
  ISO-26262-03:2018 Clause 7.4.3.1 Sicherheitsanforderungen müssen dem Automotive Safety Integrity Level (ASIL) der Funktion und dem zugehörigen Sicherheitsziel entsprechen.
  Hinweis Fahrt = ASIL-C.

  Hinweis:
  Dieser Use Case betrachtet den Fall nach der sicheren Fehlererkennung, welcher mit Hilfe der Leitworte aufgedeckt / erkannt werden soll. Je nach Art der Störung kann jedes Leitwort dafür angewendet worden sein.
- Vor dem Wiederanfahren / Fortsetzen der Fahrt, (sofern möglich und erlaubt), sind die (insbesondere stehenden) Fahrgäste vorzuwarnen, damit diese nicht von der Anfahrt überrascht werden und dadurch (anders als erwartet) Stürzen, weil die Fahrgäste keinen (nicht) sicheren Stand hatten bzw. sich nicht festgehalten haben.

Risikograph:



UC-31 Entscheidungsl	W3	W2	W1
C1	a	n/a	n/a
C2 F1 P1	b	a	n/a
C2 F1 P2	c	b	a
C2 F2 P1	d	c	b
C2 F2 P2	e	d	c
C3 F1	f	e	d
C3 F2	g	f	e
C4	h	g	f

≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall.
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
✖	
W1	Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.32 UC-32 Detektion von Trajektorien Abweichung

Erkennung von Abweichungen der gefahrenen Trajektorie des AD-Fahrzeugs von der (ggfs. von der Infrastruktur) vorgegebenen Trajektorie und Erzeugung einer entsprechenden Fehlernachricht. Anschließend, nach dem UseCase, ist dann eine entsprechende Maßnahme (beispielsweise "Risikominimalen Zustand einnehmen", "Geschwindigkeit reduzieren" oder "Fahrt zu bestimmtem Haltepunkt") vom Fahrzeug oder von der AD-Zentrale veranlaßt nötig.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine	keine
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung und Konfiguration der Fahrbereitschaft zur Aufrechterhaltung der Betriebsfortsetzung, sofern möglich. Andernfalls Bergung veranlassen.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Das Operator-HMI (AD) übernimmt die Freigabe sowie Steuerung von Fahrfunktionen inklusive Konfliktbehandlung durch den Operator im Fahrzeug im autonomen Fahrbetrieb.

Hinweis:
Das Fahrzeug-Interface stellt lesenden Zugriff auf technische Zustandsdaten des Fahrzeugs (z.B. Batterie-Ladezustand) zur Verfügung.

Hinweis:
Das Verkehrsinfrastruktur-Interface umfaßt die Kommunikation mit ansteuerbaren Verkehrs-Infrastruktur-Elementen auf der Strecke und im Betriebshof (LSA, Poller, Schranke, etc.)

Hinweis:
Das Umwelt-IF (AD) umfaßt die Sensorik zur Umwelterfassung und -kommunikation für das automatisierte Fahren. Hierzu zählen Kameras, Radar, LiDAR, AD-Infrastruktur, C2I-Kommunikation und C2C-Kommunikation. Die Aktorik umfaßt sämtliche Einrichtungen, die zur Durchführung des automatisierten Fahrens benötigt werden (Lenkung, Antrieb, Bremse), sowie Türsteuerung, Blinker, Warnleuchten, Hupe, etc.

Hinweis:
Die Eingriffsnotwendigkeit der Technischen Aufsicht (TA) kann sowohl im Regelbetrieb der Fahrgastbeförderung, als auch innerhalb des BHMS bei der Fahrzeugpflege (Service & Wartung) auftreten.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Ereignisfall (Besondere Situation / Ereignis → planbarer Regelbetrieb).

Aktionen (Fahrzeugsystemüberwachung durch das AD-Bordsystem):

- Das AD-Bordsystem überwacht kontinuierlich die autonome Fahrt über die Sensorik und die Peripherie des Fahrzeuges und sendet technische Informationen (über 8) an die AD-Leitstelle.
- Das AD-Bordsystem erkennt eine Störung → UC-12 Systemüberwachung und ggf. Störmeldung.
  Hinweis:
  Das AD-Bordsystem meldet Störungen (über 14) informativ an den ÖV-Bordrechner und (über 8) zur Bearbeitung an die AD-Leitstelle. Der ÖV-Bordrechner verarbeitet die Störungsinformation und meldet, sofern sich das Fahrzeug außerhalb des Betriebshofes befindet und gewünscht, dieses (über 7) an die ÖV Leitstelle zur weiteren Bearbeitung. Sollte sich das Fahrzeug im Betriebshof befinden, so erfolgt die Meldung (über 6) an das BHMS.

- Die Systemüberwachung des AD-Bordsystems leitet stabilisierende Maßnahmen der Fehlerkorrektur, Stabilisierung, Robustheit ein und überprüft ob die Maßnahmen hinreichend wirksam sind.
  - Sofern die Maßnahmen hinreichend sind, erfolgt ein Ereigniseintrag.
    Hinweis: hinreichend bedeutet, daß die Maßnahmen die Störung kompensieren können.
  - Sofern die Maßnahmen unzureichend sind, erfolgt (über 8) eine Warnmeldung (z.B. Meldung: Fehler Trajektorien Abweichung festgestellt) an die AD-Leitstelle.
    Hinweis: unzureichend bedeutet, daß die Maßnahmen die Störung nur teilweise, jedoch ausreichend, kompensieren können.
    (Warnlampe Gelb)
    Hinweis:
    Abhängig von der Art der Störung kann das AD-Bordsystem durch das Aktivieren des Warnblinkers die Umgebung warnen.
    Folglich kann ein Eingriff der Technischen Aufsicht (TA) der AD-Leitstelle notwendig werden, um den Warnblinker wieder zu deaktivieren oder das Fahrzeug manuell zu übernehmen.
    Hinweis:
    Ein Fehler in der Trajektorie bedeutet, das Fahrzeug fährt abweichend zu den spezifizierten Regelungsparametern (außerhalb der Toleranz) noch einigermaßen korrekt (zumindest in der korrekten Richtung) auf der Straße, aber nicht korrekt zum (bestimmten, vorgegebenen) Sollwert.
    - Die Technische Aufsicht (TA) der AD-Leitstelle analysiert die Situation und entscheidet über die Eingriffsnotwendigkeit → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).
      Hinweis:
      Da die Abweichung / Störung ausreichend kompensiert werden kann, ist kein Minimum Risk Manoeuvre (MRM) erforderlich.
      Hinweis:
      Abhängig von der Art der Störung kann das AD-Bordsystem durch das Aktivieren des Warnblinkers die Umgebung warnen.
      Folglich kann ein Eingriff der Technischen Aufsicht (TA) der AD-Leitstelle notwendig werden, um den Warnblinker wieder zu deaktivieren, (z.B. beim Fahren nach gelben statt weißen Linien) und/oder das Fahrzeug manuell zu übernehmen.
    - Die AD-Leitstelle leitet weitere Maßnahmen zur Erhöhung der Fahrzeugsicherheit ein, damit die Aufrechterhaltung des sicheren Zustandes, trotz der Störung, gewährleistet wird.
      Hinweis:
      Dieses kann z.B. eine Änderung im Toleranzbereich der Sensorwerte sein.
      Dieses kann z.B. eine Änderung der Unterstützungsleistung oder Dämpfung sein
      Dieses kann z.B. eine Reduzierung der maximal erlaubten Geschwindigkeit sein.
  - Sofern die Maßnahmen ungenügend sind, wird das Minimum Risk Manoeuvre (MRM) ausgeführt und das AD-Bordsystem meldet (über 8) die Systemstörung an die AD-Leitstelle sowie (über 14) an den ÖV-Bordrechner.
    Hinweis: ungenügend bedeutet, daß die Maßnahmen die Störung nicht ausreichend kompensieren können ⚠ Warnlampe Rot.
    Hinweis: Bei einem Minimum Risk Manoeuvre (MRM) ist unabhängig der Kategorie (A bis E) der Warnblinker zu aktivieren und die Technische Aufsicht (TA) der AD-Leitstelle ist verpflichtet unverzüglich Kontakt mit den Insassen des Kraftfahrzeugs herzustellen.
- Die Technische Aufsicht (TA) der AD-Leitstelle analysiert die Situation und entscheidet über die Eingriffsnotwendigkeit → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).

Aktionen (Fahrzeugüberwachung durch die AD-Leitstelle):

- Die Technische Aufsicht (TA) der AD-Leitstelle erkennt die Abweichung, analysiert die Situation und entscheidet über die Eingriffsnotwendigkeit → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).
  Hinweis:
  Die Fahrzeugüberwachung wird durch das Video der Außenkamera, der kontinuierlichen Statusmeldungen und ggf. auch durch priorisierte Störmeldungen aus UC-12 unterstützt.

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.
- AFGBV §12 Anforderungen an den Hersteller Absatz 1 Punkt 2
  Der Hersteller eines Kraftfahrzeugs mit autonomer Fahrfunktion hat
  ein Sicherheitskonzept zur funktionalen Sicherheit nach Anlage I Nummer 7.2 zu erstellen, und dabei
  a) auf Basis dieses Sicherheitskonzeptes eine Gefährdungsanalyse nach Anlage I Ziffer 7.2.1 durchzuführen,
  b) das Sicherheitskonzept nach Anlage III Ziffer 3 zu dokumentieren,

c) die Sicherheit der autonomen Fahrfunktion entsprechend dieses Sicherheitskonzepts zu überprüfen und die Sicherheit gegenüber dem Kraftfahrt-Bundesamt nach den Anforderungen nach Anlage I Ziffer 10 nachzuweisen.

- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 3
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihnen anvertrauten Aufgaben zuverlässig sind; zur Beurteilung ihrer Zuverlässigkeit sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde sowie, bei Einsatz für die Durchführung von Fahrten im manuellen Betrieb, eine Auskunft aus dem Fahrerlaubnisregister vorzulegen; § 8 Absatz 3 gilt entsprechend.
- AFGBV §13 Anforderungen an den Halter Absatz 5
  Die Anforderungen zur Dokumentenverwaltung für die Anweisungen nach Absatz 3 und der Berichte nach Absatz 4 müssen dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik wird vermutet, wenn die Vorgaben der ISO 9001:2015 Qualitätsmanagementsysteme – Grundlagen und Begriffe erfüllt werden. Darüber hinaus muß die Dokumentenverwaltung den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 genügen.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach §1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie in der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik, Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik über einen Abschluß verfügt als
  - ► Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert),
  - ► Bachelor, Master oder
  - ► staatlich geprüfter Techniker.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 2
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie eine entsprechende Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen hat.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 3
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muß, und
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 4
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihr anvertrauten Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes zuverlässig ist.
  Zur Beurteilung der Zuverlässigkeit im Sinne des Satzes 2 Nummer 4 sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde, eine Auskunft aus dem Fahrerlaubnisregister sowie eine Auskunft über Eintragungen aus dem Fahreignungsregister vorzulegen. Sofern in dem Fahrerlaubnisregister mehr als drei Punkte eingetragen sind, ist die Zuverlässigkeit nicht gegeben. § 8 Absatz 3 gilt bezüglich Satz 3 entsprechend.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 2
  Die als Technische Aufsicht eingesetzte natürliche Person darf sich mit Zustimmung des Halters zur Erfüllung ihrer Pflichten weiterer geeigneter natürlicher Personen bedienen, die über mindestens drei Jahre Berufserfahrung im Bereich des Verkehrs- oder Kraftfahrzeugwesens verfügen. Die eingesetzten natürlichen Personen müssen wiederkehrend, mindestens jedoch jährlich beim Hersteller in Bezug auf den Umgang mit dem Kraftfahrzeug sowie wesentliche Veränderungen am Kraftfahrzeug oder der autonomen Fahrfunktion geschult werden. Die Schulung ist mit einer praktischen Prüfung einschließlich der Bewältigung simulierter Betriebsstörungen abzuschließen. Der erfolgreiche Abschluß der Schulung von eingesetzten natürlichen Personen ist von der Technischen Aufsicht zu dokumentieren. Sollen die eingesetzten natürlichen Personen Fahrten im manuellen Fahrbetrieb übernehmen oder Fahrmanöver freigeben, müssen diese Personen eine

gültige Fahrerlaubnis besitzen. Die Klasse der Fahrerlaubnis muß der des Fahrzeugs mit autonomer Fahrfunktion entsprechen.

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 3
  Befindet sich das Kraftfahrzeug mit autonomer Fahrfunktion im risikominimalen Zustand im Sinne des § 1d Absatz 4 des Straßenverkehrsgesetzes, hat die als Technische Aufsicht eingesetzte natürliche Person eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durchzuführen, bevor sie dessen Beendigung veranlassen darf. Das Ergebnis der Untersuchung ist zu dokumentieren. Wurde der risikominimale Zustand durch einen Defekt am Kraftfahrzeug ausgelöst, muß nach Erreichen des risikominimalen Zustands die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage 1 Nummer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
  Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist ungeachtet der Sätze 1 und 3 das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen. In diesen Fällen erfolgt die Untersuchung der Technischen Aufsicht gemäß Satz 1 im Nachgang des Abtransports auf Grundlage der gespeicherten Fahrdaten.
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV §15 Datenspeicherung Absatz 2
  Die gespeicherten Daten dürfen nur durch das Kraftfahrt-Bundesamt und die zuständige Behörde und nur zum Zweck der Nachprüfung der Erfüllung der Voraussetzungen der Genehmigung und der mit der Genehmigung verbundenen Überwachungspflichten erhoben, gespeichert und verwendet werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 2 Risikominimaler Zustand
  Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur Ausübung der Fahraufgabe gilt: Das Kraftfahrzeug kann nur auf Veranlassung der Technischen Aufsicht den risikominimalen Zustand verlassen.
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse
  siehe Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.

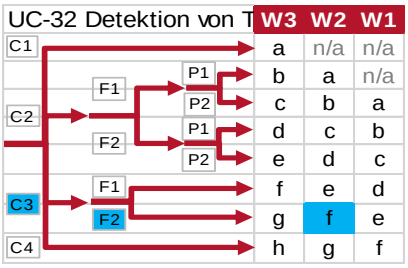
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

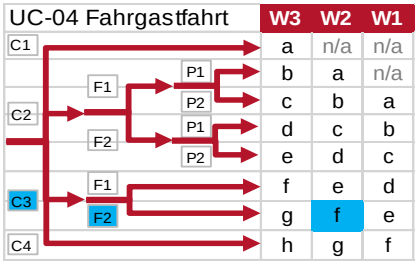
Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.

Risikograph:



≙ ASIL-C ←



≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall.
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.33 UC-33 Interpretation des fahrzeuginternen Systemzustandes

Zustandsdaten einzelner Komponenten des automatisierten Fahrsystems im AD-Fahrzeug werden für die AD-Leitstelle interpretierbar gemacht. Liefert ein Sensor des AD-Fahrzeugs bspw. über einen bestimmten Zeitraum keine Daten mehr und beeinträchtigt somit den Fahrbetrieb, so wird dieses an die AD-Leitstelle kommuniziert. In diesem Fall werden die Informationen über den Ausfall des Sensors oder der Kommunikation mit dem Sensor als Fehlverhalten interpretiert. Auch bei Nicht-Auftreten von Fehlern einzelner Systemkomponenten werden die fahrzeuginternen Systemzustände an die technische Aufsicht in der AD-Leitstelle weitergegeben.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine	keine
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung und Konfiguration der Fahrbereitschaft zur Aufrechterhaltung der Betriebsfortsetzung, sofern möglich. Andernfalls Bergung veranlassen.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Das Operator-HMI (AD) übernimmt die Freigabe sowie Steuerung von Fahrfunktionen inklusive Konfliktbehandlung durch den Operator im Fahrzeug im autonomen Fahrbetrieb.

Hinweis:
Das Fahrzeug-Interface stellt lesenden Zugriff auf technische Zustandsdaten des Fahrzeugs (z.B. Batterie-Ladezustand) zur Verfügung.

Hinweis:
Das Verkehrsinfrastruktur-Interface umfaßt die Kommunikation mit ansteuerbaren Verkehrs-Infrastruktur-Elementen auf der Strecke und im Betriebshof (LSA, Poller, Schranke, etc.)

Hinweis:
Das Umwelt-IF (AD) umfaßt die Sensorik zur Umwelterfassung und -kommunikation für das automatisierte Fahren. Hierzu zählen Kameras, Radar, LiDAR, AD-Infrastruktur, C2I-Kommunikation und C2C-Kommunikation. Die Aktorik umfaßt sämtliche Einrichtungen, die zur Durchführung des automatisierten Fahrens benötigt werden (Lenkung, Antrieb, Bremse), sowie Türsteuerung, Blinker, Warnleuchten, Hupe, etc.

Hinweis:
Die Eingriffsnotwendigkeit der Technischen Aufsicht (TA) kann sowohl im Regelbetrieb der Fahrgastbeförderung, als auch innerhalb des BHMS bei der Fahrzeugpflege (Service & Wartung) auftreten.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Ereignisfall (Besondere Situation / Ereignis → planbarer Regelbetrieb).

Aktionen:

- Die Systemüberwachung des AD-Bordsystems leitet stabilisierende Maßnahmen der Fehlerkorrektur, Stabilisierung, Robustheit ein und überprüft ob die Maßnahmen hinreichend wirksam sind.
  - Sofern die Maßnahmen hinreichend sind, erfolgt ein Ereigniseintrag.
    Hinweis: hinreichend bedeutet, daß die Maßnahmen die Störung kompensieren können.
  - Sofern die Maßnahmen unzureichend sind, erfolgt (über 8) eine Warnmeldung (z.B. Meldung: Fehler bei Sensor […], die Sensordaten werden nur sporadisch übermittelt) an die AD-Leitstelle.
    Hinweis: unzureichend bedeutet, daß die Maßnahmen die Störung nur teilweise, jedoch ausreichend, kompensieren können.
    (Warnlampe Gelb)
    Hinweis:
    Abhängig von der Art der Störung kann das AD-Bordsystem durch das Aktivieren des Warnblinkers die Umgebung warnen.
    Folglich kann ein Eingriff der Technischen Aufsicht (TA) der AD-Leitstelle notwendig werden, um den Warnblinker wieder zu deaktivieren oder das Fahrzeug manuell zu übernehmen.
    Hinweis:
    Diese Use Case beschreibt das Erkennen von fehlenden / ausbleibenden Sensordaten.
    - Die Technische Aufsicht (TA) der AD-Leitstelle analysiert die Situation und entscheidet über die Eingriffsnotwendigkeit → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).
      Hinweis:
      Da die Abweichung / Störung ausreichend kompensiert werden kann, ist kein Minimum Risk Manoeuvre (MRM) erforderlich.
      Hinweis:
      Abhängig von der Art der Störung kann das AD-Bordsystem durch das Aktivieren des Warnblinkers die Umgebung warnen.
      Folglich kann ein Eingriff der Technischen Aufsicht (TA) der AD-Leitstelle notwendig werden, um den Warnblinker wieder zu deaktivieren, (z.B. beim Fahren nach gelben statt weißen Linien) und/oder das Fahrzeug manuell zu übernehmen.
      Hinweis:
      Bei diesem Fehlerfall werden die sicheren Zeitersatzwerte aus der Absicherung Robustheit (Gegenmaßnahme) verwendet, jedoch ist dadurch die Regelschleife beeinträchtigt, d.h. es kann zu einer leicht ruckelnden Fahrt führen, welche den Fahrkomfort der Fahrgäste für sie deutlich spürbar beeinträchtigt.
    - Die AD-Leitstelle leitet weitere Maßnahmen zur Erhöhung der Fahrzeugsicherheit ein, damit die Aufrechterhaltung des sicheren Zustandes, trotz der Störung, gewährleistet wird.
      Hinweis:
      Dieses kann z.B. eine Änderung im Toleranzbereich der Sensorwerte sein.
      Dieses kann z.B. eine Änderung der Unterstützungsleistung oder Dämpfung sein
      Dieses kann z.B. eine Reduzierung der maximal erlaubten Geschwindigkeit sein.
  - Sofern die Maßnahmen ungenügend sind, wird das Minimum Risk Manoeuvre (MRM) ausgeführt und das AD-Bordsystem meldet (über 8) die Systemstörung an die AD-Leitstelle sowie (über 14) an den ÖV-Bordrechner.
    Hinweis: ungenügend bedeutet, daß die Maßnahmen die Störung nicht ausreichend kompensieren können ⚠ Warnlampe Rot.
    Hinweis: Bei einem Minimum Risk Manoeuvre (MRM) ist unabhängig der Kategorie (A bis E) der Warnblinker zu aktivieren und die Technische Aufsicht (TA) der AD-Leitstelle ist verpflichtet unverzüglich Kontakt mit den Insassen des Kraftfahrzeugs herzustellen.
- Die Technische Aufsicht (TA) der AD-Leitstelle analysiert die Situation und entscheidet über die Eingriffsnotwendigkeit → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.
- AFGBV §12 Anforderungen an den Hersteller Absatz 1 Punkt 2
  Der Hersteller eines Kraftfahrzeugs mit autonomer Fahrfunktion hat
  ein Sicherheitskonzept zur funktionalen Sicherheit nach Anlage I Nummer 7.2 zu erstellen, und dabei
  a) auf Basis dieses Sicherheitskonzeptes eine Gefährdungsanalyse nach Anlage I Ziffer 7.2.1 durchzuführen,
  b) das Sicherheitskonzept nach Anlage III Ziffer 3 zu dokumentieren,
  c) die Sicherheit der autonomen Fahrfunktion entsprechend dieses Sicherheitskonzepts zu überprüfen und die

Sicherheit gegenüber dem Kraftfahrt-Bundesamt nach den Anforderungen nach Anlage I Ziffer 10 nachzuweisen.

- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 3
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihnen anvertrauten Aufgaben zuverlässig sind; zur Beurteilung ihrer Zuverlässigkeit sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde sowie, bei Einsatz für die Durchführung von Fahrten im manuellen Betrieb, eine Auskunft aus dem Fahrerlaubnisregister vorzulegen; § 8 Absatz 3 gilt entsprechend.
- AFGBV §13 Anforderungen an den Halter Absatz 5
  Die Anforderungen zur Dokumentenverwaltung für die Anweisungen nach Absatz 3 und der Berichte nach Absatz 4 müssen dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik wird vermutet, wenn die Vorgaben der ISO 9001:2015 Qualitätsmanagementsysteme – Grundlagen und Begriffe erfüllt werden. Darüber hinaus muß die Dokumentenverwaltung den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 genügen.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach §1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie in der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik, Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik über einen Abschluß verfügt als
  - Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert),
  - Bachelor, Master oder
  - staatlich geprüfter Techniker.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 2
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie eine entsprechende Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen hat.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 3
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muß, und
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 4
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihr anvertrauten Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes zuverlässig ist.
  Zur Beurteilung der Zuverlässigkeit im Sinne des Satzes 2 Nummer 4 sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde, eine Auskunft aus dem Fahrerlaubnisregister sowie eine Auskunft über Eintragungen aus dem Fahreignungsregister vorzulegen. Sofern in dem Fahrerlaubnisregister mehr als drei Punkte eingetragen sind, ist die Zuverlässigkeit nicht gegeben. § 8 Absatz 3 gilt bezüglich Satz 3 entsprechend.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 2
  Die als Technische Aufsicht eingesetzte natürliche Person darf sich mit Zustimmung des Halters zur Erfüllung ihrer Pflichten weiterer geeigneter natürlicher Personen bedienen, die über mindestens drei Jahre Berufserfahrung im Bereich des Verkehrs- oder Kraftfahrzeugwesens verfügen. Die eingesetzten natürlichen Personen müssen wiederkehrend, mindestens jedoch jährlich beim Hersteller in Bezug auf den Umgang mit dem Kraftfahrzeug sowie wesentliche Veränderungen am Kraftfahrzeug oder der autonomen Fahrfunktion geschult werden. Die Schulung ist mit einer praktischen Prüfung einschließlich der Bewältigung simulierter Betriebsstörungen abzuschließen. Der erfolgreiche Abschluß der Schulung von eingesetzten natürlichen Personen ist von der Technischen Aufsicht zu dokumentieren. Sollen die eingesetzten natürlichen Personen Fahrten im manuellen Fahrbetrieb übernehmen oder Fahrmanöver freigeben, müssen diese Personen eine gültige Fahrerlaubnis besitzen. Die Klasse der Fahrerlaubnis muß der des Fahrzeugs mit autonomer Fahrfunktion entsprechen.

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 3
  Befindet sich das Kraftfahrzeug mit autonomer Fahrfunktion im risikominimalen Zustand im Sinne des § 1d Absatz 4 des Straßenverkehrsgesetzes, hat die als Technische Aufsicht eingesetzte natürliche Person eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durchzuführen, bevor sie dessen Beendigung veranlassen darf. Das Ergebnis der Untersuchung ist zu dokumentieren. Wurde der risikominimale Zustand durch einen Defekt am Kraftfahrzeug ausgelöst, muß nach Erreichen des risikominimalen Zustands die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage 1 Nummer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
  Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist ungeachtet der Sätze 1 und 3 das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen. In diesen Fällen erfolgt die Untersuchung der Technischen Aufsicht gemäß Satz 1 im Nachgang des Abtransports auf Grundlage der gespeicherten Fahrdaten.
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV §15 Datenspeicherung Absatz 2
  Die gespeicherten Daten dürfen nur durch das Kraftfahrt-Bundesamt und die zuständige Behörde und nur zum Zweck der Nachprüfung der Erfüllung der Voraussetzungen der Genehmigung und der mit der Genehmigung verbundenen Überwachungspflichten erhoben, gespeichert und verwendet werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 2 Risikominimaler Zustand
  Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur Ausübung der Fahraufgabe gilt: Das Kraftfahrzeug kann nur auf Veranlassung der Technischen Aufsicht den risikominimalen Zustand verlassen.
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse
  siehe Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.

Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

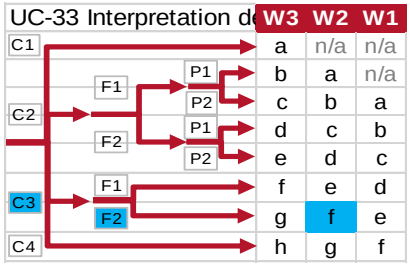
Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.

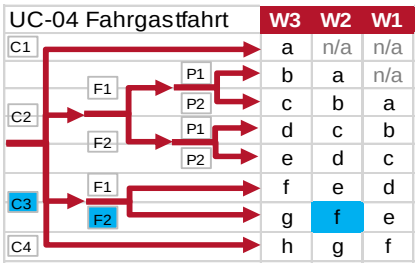
Hinweis:
*Dieser Use Case betrachtet / beschreibt **bewußt eine durch Maßnahmen korrigierbare** oder zumindest Gefahren minimierbare Situation. Sollte kein sicherer Zeitersatzwert verfügbar bzw. möglich sein (z.B. Sensorbeeinträchtigung bei der Umgebungserfassung, Hüllbox), weshalb Gegenstände oder Personen im Umfeld des Kraftfahrzeugs nicht korrekt erfaßt werden, welches einen schweren Unfall zur Folge haben könnte, ist ein automatisiertes Minimum Risk Manoeuvre (MRM) zwingend umzusetzen.*

Hinweis:
Wenn sichere Zeitersatzwerte nicht möglich sind, kann es auch keine unzureichenden Maßnahmen (welche die Störung nur teilweise, jedoch ausreichend, kompensieren können) geben.
Folglich können nur ungenügende Maßnahmen implementiert sein, welches der Warnlampe Rot entspricht, die den Fahrzeugführer, im konventionellen Betrieb, zum unverzüglichen Anhalten auffordert.

Risikograph:



≙ ASIL-C ←



≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall.
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.34 UC-34 Interpretation des Gesamtsystemzustandes zwischen Infrastruktur/Leitstelle und Fahrzeug

Informationszustände einzelner Systemkomponenten der autonomen Fahrerassistenzsysteme des AD-Fahrzeugs werden periodisch konsolidiert, interpretiert und zusammengefaßt zu einem Gesamtsystem-„Gesundheitszustand“. Dieser Zustand wird periodisch an die AD-Leitstelle übertragen. In der AD-Leitstelle wird die Information visualisiert und bei aktuellen Störungsfällen wird die Information für die Technische Aufsicht verfügbar gemacht.

Hinweis:
Solange keine anomalen Werte / Störungen erkannt werden, welche einen Eingriff der Technischen Aufsicht (TA) der AD-Leitstelle erforderlich machen, werden die überwachten, technischen Signalwerte in dem Ereignisspeicher im Hintergrund hinterlegt. Sobald eine Störung erkannt wird, werden die zugehörigen Ereignismeldungen (über geeignete Filter) der Technischen Aufsicht (TA) automatisiert von der Benutzeroberfläche (GUI) der AD-Leitstelle mit Priorisierung (ggf. farblich hervorgehoben) zur Verfügung gestellt.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine	keine
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung und Konfiguration der Fahrbereitschaft zur Aufrechterhaltung der Betriebsfortsetzung, sofern möglich. Andernfalls Bergung veranlassen.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Das Operator-HMI (AD) übernimmt die Freigabe sowie Steuerung von Fahrfunktionen inklusive Konfliktbehandlung durch den Operator im Fahrzeug im autonomen Fahrbetrieb.

Hinweis:
Das Fahrzeug-Interface stellt lesenden Zugriff auf technische Zustandsdaten des Fahrzeugs (z.B. Batterie-Ladezustand) zur Verfügung.

Hinweis:
Das Verkehrsinfrastruktur-Interface umfaßt die Kommunikation mit ansteuerbaren Verkehrs-Infrastruktur-Elementen auf der Strecke und im Betriebshof (LSA, Poller, Schranke, etc.)

Hinweis:
Das Umwelt-IF (AD) umfaßt die Sensorik zur Umwelterfassung und -kommunikation für das automatisierte Fahren. Hierzu zählen Kameras, Radar, LiDAR, AD-Infrastruktur, C2I-Kommunikation und C2C-Kommunikation. Die Aktorik umfaßt sämtliche Einrichtungen, die zur Durchführung des automatisierten Fahrens benötigt werden (Lenkung, Antrieb, Bremse), sowie Türsteuerung, Blinker, Warnleuchten, Hupe, etc.

Hinweis:
Die Eingriffsnotwendigkeit der Technischen Aufsicht (TA) kann sowohl im Regelbetrieb der Fahrgastbeförderung, als auch innerhalb des BHMS bei der Fahrzeugpflege (Service & Wartung) auftreten.

Hinweis:
Dieser Use Case beschreibt Anforderungen an die Benutzeroberfläche / Graphical User Interface (GUI) ≙ Anwendersoftware ≙ App, womit der Operator der Technischen Aufsicht (TA) der AD-Leitstelle arbeitet.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Datenvorhaltung und -visualisierung in der AD-Leitstelle (Regelbetrieb).

Aktionen:

- Das AD-Bordsystem überwacht kontinuierlich die autonome Fahrt über die Sensorik und die Peripherie des Fahrzeugs und sendet technische Informationen (über 8) an die AD-Leitstelle.
- Die Benutzeroberfläche / Graphical User Interface (GUI) ≙ Anwendersoftware ≙ App der AD-Leitstelle visualisiert die Information zur erleichterten Wahrnehmung und Unterstützung des menschlichen Operators der Technischen Aufsicht (TA).
- Sobald eine Störungsmeldung eintrifft, wird diese dem Operator, graphisch aufbereitet, angezeigt.

Juristische Anforderungen:

- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als

Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.

- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.

Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

Gefahren nach HAZOP:

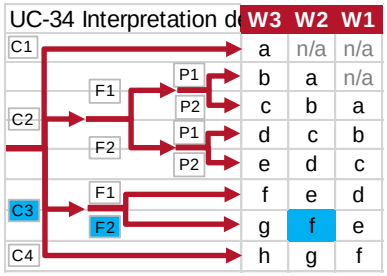
- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.
- Die GUI muß dem Operator die relevanten Informationen vollständig anzeigen. (Vollständigkeit)
  (Die Filterung der Ereignisse darf relevante Informationen nicht entfernen / verschweigen).
- Die GUI muß dem Operator nur die relevanten Informationen anzeigen. (Übersichtlichkeit)
  (Die Filterung der Ereignisse darf nicht mehr Informationen anzeigen als benötigt).
- Die GUI muß dem Operator alle relevanten Informationen anzeigen. (Übersichtlichkeit)
  (Die Filterung der Ereignisse darf nicht weniger Informationen anzeigen als benötigt).
- Die GUI muß dem Operator nur die benötigten Informationen anzeigen. (Übersichtlichkeit)
  (Die Filterung der Ereignisse darf nicht gleichzeitig sowohl als auch relevante sowie nicht relevante Informationen anzeigen).

Hinweis:
Obige Liste kann mit den Leitworten weiter vervollständigt werden, jedoch ist es nicht wirklich zielführend, da keine neuen Erkenntnisse hinzukommen.

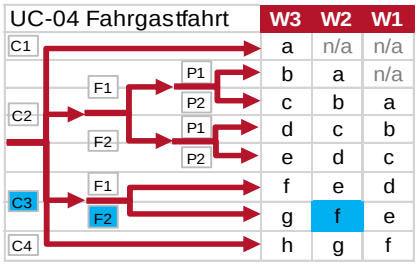
Risikograph (Verfügbarkeit der relevanten Daten):

Hinweis:
*Wenn relevante Daten fehlen und nicht rechtzeitig angezeigt werden, dann kann dieses **zu Fehlentscheidungen führen**, welche eine Gefahr für Leib und Leben auslösen können.*

Hinweis:
Fehlende Informationen führen zu einer Nicht-Beherrschbarkeit = C3 Difficult to control or uncontrollable gemäß ISO-26262 Band 3: 2018 – Tabelle 3.
In Kombination zum Schadenspotential S3 Life-threatening injuries (survival uncertain), fatal injuries
und der Auftretenswahrscheinlichkeit E4 High probability ≙ Highway / Country Road (Tabelle B2)
führt dieses zu einer ASIL-D Bewertung, aber da AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1 und AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1 ausschließlich technisch qualifiziertes Personal (Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfter Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann) einfordert, reduziert sich die Auftretenswahrscheinlichkeit (fehlende Informationen werden erkannt und im Bedarfsfall eingesehen) auf E3 Medium probability → ASIL-C.



≙ ASIL-C ←



≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall.
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.35 UC-35 Detektion von Abweichungen in Sensordaten zwischen Fahrzeug und Infrastruktur

Sensordaten aus dem AD-Fahrzeug werden an Detektionskomponenten übermittelt. Gleichzeitig werden Daten aus der AD-Infrastruktur herangezogen und basierend darauf die Abweichung und deren Kritikalität bestimmt. Abweichungen können zwischen gleich- oder verschiedenartigen Daten erfolgen. So können z.B. die erkannten Objekte des automatisierten Fahrsystems des AD-Fahrzeugs mit denen der AD-Infrastruktur abgeglichen werden. Ein anderes Beispiel wäre die Position des AD-Fahrzeugs mit dem jeweiligen Objekt, welches die AD-Infrastruktur erkannt hat, miteinander zu vergleichen.

Beispiele: Umgebungsobjekte oder Lichtsignalanlage

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine	keine
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung und Konfiguration der Fahrbereitschaft zur Aufrechterhaltung der Betriebsfortsetzung, sofern möglich. Andernfalls Bergung veranlassen.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Das Operator-HMI (AD) übernimmt die Freigabe sowie Steuerung von Fahrfunktionen inklusive Konfliktbehandlung durch den Operator im Fahrzeug im autonomen Fahrbetrieb.

Hinweis:
Das Fahrzeug-Interface stellt lesenden Zugriff auf technische Zustandsdaten des Fahrzeugs (z.B. Batterie-Ladezustand) zur Verfügung.

Hinweis:
Das Verkehrsinfrastruktur-Interface umfaßt die Kommunikation mit ansteuerbaren Verkehrs-Infrastruktur-Elementen auf der Strecke und im Betriebshof (LSA, Poller, Schranke, etc.)

Hinweis:
Das Umwelt-IF (AD) umfaßt die Sensorik zur Umwelterfassung und -kommunikation für das automatisierte Fahren. Hierzu zählen Kameras, Radar, LiDAR, AD-Infrastruktur, C2I-Kommunikation und C2C-Kommunikation. Die Aktorik umfaßt sämtliche Einrichtungen, die zur Durchführung des automatisierten Fahrens benötigt werden (Lenkung, Antrieb, Bremse), sowie Türsteuerung, Blinker, Warnleuchten, Hupe, etc.

Hinweis:
Die Eingriffsnotwendigkeit Technische Aufsicht (TA) kann sowohl im Regelbetrieb der Fahrgastbeförderung, als auch innerhalb des BHMS bei der Fahrzeugpflege (Service & Wartung) auftreten.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Datenanalyse und Plausibilitätsprüfung durch das AD-Bordsystem (Regelbetrieb).

Aktionen:

- Das AD-Bordsystem erfaßt (über 19) die Umgebung mittels der Sensordaten aus dem Umwelt-Interface AD.
  Hinweis:
  Das Umwelt-IF (AD) umfaßt die Sensorik zur Umwelterfassung und -kommunikation für das automatisierte Fahren. Hierzu zählen Kameras, Radar, LiDAR, AD-Infrastruktur, C2I-Kommunikation und C2C-Kommunikation. Die Aktorik umfaßt sämtliche Einrichtungen, die zur Durchführung des automatisierten Fahrens benötigt werden (Lenkung, Antrieb, Bremse), sowie Türsteuerung, Blinker, Warnleuchten, Hupe, etc.
- Das AD-Bordsystem erfaßt (über 18) die Informationen / Sensordaten aus dem Verkehrsinfrastruktur-Interface.
  Hinweis:
  Das Verkehrsinfrastruktur-Interface umfaßt die Kommunikation mit ansteuerbaren Verkehrs-Infrastruktur-Elementen auf der Strecke und im Betriebshof (LSA, Poller, Schranke, etc.)
- Das AD-Bordsystem vergleicht die Informationen und meldet (über 8) priorisiert Abweichungen zwischen den Verkehrsinfrastruktur- und Umwelt-Interface AD Sensordaten an die Technische Aufsicht (TA) der AD-Leitstelle.
- Die Benutzeroberfläche / Graphical User Interface (GUI) ≙ Anwendersoftware ≙ App der AD-Leitstelle visualisiert (ggf. farblich) die priorisierte Information zur erleichterten Wahrnehmung und Unterstützung des menschlichen Operators der Technischen Aufsicht (TA).

- Die Technische Aufsicht (TA) der AD-Leitstelle analysiert die Situation und entscheidet über die Eingriffsnotwendigkeit → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).

Juristische Anforderungen:

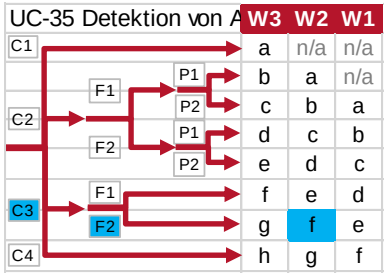
- AFGBV Anlage 1 Teil 1 Abschnitt 7.1 Betriebshandbuch
  Zweck des Betriebshandbuchs ist es, mittels detaillierter Vorgaben den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten und der Technischen Aufsicht die richtige Reaktion auf Fehlerfälle zu ermöglichen.

  Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.
- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

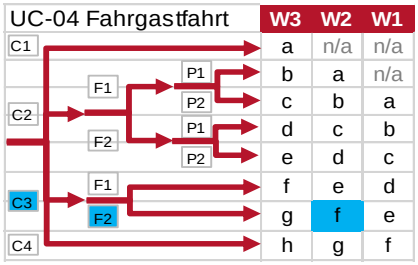
Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.

Risikograph:



≙ ASIL-C ←



≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall.
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.36 UC-36 Detektion und Rückmeldung übertreten der Operativen Design Domain (Kartierung, Wetter, Geschwindigkeit)

Wird während der Betriebsfahrt ein Überschreiten der Operational Design Domain (ODD) erkannt, so wird dies an die AD-Leitstelle übermittelt. Dies tritt bspw. auf, wenn die Geschwindigkeitsvorgabe überschritten wird, obwohl es die Situation wetterbedingt nicht zuläßt.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine	keine
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung und Konfiguration der Fahrbereitschaft zur Aufrechterhaltung der Betriebsfortsetzung, sofern möglich. Andernfalls Bergung veranlassen.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Das Operator-HMI (AD) übernimmt die Freigabe sowie die Steuerung von Fahrfunktionen inklusive Konfliktbehandlung durch den Operator im Fahrzeug im autonomen Fahrbetrieb.

Hinweis:
Das Fahrzeug-Interface stellt lesenden Zugriff auf technische Zustandsdaten des Fahrzeugs (z.B. Batterie-Ladezustand) zur Verfügung.

Hinweis:
Das Verkehrsinfrastruktur-Interface umfaßt die Kommunikation mit ansteuerbaren Verkehrs-Infrastruktur-Elementen auf der Strecke und im Betriebshof (LSA, Poller, Schranke, etc.)

Hinweis:
Das Umwelt-IF (AD) umfaßt die Sensorik zur Umwelterfassung und -kommunikation für das automatisierte Fahren. Hierzu zählen Kameras, Radar, LiDAR, AD-Infrastruktur, C2I-Kommunikation und C2C-Kommunikation. Die Aktorik umfaßt sämtliche Einrichtungen, die zur Durchführung des automatisierten Fahrens benötigt werden (Lenkung, Antrieb, Bremse), sowie Türsteuerung, Blinker, Warnleuchten, Hupe, etc.

Hinweis:
Die Eingriffsnotwendigkeit Technische Aufsicht (TA) kann sowohl im Regelbetrieb der Fahrgastbeförderung, als auch innerhalb des BHMS bei der Fahrzeugpflege (Service & Wartung) auftreten.

Hinweis:
Die Operational Design Domain (ODD) steckt den Bereich genau ab, in dem automatisierte Fahrfunktionen zum Einsatz kommen dürfen. Somit stellen sie eine grundlegende Voraussetzung für sicheres automatisiertes / autonomes Fahren dar.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Grenzwertvorgabe & Überwachung der Grenzwerteinhaltung (Regelbetrieb).

Aktionen:

- Die Systemüberwachung des AD-Bordsystems überwacht die spezifizierten Wertebereiche auf Einhaltung ihrer Grenzwerte (typisch maximal zugelassener Wert und minimal notwendiger Wert).
- Die Systemüberwachung des AD-Bordsystems erkennt eine Über- / Unterschreitung der Werte gegenüber dem zugelassenen Wertebereich.
- Die Systemüberwachung des AD-Bordsystems leitet stabilisierende Maßnahmen der Fehlerkorrektur, Stabilisierung, Robustheit ein und überprüft ob die Maßnahmen hinreichend wirksam sind.
- Die Systemüberwachung des AD-Bordsystems meldet (über 8) das Ereignis *(der Abweichung / Störung)* an die AD-Leitstelle priorisiert.
  - Sofern die Maßnahmen hinreichend sind, erfolgt lediglich ein Ereigniseintrag *(im Hintergrund)*.
    Hinweis: hinreichend bedeutet, daß die Maßnahmen die Störung kompensieren können.
  - Sofern die Maßnahmen unzureichend sind, erfolgt eine Warnmeldung Gelb
    (z.B. Meldung: Lenkung ist schwergängig, Unterstützungsleistung ist häufig aktiv) an die AD-Leitstelle.
    Hinweis: unzureichend bedeutet, daß die Maßnahmen die Störung nur teilweise, jedoch ausreichend, kompensieren können.
  - Sofern die Maßnahmen ungenügend sind, erfolgt eine Warnmeldung Rot
    Hinweis: ungenügend bedeutet, daß die Maßnahmen die Störung nicht ausreichend kompensieren können.
    Hinweis:
    Das AD-Bordsystem veranlaßt ein Minimum Risk Manoeuvre (MRM) im Fahrzeug und startet die Datenaufzeichnung gemäß AFGBV §15 Datenspeicherung Absatz 1 ff.

Weiter mit → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse
  siehe Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.

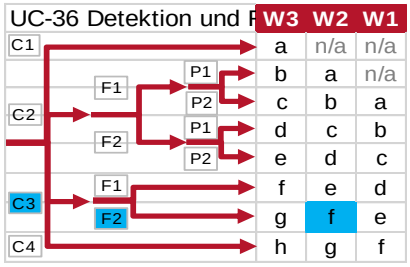
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

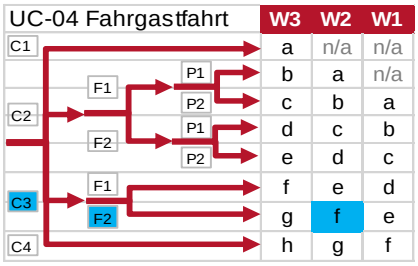
Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.
- Die Gefährdung hängt vom überwachten Wert / Wertebereich ab, insofern entscheidet hier die Funktion über die Sicherheitsrelevanz.
  Hinweis: Der Use Case beschreibt einen Watchdog.

Risikograph:



≙ ASIL-C ←



≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall.
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
✖	
W2	Von der Auftretenswahrscheinlichkeit ist das ein W3, aber es gibt nur wenige unerwünschte Ereignisse ≙ W1 ■ W1 Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich. ■ W2 Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich. ■ W3 Eine relativ hohe Auftretenswahrscheinlichkeit und häufige unerwünschte Ereignisse sind wahrscheinlich. Ein W3 würde auf g = ASIL-D schwer / unkontrollierbarer Prozeß führen, was gar nicht zur Funktion paßt, weil ein Watchdog ein kontrollierter Prozeß ist. Ein W1 führt auf e = ASIL-C, was zur Fahrt paßt Ein W2 führt auf f = ASIL-C, was ebenfalls zur Fahrt paßt, bzw. dieser entspricht, deshalb wird dieser als Ableitung angewendet.

3.2.37 UC-37 Bereitstellen von Verhaltensinformationen an AD-Leitstelle zum späteren System Lernen

Erkennt das AD-Fahrzeug während der Betriebsfahrt eine unbekannte oder nicht auflösbare Situation, so wird der AD-Leitstelle eine ausgewählte Menge an Verhaltensvorschlägen übermittelt. Die AD-Leitstelle kann darauf einen Vorschlag übernehmen und diesen freigeben.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine	keine
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung und Konfiguration der Fahrbereitschaft zur Aufrechterhaltung der Betriebsfortsetzung, sofern möglich. Andernfalls Bergung veranlassen.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Das Operator-HMI (AD) übernimmt die Freigabe sowie Steuerung von Fahrfunktionen inklusive Konfliktbehandlung durch den Operator im Fahrzeug im autonomen Fahrbetrieb.

Hinweis:
Das Fahrzeug-Interface stellt lesenden Zugriff auf technische Zustandsdaten des Fahrzeugs (z.B. Batterie-Ladezustand) zur Verfügung.

Hinweis:
Das Verkehrsinfrastruktur-Interface umfaßt die Kommunikation mit ansteuerbaren Verkehrs-Infrastruktur-Elementen auf der Strecke und im Betriebshof (LSA, Poller, Schranke, etc.)

Hinweis:
Das Umwelt-IF (AD) umfaßt die Sensorik zur Umwelterfassung und -kommunikation für das automatisierte Fahren. Hierzu zählen Kameras, Radar, LiDAR, AD-Infrastruktur, C2I-Kommunikation und C2C-Kommunikation. Die Aktorik umfaßt sämtliche Einrichtungen, die zur Durchführung des automatisierten Fahrens benötigt werden (Lenkung, Antrieb, Bremse), sowie Türsteuerung, Blinker, Warnleuchten, Hupe, etc.

Hinweis:
Die Eingriffsnotwendigkeit Technische Aufsicht (TA) kann sowohl im Regelbetrieb der Fahrgastbeförderung, als auch innerhalb des BHMS bei der Fahrzeugpflege (Service & Wartung) auftreten.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Datenanalyse und KI gestützte Situationsverhaltensmaßnahmen vom AD-Bordsystem (Regelbetrieb).

Aktionen:

- Das AD-Bordsystem erkennt eine unbekannte, (noch nie dagewesene oder vergleichbare) Situation, welche der implementierte Regelalgorithmus nicht selbständig verarbeiten kann.
- Das AD-Bordsystem kann auf Basis von Statistikdaten, KI gestützt, Vorschläge zur Behebung der Situation (Störung) der AD-Leitstelle unterbreiten.
  Hinweis:
  Bei unbekannten Situationen stehen dem AD-Bordsystem vordefinierte Ersatzwerte zur Verfügung aus welchen es auswählen und Vorschläge unterbreiten kann, teilweise kann dieses Ersatzverhalten auch als direkt umsetzbare Verhaltenshandlung spezifiziert / implementiert sein, z.B. das Minimum Risk Manoeuvre (MRM).
- Das AD-Bordsystem unterbreitet (über 8) der Technischen Aufsicht (TA) der AD-Leitstelle eine Liste von Handlungsoptionen.
- Die Technische Aufsicht (TA) der AD-Leitstelle kann eine Option aus der Liste der vorgeschlagenen Handlungen zur Umsetzung auswählen und/oder andere Maßnahmen eigenständig einleiten.
  → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).

Juristische Anforderungen:

- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf

unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind.

- AFGBV Anlage 1 Teil 1 Abschnitt 1.1 Generelle Kollisionsvermeidung
  Kollisionen mit anderen Verkehrsteilnehmenden und unbeteiligten Dritten müssen vermieden werden, sofern dies durch
  1. Notbremseingriffe oder
  2. andere Teilnehmende des umgebenden Verkehrs, andere unbeteiligte Dritte oder die Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nicht gefährdende Ausweichmanöver möglich ist. Kann eine Kollision zur Abwendung einer Gefährdung des Lebens der Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nur durch eine Gefährdung des Lebens anderer Teilnehmender des umgebenden Verkehrs oder unbeteiligter Dritter vermieden werden (unvermeidbare alternative Gefährdung von Menschenleben), darf der Schutz der anderen Teilnehmenden des umgebenden Verkehrs und der unbeteiligten Dritten nicht nachrangig gegenüber dem Schutz der Insassen des autonom fahrenden Kraftfahrzeugs erfolgen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.2 Interaktion mit anderen Verkehrsteilnehmenden
  a) Vorausfahrende Verkehrsteilnehmende auf der Fahrbahn werden erkannt. Es wird jederzeit in jedem Geschwindigkeitsbereich und in jeder möglichen Fahrsituation ein angemessener Sicherheitsabstand eingehalten. Der einzuhaltende Sicherheitsabstand bestimmt sich nach § 4 der Straßenverkehrs-Ordnung.
  b) Der Fahrstreifenwechsel vorausfahrender oder nachfolgender Fahrzeuge, der von einem benachbarten Fahrstreifen in den eigenen Fahrstreifen oder aus dem eigenen Fahrstreifen heraus in einen benachbarten Fahrstreifen erfolgt, wird erkannt und bei der Fahraufgabe entsprechend berücksichtigt.
  c) Situationen, welche einen Fahrstreifenwechsel bedingen (beispielsweise anhaltende oder langsame Fahrzeuge auf der Fahrbahn, Ende eines Fahrstreifens), werden erkannt und geeignete Manöver zum Fahrstreifenwechsel werden sicher durchgeführt.
  d) Einsatzfahrzeuge werden erkannt und geeignete Fahrmanöver sicher durchgeführt.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.3 Planung der Fahrpfade und Geschwindigkeiten
  Bei Geschwindigkeitsanpassungen kommt es zu keiner vermeidbaren Beeinträchtigung von Insassen, anderen Verkehrsteilnehmenden und unbeteiligten Dritten. Es gelten folgende Anforderungen:
  a) Geschwindigkeitsbeschränkungen und Änderungen der Geschwindigkeitsbeschränkung werden erkannt und die Geschwindigkeit wird entsprechend angepaßt.
  b) Besondere Anforderungen an die Geschwindigkeit werden erkannt und im Geschwindigkeits- und Fahrtverlauf befolgt (beispielsweise in Bereichen vor Schulen und an Arbeitsstellen an Straßen, an Bushaltestellen, Bahnübergängen, in engen Kurvenradien oder bei Gefällen, in Engstellen, in denen der eigene Fahrstreifen vom Gegenverkehr mitbenutzt werden muß).
  c) Zeichen und Weisungen der Polizeibeamten gemäß § 36 der Straßenverkehrs-Ordnung, Wechsellichtzeichen gemäß § 37 der Straßenverkehrs-Ordnung, sonstige Zeichen gemäß der §§ 39 bis 42 der Straßenverkehrs-Ordnung sowie Verkehrseinrichtungen gemäß § 43 der Straßenverkehrs-Ordnung werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  d) Situationen, in denen die Vorfahrt anderen gewährt werden muß (beispielsweise vor Fußgängerüberwegen, in Kreuzungsbereichen oder Einmündungen), werden erkannt und ohne Gefährdung oder Behinderung der Vorfahrtberechtigten bewältigt. Es ist eine berechnete Zeit bis zum Aufprall von mehr als drei Sekunden bezüglich des Vorfahrtberechtigen einzuhalten. Wird von diesen Werten abgewichen, muß dies ausreichend begründet und auf Basis von systematischen Sicherheitsbewertungen nach dem Stand der Technik dokumentiert werden. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO-26262:2018-12 Straßenfahrzeuge – Funktionale Sicherheit erfüllt werden.
  e) Bauliche Straßengestaltungen mit Auswirkung auf das Verhaltensrecht (beispielsweise bis zu 5 Meter vom Fahrbahnrand einer vorfahrtberechtigten Straße abgesetzte Radwege nach § 9 Absatz 3 der Straßenverkehrs-Ordnung oder abgesenkte Bordsteine nach § 10 der Straßenverkehrs-Ordnung) werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  f) Arbeitsstellen an Straßen, temporär veränderte Fahrbahnverläufe oder Fahrbahnmarkierungen werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  g) Defizite am Zubehör, insbesondere der Verkehrseinrichtungen (zum Beispiel verschlissene, beschädigte, fehlende oder defekte temporäre oder dauerhafte Fahrbahnmarkierungen und Verkehrszeichen, Phantommarkierungen) und der Straßenausstattung, insbesondere solcher nach vorstehenden Buchstaben a bis f werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Dies gilt insbesondere nach Sturm- und sonstigen Witterungsereignissen.

- AFGBV Anlage 1 Teil 1 Abschnitt 1.4 Reaktion auf Umweltbedingungen
  Wetter-, Umwelt- und Straßeninfrastrukturbedingungen (beispielsweise Regen, Sichtbehinderung durch Rauch, Schlaglöcher) werden im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Fahrpfad und Geschwindigkeit sind – bis hin zum Stillstand des Fahrzeugs – so zu wählen, daß die in den Nummern 1.1 bis 1.3 gestellten Anforderungen auch bei geänderten Umweltbedingungen erfüllt werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.

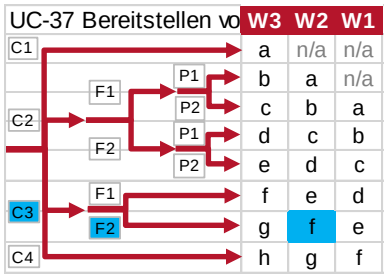
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

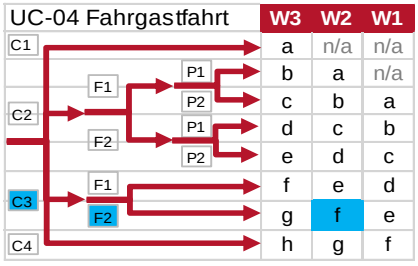
Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.
- Die Gefährdung hängt vom überwachten Wert / Wertebereich ab in Kombination mit einer unbekannten Situation, weshalb die Nachfrage bei der Technischen Aufsicht der AD-Leitstelle vom AD-Bordsystem zu spät gestellt werden kann, weil das Lernen Verarbeitungszeit benötigt.
  Insofern entscheidet hier die Funktion über die Sicherheitsrelevanz.

Risikograph:



≙ ASIL-C ←



≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall.
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich. *Hinweis:* *Wenig unerwünschte Ereignisse, weil durch die Technische Aufsicht (TA) der AD-Leitstelle die Entscheidungsfindung abgesichert wird.*

3.2.38 UC-38 Lernen von Verhalten im Störfall aus früheren Fahrsituationen, die von der AD-Leitstelle begleitet wurden

Wird während der Betriebsfahrt ein Problemfall detektiert, der strukturell bedingt ist (parkendes Auto am Straßenrand, Mülltonne, etc.), kommuniziert das autonome Fahrzeug automatisiert mit der AD-Leitstelle um vorherige Handlungsvorschläge aus dergleichen oder ähnlichen Situationen zu erhalten.

Sind die Ereignisse / Störmeldungen identisch, wählt das Fahrzeug automatisiert die passende Lösungsstrategie aus und führt diese aus. Die technische Aufsicht ist in diesem Fall unbeteiligt.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine	keine
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung und Konfiguration der Fahrbereitschaft zur Aufrechterhaltung der Betriebsfortsetzung, sofern möglich. Andernfalls Bergung veranlassen.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Das Operator-HMI (AD) übernimmt die Freigabe sowie Steuerung von Fahrfunktionen inklusive Konfliktbehandlung durch den Operator im Fahrzeug im autonomen Fahrbetrieb.

Hinweis:
Das Fahrzeug-Interface stellt lesenden Zugriff auf technische Zustandsdaten des Fahrzeugs (z.B. Batterie-Ladezustand) zur Verfügung.

Hinweis:
Das Verkehrsinfrastruktur-Interface umfaßt die Kommunikation mit ansteuerbaren Verkehrs-Infrastruktur-Elementen auf der Strecke und im Betriebshof (LSA, Poller, Schranke, etc.)

Hinweis:
Das Umwelt-IF (AD) umfaßt die Sensorik zur Umwelterfassung und -kommunikation für das automatisierte Fahren. Hierzu zählen Kameras, Radar, LiDAR, AD-Infrastruktur, C2I-Kommunikation und C2C-Kommunikation. Die Aktorik umfaßt sämtliche Einrichtungen, die zur Durchführung des automatisierten Fahrens benötigt werden (Lenkung, Antrieb, Bremse), sowie Türsteuerung, Blinker, Warnleuchten, Hupe, etc.

Hinweis:
Die Eingriffsnotwendigkeit Technische Aufsicht (TA) kann sowohl im Regelbetrieb der Fahrgastbeförderung, als auch innerhalb des BHMS bei der Fahrzeugpflege (Service & Wartung) auftreten.

Hinweis:
Die Operational Design Domain (ODD) steckt den Bereich genau ab, in dem automatisierte Fahrfunktionen zum Einsatz kommen dürfen. Somit stellen sie eine grundlegende Voraussetzung für sicheres automatisiertes / autonomes Fahren dar.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Datenanalyse und KI gestützte Situationsverhaltensmaßnahmen vom AD-Bordsystem (Regelbetrieb).

Aktionen:

- Das AD-Bordsystem erkennt ein plötzlich auftretendes unerwartetes Ereignis (z.B. parkendes Auto am Straßenrand) im Umfeld des autonomen Fahrzeugs und berechnet die Anpassung des Fahrpfades im Rahmen des Betriebsbereiches (z.B. Stadtfahrt, Überlandfahrt) der dynamischen Fahraufgabe, wobei statistische Handlungsoptionen (aus der Vergangenheit), KI gestützt, in dem Auswahlprozeß (Lernen aus der Vergangenheit) der verfügbaren Optionsmöglichkeiten mit berücksichtigt werden.
- Das AD-Bordsystem meldet (über 8) der Technischen Aufsicht (TA) der AD-Leitstelle
  - die ausgewählte Handlungsoption (mit der zugrundeliegenden Berechnung und der Begründung der getroffenen Auswahl)
    - zur Information als Logbucheintrag sowie für die Statistik.
    - zur Überprüfung der Eignung und Bestätigung der Handlungsoption (begleitendes Lernen).
      Hinweis. Der Schwellwert, welcher eine Maßnahme als geeignet bewertet wurde erfüllt.
  - Sofern keine geeignete Handlungsoption berechnet werden konnte, führt das AD-Bordsystem automatisch ein Minimum Risk Manoeuvre (MRM) durch und startet die Datenaufzeichnung gemäß AFGBV §15 Datenspeicherung Absatz 1 ff → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).
    Hinweis: In diesem Fall wird der Technischen Aufsicht (TA) der AD-Leitstelle eine priorisierte Warnmeldung angezeigt.

Juristische Anforderungen:

- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
  Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
  Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.1 Generelle Kollisionsvermeidung
  Kollisionen mit anderen Verkehrsteilnehmenden und unbeteiligten Dritten müssen vermieden werden, sofern dies durch
  1. Notbremseingriffe oder
  2. andere Teilnehmende des umgebenden Verkehrs, andere unbeteiligte Dritte oder die Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nicht gefährdende Ausweichmanöver möglich ist. Kann eine Kollision zur Abwendung einer Gefährdung des Lebens der Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nur durch eine Gefährdung des Lebens anderer Teilnehmender des umgebenden Verkehrs oder unbeteiligter Dritter vermieden werden (unvermeidbare alternative Gefährdung von Menschenleben), darf der Schutz der anderen Teilnehmenden des umgebenden Verkehrs und der unbeteiligten Dritten nicht nachrangig gegenüber dem Schutz der Insassen des autonom fahrenden Kraftfahrzeugs erfolgen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.2 Interaktion mit anderen Verkehrsteilnehmenden
  a) Vorausfahrende Verkehrsteilnehmende auf der Fahrbahn werden erkannt. Es wird jederzeit in jedem Geschwindigkeitsbereich und in jeder möglichen Fahrsituation ein angemessener Sicherheitsabstand eingehalten. Der einzuhaltende Sicherheitsabstand bestimmt sich nach § 4 der Straßenverkehrs-Ordnung.
  b) Der Fahrstreifenwechsel vorausfahrender oder nachfolgender Fahrzeuge, der von einem benachbarten Fahrstreifen in den eigenen Fahrstreifen oder aus dem eigenen Fahrstreifen heraus in einen benachbarten Fahrstreifen erfolgt, wird erkannt und bei der Fahraufgabe entsprechend berücksichtigt.
  c) Situationen, welche einen Fahrstreifenwechsel bedingen (beispielsweise anhaltende oder langsame Fahrzeuge auf der Fahrbahn, Ende eines Fahrstreifens), werden erkannt und geeignete Manöver zum Fahrstreifenwechsel werden sicher durchgeführt.
  d) Einsatzfahrzeuge werden erkannt und geeignete Fahrmanöver sicher durchgeführt.

- AFGBV Anlage 1 Teil 1 Abschnitt 1.3 Planung der Fahrpfade und Geschwindigkeiten
  Bei Geschwindigkeitsanpassungen kommt es zu keiner vermeidbaren Beeinträchtigung von Insassen, anderen Verkehrsteilnehmenden und unbeteiligten Dritten. Es gelten folgende Anforderungen:
  a) Geschwindigkeitsbeschränkungen und Änderungen der Geschwindigkeitsbeschränkung werden erkannt und die Geschwindigkeit wird entsprechend angepaßt.
  b) Besondere Anforderungen an die Geschwindigkeit werden erkannt und im Geschwindigkeits- und Fahrtverlauf befolgt (beispielsweise in Bereichen vor Schulen und an Arbeitsstellen an Straßen, an Bushaltestellen, Bahnübergängen, in engen Kurvenradien oder bei Gefällen, in Engstellen, in denen der eigene Fahrstreifen vom Gegenverkehr mitbenutzt werden muß).
  c) Zeichen und Weisungen der Polizeibeamten gemäß § 36 der Straßenverkehrs-Ordnung, Wechsellichtzeichen gemäß § 37 der Straßenverkehrs-Ordnung, sonstige Zeichen gemäß der §§ 39 bis 42 der Straßenverkehrs-Ordnung sowie Verkehrseinrichtungen gemäß § 43 der Straßenverkehrs-Ordnung werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  d) Situationen, in denen die Vorfahrt anderen gewährt werden muß (beispielsweise vor Fußgängerüberwegen, in Kreuzungsbereichen oder Einmündungen), werden erkannt und ohne Gefährdung oder Behinderung der Vorfahrtberechtigten bewältigt. Es ist eine berechnete Zeit bis zum Aufprall von mehr als drei Sekunden bezüglich des Vorfahrtberechtigen einzuhalten. Wird von diesen Werten abgewichen, muß dies ausreichend begründet und auf Basis von systematischen Sicherheitsbewertungen nach dem Stand der Technik dokumentiert werden. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO-26262:2018-12 Straßenfahrzeuge – Funktionale Sicherheit erfüllt werden.
  e) Bauliche Straßengestaltungen mit Auswirkung auf das Verhaltensrecht (beispielsweise bis zu 5 Meter vom Fahrbahnrand einer vorfahrtberechtigten Straße abgesetzte Radwege nach § 9 Absatz 3 der Straßenverkehrs-Ordnung oder abgesenkte Bordsteine nach § 10 der Straßenverkehrs-Ordnung) werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  f) Arbeitsstellen an Straßen, temporär veränderte Fahrbahnverläufe oder Fahrbahnmarkierungen werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
  g) Defizite am Zubehör, insbesondere der Verkehrseinrichtungen (zum Beispiel verschlissene, beschädigte, fehlende oder defekte temporäre oder dauerhafte Fahrbahnmarkierungen und Verkehrszeichen, Phantommarkierungen) und der Straßenausstattung, insbesondere solcher nach vorstehenden Buchstaben a bis f werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Dies gilt insbesondere nach Sturm- und sonstigen Witterungsereignissen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.4 Reaktion auf Umweltbedingungen
  Wetter-, Umwelt- und Straßeninfrastrukturbedingungen (beispielsweise Regen, Sichtbehinderung durch Rauch, Schlaglöcher) werden im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Fahrpfad und Geschwindigkeit sind – bis hin zum Stillstand des Fahrzeugs – so zu wählen, daß die in den Nummern 1.1 bis 1.3 gestellten Anforderungen auch bei geänderten Umweltbedingungen erfüllt werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.

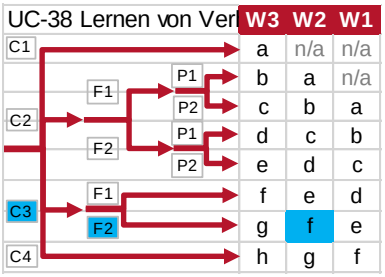
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

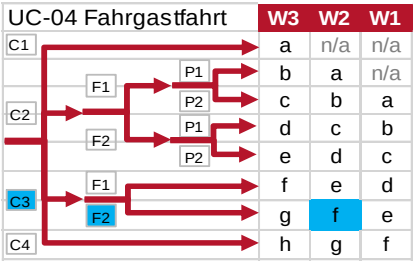
Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.

Risikograph (dynamische Fahraufgabe):



≙ ASIL-C ←



≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall.
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
✖	
W2	Entsprechend der Auftretenswahrscheinlichkeit ist das ein W3, aber es gibt nur wenige unerwünschte Ereignisse ≙ W1 ■ W1 Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich. ■ W2 Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich. ■ W3 Eine relativ hohe Auftretenswahrscheinlichkeit und häufige unerwünschte Ereignisse sind wahrscheinlich. Ein W3 würde auf g = ASIL-D schwer / unkontrollierbarer Prozeß führen, was gar nicht zur Funktion paßt, weil ein Watchdog ein kontrollierter Prozeß ist. Ein W1 führt auf e = ASIL-C, was zur Fahrt paßt Ein W2 führt auf f = ASIL-C, was ebenfalls zur Fahrt paßt, bzw. dieser entspricht, deshalb wird dieser als Ableitung angewendet.

3.2.39 UC-39 Ausgestaltung der AD-Leitstelle für die Technische Aufsicht (TA)

In einer Verkehrsszene tritt ein Fehler/Äußerer Einfluß/Interner Einfluß auf, der den reibungslosen Betrieb des automatisierten Flottenbetriebs stört, so daß Hilfe von der AD-Leitstelle wünschenswert ist.

Der Grund der Störung wird automatisiert anhand der aktuellen Datenlage ggf. über ein maschinelles Lernverfahren ermittelt und Lösungsvorschläge über die Kommunikationsinfrastruktur (über 8) an die AD-Leitstelle übermittelt.

Dort wird eine Meldung im HMI (z.B. mit einer Auswahlmöglichkeit zwischen vorgeschlagenen Optionen oder der Möglichkeit des Setzens von Wegpunkten) angezeigt, die sich dazu eignet, daß die Technische Aufsicht (TA) eine Problemlösung vorgeben kann. Dazu gehört z.B. auch, daß die Rohdaten der relevanten Sensoren abstrahiert und in einer nützlichen Form der Technischen Aufsicht (TA) zur Verfügung gestellt werden.

Schließlich werden die Anweisungen der AD-Leitstelle an das AD-Fahrzeug übermittelt.

- Beispiel 1 „Überhol-Problem“:
  - Ein AD-Fahrzeug steht auf einer Straße und meldet Stau (parkendes Fahrzeug) vor sich auf der Straße.
  - Das AD-Fahrzeug berechnet eine Überholtrajektorie, die an die AD-Leitstelle kommuniziert wird.
  - Der AD-Leitstand visualisiert die Warnung für die technische Aufsicht (TA) und zeigt nahliegende Verkehrskameras an, mit denen die technische Aufsicht die Situation einschätzt und die Fahrzeug-Trajektorie freigibt.
  - Das AD-Fahrzeug überholt das parkende Auto und führt seine Fahrt fort.
- Beispiel 2 „Baustelle“:
  - Eine Baustelle hat die Straße so verändert, daß das AD-Fahrzeug Unterstützung von der AD-Leitstelle benötigt. → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).
    Hinweis: Die Technische Aufsicht hilft z. B. durch die Vorgabe von Wegpunkten oder mittels Remote-Lenkrad.
- Beispiel 3 „Unbekanntes Objekt“:
  - In der Fahrbahnmitte befindet sich ein unbekanntes Objekt, bei dem das AD-Fahrzeug zwar dessen Existenz detektiert, aber nicht die Klassifikation des Objektes sicher feststellen kann.
    → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).
  - Technische Aufsicht wählt zwischen den Optionen:
    - Fall Plastiktüte: überfahren
    - Fall Leitkegel: rechts/links umfahren
    - Fall Tier: warten/hupen

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine	keine
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung und Konfiguration der Fahrbereitschaft zur Aufrechterhaltung der Betriebsfortsetzung, sofern möglich. Andernfalls Bergung veranlassen.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Die Eingriffsnotwendigkeit Technische Aufsicht (TA) kann sowohl im Regelbetrieb der Fahrgastbeförderung, als auch innerhalb des BHMS bei der Fahrzeugpflege (Service & Wartung) auftreten.

Hinweis:
Das Operator-HMI (AD) übernimmt die Freigabe sowie Steuerung von Fahrfunktionen inklusive Konfliktbehandlung durch den Operator im Fahrzeug im autonomen Fahrbetrieb.

Hinweis:
Das Fahrzeug-Interface stellt lesenden Zugriff auf technische Zustandsdaten des Fahrzeugs (z.B. Batterie-Ladezustand) zur Verfügung.

Hinweis:
Das Verkehrsinfrastruktur-Interface umfaßt die Kommunikation mit ansteuerbaren Verkehrs-Infrastruktur-Elementen auf der Strecke und im Betriebshof (LSA, Poller, Schranke, etc.)

Hinweis:
Das Umwelt-IF (AD) umfaßt die Sensorik zur Umwelterfassung und -kommunikation für das automatisierte Fahren. Hierzu zählen Kameras, Radar, LiDAR, AD-Infrastruktur, C2I-Kommunikation und C2C-Kommunikation. Die Aktorik umfaßt sämtliche Einrichtungen, die zur Durchführung des automatisierten Fahrens benötigt werden (Lenkung, Antrieb, Bremse), sowie Türsteuerung, Blinker, Warnleuchten, Hupe, etc.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff

durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Tätigkeiten der Technischen Aufsicht (TA) der AD-Leitstelle (Regelbetrieb).

Aktionen:

- Das AD-Bordsystem erkennt ein plötzlich auftretendes unerwartetes Ereignis, (z.B. parkendes Auto am Straßenrand), im Umfeld des autonomen Fahrzeuges und berechnet die Anpassung des Fahrpfades im Rahmen des Betriebsbereiches (z.B. Stadtfahrt, Überlandfahrt) der dynamischen Fahraufgabe, wobei statistische Handlungsoptionen (aus der Vergangenheit), KI gestützt, in dem Auswahlprozeß (Lernen aus der Vergangenheit) der verfügbaren Optionsmöglichkeiten mit berücksichtigt werden.
- Das AD-Bordsystem meldet (über 8) der Technischen Aufsicht (TA) der AD-Leitstelle
  - die ausgewählte Handlungsoption (mit der zugrundeliegenden Berechnung und der Begründung der getroffenen Auswahl)
    - zur Information als Logbucheintrag sowie für die Statistik → UC-38 Lernen von Verhalten im Störfall aus früheren Fahrsituationen, die von der AD-Leitstelle begleitet wurden.
    - zur Überprüfung der Eignung und Bestätigung der Handlungsoption (begleitendes Lernen).
      Hinweis. Der Schwellwert, welcher eine Maßnahme als geeignet bewertet, wurde nicht erfüllt.
      - Es werden zusätzlich Sensordaten vom Fahrzeug angefordert, welche die Technische Aufsicht (TA) der AD-Leitstelle bei der Beurteilung der Situation unterstützen sollen.
        Außerdem kann die Umgebung durch die Fahrzeugkamera (über UM0.19.2 CameraImage) eingesehen werden, welches zur Bewertung der Situation hilfreich ist.
      - Sofern möglich können auch nahliegende Verkehrskameras (über 18) das Verkehrsinfrastruktur-Interface hinzugezogen werden.
      - Die Ereignismeldung mit den zugehörigen Informationen wird über geeignete Filter der Technischen Aufsicht (TA) automatisiert von der Benutzeroberfläche (GUI) der AD-Leitstelle mit Priorisierung (ggf. farblich hervorgehoben) zur Verfügung gestellt, damit diese schnell und effizient die Situation klären kann. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
- Die Technische Aufsicht (TA) der AD-Leitstelle leitet geeignete Maßnahmen ein
  → UC-28 Eingriffsnotwendigkeit Technische Aufsicht (TA).

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach §1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie in der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik, Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik über einen Abschluß verfügt als
  - ► Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert),
  - ► Bachelor, Master oder
  - ► staatlich geprüfter Techniker.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 2
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie eine entsprechende Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen hat.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 3
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muß, und
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 4
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihr anvertrauten Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes zuverlässig ist.
  Zur Beurteilung der Zuverlässigkeit im Sinne des Satzes 2 Nummer 4 sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde, eine Auskunft aus dem Fahrerlaubnisregister sowie eine Auskunft über Eintragungen aus dem Fahreignungsregister vorzulegen. Sofern in dem Fahrerlaubnisregister mehr als drei Punkte eingetragen sind, ist die Zuverlässigkeit nicht gegeben. § 8 Absatz 3 gilt bezüglich Satz 3 entsprechend.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 2
  Die als Technische Aufsicht eingesetzte natürliche Person darf sich mit Zustimmung des Halters zur Erfüllung ihrer Pflichten weiterer geeigneter natürlicher Personen bedienen, die über mindestens drei Jahre Berufserfahrung im Bereich des Verkehrs- oder Kraftfahrzeugwesens verfügen. Die eingesetzten natürlichen Personen müssen wiederkehrend, mindestens jedoch jährlich beim Hersteller in Bezug auf den Umgang mit dem Kraftfahrzeug sowie wesentliche Veränderungen am Kraftfahrzeug oder der autonomen Fahrfunktion geschult werden. Die Schulung ist mit einer praktischen Prüfung einschließlich der Bewältigung simulierter Betriebsstörungen abzuschließen. Der erfolgreiche Abschluß der Schulung von eingesetzten natürlichen Personen ist von der Technischen Aufsicht zu dokumentieren. Sollen die eingesetzten natürlichen Personen Fahrten im manuellen Fahrbetrieb übernehmen oder Fahrmanöver freigeben, müssen diese Personen eine gültige Fahrerlaubnis besitzen. Die Klasse der Fahrerlaubnis muß der des Fahrzeugs mit autonomer Fahrfunktion entsprechen.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 3
  Befindet sich das Kraftfahrzeug mit autonomer Fahrfunktion im risikominimalen Zustand im Sinne des § 1d Absatz 4 des Straßenverkehrsgesetzes, hat die als Technische Aufsicht eingesetzte natürliche Person eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durchzuführen, bevor sie dessen Beendigung veranlassen darf. Das Ergebnis der Untersuchung ist zu dokumentieren. Wurde der risikominimale Zustand durch einen Defekt am Kraftfahrzeug ausgelöst, muß nach Erreichen des risikominimalen Zustands die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage 1 Nummer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
  Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist ungeachtet der Sätze 1 und 3 das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen. In diesen Fällen erfolgt die Untersuchung der Technischen Aufsicht gemäß Satz 1 im Nachgang des Abtransports auf Grundlage der gespeicherten Fahrdaten.

Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

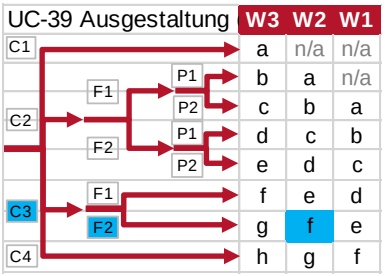
Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben

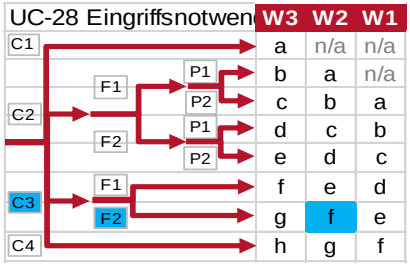
um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.

Hinweis:
Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.

Risikograph:



≙ ASIL-C ←



≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.40 UC-40 Nothalt

Der Nothalt wird durch eine Person im Fahrgastraum betätigt, woraufhin das AD-Bordsystem ein Minimal Risk Manoeuvre (MRM) umsetzt, welches in Abhängigkeit der Zeitspanne zur Abfahrt ein sofortiger Nothalt sein kann, dazu wird im Fahrgastraum eine Ansage bzgl. des Nothalts ausgegeben. Das AD-Bordsystem informiert automatisiert die ÖV- und AD-Leitstelle. Die Technische Aufsicht (TA) der AD-Leitstelle entscheidet ob eine Einbindung des Fahrgast-Notfall-Managements sinnvoll und erforderlich ist, leitet die erforderlichen Maßnahmen (inklusive ggf. Einsatz von Rettungs- und Bergungskräften) zur Beendigung des Notfalls ein und dokumentiert dieses vorschriftsmäßig (AFGBV).

Hinweis:
Im konventionellen Betrieb wird die Aufgabe des AD-Bordsystems und der Technischen Aufsicht durch den Fahrzeugführer ausgeübt, welcher zusätzlich vorort als Ersthelfer fungiert.

Hinweis:
Notaus- / Nothalt-Schalter sind typisch als Einrastschalter ausgelegt, dieser kann nach dem Auslösen per Drehentriegelung, ggf. auch per Schlüssel gesichert, zurückgesetzt werden. Da sich im autonomen Fahrzeug kein Fahrzeugführer an Bord befindet muß die Entriegelung remote durch die Technische Aufsicht (TA) der AD-Leitstelle möglich sein, welches beim Einbau in das Fahrzeug / AD-Kit zu berücksichtigen ist.

Sowohl im konventionellen als auch im autonomen Betrieb wird die Fahraufgabe von den automatischen, fahrzeugspezifischen Sicherheits- und Steuersystemen, den sogenannten Fahrerassistenzsystemen unterstützt, bei denen es sich typischerweise handelt um:

- Adaptive Cruise Control (ACC)
- Automatic Emergency Braking (AEB) ≙ Automatischer Notbremsassistent (ANB)
  Hinweis:
  Namentliche Bezeichnung eines süddeutschen versus norddeutschen Fahrzeugherstellers.
- Notbremsanzeige (NBA)
  Hinweis:
  Notbremsanzeige (NBA) gehört zur Funktion "Notfall-Bremse"
  Definition Notfall-Bremse %:
  $a < -2{,}5\ m/s^2$ → "Blinklicht Rot" = Bremslichter pulsieren (blinken heller rechts/links im Wechsel)
  Dieses ist eine Warnung / Anzeige für den nachfolgenden Verkehr "Achtung starkes Bremsen"
  $a_{Verzögerung,\ max} = -4m/s^2$ plus wenn v < 10km/h erreicht, dann schaltet sich der Warnblinker automatisch zu.
- Antiblockiersystem (ABS)
- Anhaltewegverkürzung (AWV)
- Electronic Stability Control (ESC)
- Emergency-Assistant (EA)

Hinweis:
Eine U-Bahn hält nicht im Tunnel, sondern erst in der nächsten Station,
aber bei einem Bus ist dieses anders, hier hängt es vom Tunnel-Notfallsystem und den Fluchtwegen ab.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Überwachung der Fahrplanumsetzung auf Einhaltung der Fahrplandaten inklusive Pünktlichkeit. Informieren der Fahrgäste über das Ereignis „Nothalt“ sowie der daraus resultierenden Abweichungen gegenüber dem Fahrplan inklusive Unterstützung bei der Sicherstellung des reibungslosen Reiseablaufes der Fahrgäste. Sofern erforderlich Aktualisierung der Fahrplandaten.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung).
BHMS	keine	keine
AD-Leitstelle	Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle. Situationsanalyse von Ereignissen und Einleitung von sinnvollen / notwendigen Maßnahmen zur Aufrechterhaltung oder Wiederherstellung der Fahrgastsicherheit (MRM). Hilfeleistung bei Notfällen inkl. Entsendung von Rettungs- und Bergungsdiensten. Versorgung der Fahrgäste (sowie ggf. Angehörige) mit psychologischer Betreuung	Überwachung der autonomen Fahrt und Gewährleistung der Fahrgastsicherheit bei Ereignissen, sofern möglich sowie Erfüllung der Dokumentationsvorgaben gemäß AFGBV.

	über das Fahrgast-Notfallmanagement sofern sinnvoll / erforderlich.	

Hinweis:
Zuständigkeit = AD-Bordsystem für die Sicherung der AD-Fahrzeugdaten (Ereignisse / Logfiles),
aber verantwortlich für die Aufzeichnung des Ereignisses inklusive der eingeleiteten Maßnahmen ist die AD-Leitstelle.

Hinweis:
Ein Notruf kann auch von einer Person (ggf. potentieller Fahrgast) von außerhalb des Fahrzeuges ausgelöst werden.

Hinweis:
Menschliche Fehlbedienung darf zu keiner Gefährdung von Menschen / Tieren führen oder eine Betriebsgefährdung verursachen.
(Vulnerable Road User (VRU) = ungeschützter Verkehrsteilnehmer)

Hinweis:
Eine Fahrgastfahrt ist eine Fahrt, welche für die Nutzung durch Fahrgäste vorgesehen ist, unabhängig davon ob ein oder mehrere Fahrgäste davon Gebrauch machen.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Notfall (Besondere Situation / Einzelfall → planbarer Regelbetrieb).

Aktionen:

- Der Nothalt wird durch eine Person im Fahrgastraum betätigt.
- Das Fahrgast-HMI (AD) erzeugt eine Nothaltmeldung und sendet diese (über UM0.16.2) an das AD-Bordsystem.
- Das AD-Bordsystem leitet in Abhängigkeit vom Zeitpunkt der Abfahrt ein Minimal Risk Manoeuvre (MRM) ein.
  - ► Sofern der Nothalt unmittelbar / kurzfristig nach der autonomen Abfahrt ausgelöst wird, ist die Geschwindigkeit des Autonomous Drivable Object (ADO) noch gering und es kann ein sofortiger Halt ausgelöst werden, welches insbesondere im Gefährdungsfall „Tier an Leine“ von Bedeutung ist.
    Hinweis:
    Minimum Risk Manoeuvre (MRM) – CAT A = Stop immediately (TR 0)
  - ► Sollte der Nothalt jedoch erst zu einem späteren Zeitpunkt, gemessen zur autonomen Abfahrt erfolgen, wird an der nächstmöglichen / schnellstmöglichen, sicheren Position angehalten.
    Hinweis:
    Minimum Risk Manoeuvre (MRM) – CAT B
    = Hazard lights on + Stop safely in the current lane (TR1 and TR 2)
    Minimum Risk Manoeuvre (MRM) – CAT D & E
    = Hazard lights on + Leave overtaking lane(s) and stop safely on the most outer available right (left) lane,
    if traffic situation allows, otherwise stop safely in current lane (TR 1 and TR 2 and TR 3).
- Das AD-Bordsystem benachrichtigt (über 14) den ÖV-Bordrechner sowie (über 8) die AD-Leitstelle.
- Der ÖV-Bordrechner (UC-40 Nothalt → UC-23 Kommunikation mit Fahrgästen bei außergewöhnlichen Ereignissen) lädt aus der DB der Durchsagen die korrekte Ansage aus und sendet diese Sprachnachricht (über 11) an das Fahrgast HMI ÖV.
- Das Fahrgast HMI ÖV aktiviert die Lautsprecher im Fahrgastraum und informiert die Fahrgäste per Durchsage.
- Die AD-Leitstelle bereitet einerseits die Informationen über den Nothalt auf, d.h. die Technische Aufsicht (TA) stellt unverzüglich den Kontakt mit den Insassen des Kraftfahrzeugs her, wobei die Kommunikation (Audio + Video) mit dem Fahrgastraum (über UM0.15.3) und der Außenumgebung (über UM0.19.2) automatisch hergestellt und aufgezeichnet wird, andererseits führt sie eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durch.
- Die Technische Aufsicht (TA) der AD-Leitstelle entscheidet ob eine Einbindung des Fahrgast-Notfall-Managements sinnvoll und erforderlich ist, z.B. zur psychologischen Betreuung der Fahrgäste, damit die Technische Aufsicht (TA) sich darauf fokussieren kann das Fahrzeug von der derzeitigen Position zu einer besser geeigneten, zugänglicheren Position für z.B. die Rettungs- und Bergungskräfte per manuellem Fahrbetrieb zu bewegen.
  - ► Die Technische Aufsicht (TA) leitet die notwendigen Maßnahmen (inklusive ggf. Einsatz von Rettungskräften) zur Verkehrssicherung und zur Beendigung des Notfalls / des Minimal Risk Manoeuvres (MRM) ein und dokumentiert dieses ordnungsgemäß.
    - ► Die Dokumentation der Maßnahmen erfolgt als Nachweis (auch wenn keine Maßnahmen erforderlich waren), welche (über 3) als Statusmeldung zur ÖV-Leitstelle gemeldet wird.

- Die ÖV-Leitstelle kann (über 3) Rückfragen an die Technische Aufsicht (TA) der AD-Leitstelle stellen.
  Hinweis:
  Die Sprechkommunikation läuft parallel zur 3 über Funk, Telefon, Netzwerk oder Zuruf, sofern AD-Leitstelle und ÖV-Leitstelle sich in einem Raum befinden sollten.
- Die ÖV-Leitstelle entscheidet, ob eine Einbindung des Fahrgast-Informations-Managements (FGI) sinnvoll und erforderlich ist.
  - Sofern die Einbindung von dem Fahrgast-Information-Management (FGI) sinnvoll und erforderlich sein sollte, wird dieses (über 1) benachrichtigt.
    - Das Fahrgast-Information-Management (FGI) informiert die anderen Fahrgäste über App, Web, Anzeiger, …

- Sofern die Einbindung von dem Fahrgast-Notfall-Management sinnvoll und erforderlich sein sollte, wird (über 20) dieses eingebunden.
  - Das Fahrgast-Notfall-Management erhält eine Warnmeldung mit Priorität und Kategorisierung und führt eine Situationsanalyse des Ereignisses durch.
  - Das Fahrgast-Notfall-Management kann (über 20) Rückfragen an die Technische Aufsicht (TA) der AD-Leitstelle stellen.
  - Das Fahrgast-Notfall-Management kann unterstützende Maßnahmen einleiten, z.B. die Angehörigenbetreuung und ggf. Notfallseelsorge.

Hinweis:
Die beiden (außen + innen) Notruf-Knöpfe werden beim Nothalt mitberücksichtigt, sofern der Notruf unmittelbar nach der Anfahrt betätigt wird. Dieses ist sinnvoll, weil damit eine potentielle Fehlbedienung (im inneren, dem Fahrgastraum) eingefangen wird. Zusätzlich wird der Fall „Kinderwagen bereits im Fahrzeug, aber Begleitperson noch außerhalb als die Türen schließen“ durch den äußeren Nothalt abgefangen.

Hinweis:
Sofern einer der beiden (außen + innen) Notruf-Knöpfe mit einem deutlichen zeitlichen Abstand zur Abfahrt gedrückt wird, dann wird die Notruf-Kommunikation mit der AD-Leistelle aufgebaut und die Datenaufzeichnung automatisch gestartet. Eine automatisierte Umsetzung eines Minimal Risk Manoeuvres (MRM) im Fahrzeug ist bei einer z.B. medizinischen oder durch Fehlverhalten (Belustigung versus Belästigung) ausgelösten Notfallmeldung nicht erforderlich.

Hinweis:
Gemäß des Dokumentes „FG-Notfallmanagement_Loesungsvarianten_und_Entscheidung.pdf“ vom 08.03.2024 der IVU wird im Projekt ÖV-LeitmotiF-KI die praxistaugliche Losungsvariante 3 umgesetzt werden, welche eine getrennte zwei Wege Kommunikation von der ÖV-Leitstelle (über 2) zum Fahrgast-Notfallmanagement sowie eine von der Technischen Aufsicht (TA) der AD-Leitstelle (über 20) zum Fahrgast-Notfallmanagement vorsieht. Im Ereignisfall gibt es eine Aufzeichnung (Audio + Video) im Fahrzeug (AD-Bordsystem) und eine weitere Aufzeichnung in der AD-Leitstelle. Hierbei erfolgt (über 16 + 8 + 20) die Signalisierung, welche auch als Rückfallebene der Sprachkommunikation fungiert. Nach der Signalisierung soll die Sprachkommunikation jedoch (über 11 +7) fortgeführt werden, wobei jeweils nur eine Sprechfunkverbindung im Fahrzeug aktiv ist, d.h. ÖV-Disponent und die Technische Aufsicht (TA) der AD-Leitstelle hören gleichzeitig mit und können jeweils in das Geschehen eingreifen, wobei die Technische Aufsicht (TA) der AD-Leitstelle eine höhere Priorität bekommt. Damit ergibt sich als Randbedingung der Umsetzung (um unterschiedliche Latenzen zu vermeiden) ein Arbeitsplatz für ÖV-Leitstelle und AD-Leitstelle mit einem Operator der beide Aufgaben in Personalunion umsetzt oder zwei Operatoren, welche gemeinsam an einem Arbeitsplatz agieren.
Hinweis:
Die Häufigkeit der Sprachkommunikation bzgl. Fahrgastrückfragen aus dem Fahrzeug wird erwartungsgemäß bei Fragen zur Fahrtroute deutlich größer sein als der Bedarf bei Notfällen, weshalb es sinnvoll ist, daß das Headset des Operators an der ÖV-Leitstelle (statt der AD-Leitstelle angeschlossen ist. Umgekehrt benötigt die ÖV-Leitstelle keinerlei Videokommunikation um Rückfragen zu beantworten (Umsetzung der Datensparsamkeit) versus der zwingend notwendigen Videoübermittlung (ohne Aufzeichnung im Regelbetrieb) der Außenumgebung zur Überwachung der Fahrt. Im Notfallereignis sind die Außen- sowie Innenumgebung mit der Sprachkommunikation und den Daten aus dem Fahrzeug in Echtzeit, unverfälscht Datensynchron aufzuzeichnen gemäß AFGBV
Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse.

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie in der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik, Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik über einen Abschluß verfügt als
  - ► Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert),
  - ► Bachelor, Master oder
  - ► staatlich geprüfter Techniker.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 2
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie eine entsprechende Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen hat.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 3
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muß, und
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 4
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihr anvertrauten Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes zuverlässig ist.
  Zur Beurteilung der Zuverlässigkeit im Sinne des Satzes 2 Nummer 4 sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde, eine Auskunft aus dem Fahrerlaubnisregister sowie eine Auskunft über Eintragungen aus dem Fahreignungsregister vorzulegen. Sofern in dem Fahrerlaubnisregister mehr als drei Punkte eingetragen sind, ist die Zuverlässigkeit nicht gegeben. § 8 Absatz 3 gilt bezüglich Satz 3 entsprechend.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 2
  Die als Technische Aufsicht eingesetzte natürliche Person darf sich mit Zustimmung des Halters zur Erfüllung ihrer Pflichten weiterer geeigneter natürlicher Personen bedienen, die über mindestens drei Jahre Berufserfahrung im Bereich des Verkehrs- oder Kraftfahrzeugwesens verfügen. Die eingesetzten natürlichen Personen müssen wiederkehrend, mindestens jedoch jährlich beim Hersteller in Bezug auf den Umgang mit dem Kraftfahrzeug sowie wesentliche Veränderungen am Kraftfahrzeug oder der autonomen Fahrfunktion geschult werden. Die Schulung ist mit einer praktischen Prüfung einschließlich der Bewältigung simulierter Betriebsstörungen abzuschließen. Der erfolgreiche Abschluß der Schulung von eingesetzten natürlichen Personen ist von der Technischen Aufsicht zu dokumentieren. Sollen die eingesetzten natürlichen Personen Fahrten im manuellen Fahrbetrieb übernehmen oder Fahrmanöver freigeben, müssen diese Personen eine gültige Fahrerlaubnis besitzen. Die Klasse der Fahrerlaubnis muß der des Fahrzeugs mit autonomer Fahrfunktion entsprechen.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 3
  Befindet sich das Kraftfahrzeug mit autonomer Fahrfunktion im risikominimalen Zustand im Sinne des § 1d Absatz 4 des Straßenverkehrsgesetzes, hat die als Technische Aufsicht eingesetzte natürliche Person eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durchzuführen, bevor sie dessen Beendigung veranlassen darf. Das Ergebnis der Untersuchung ist zu dokumentieren. Wurde der risikominimale Zustand durch einen Defekt am Kraftfahrzeug ausgelöst, muß nach Erreichen des risikominimalen Zustands die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage 1 Nummer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
  Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist ungeachtet der Sätze 1 und 3 das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen. In diesen Fällen erfolgt die Untersuchung der Technischen Aufsicht gemäß Satz 1 im Nachgang des Abtransports auf Grundlage der gespeicherten Fahrdaten.
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV §15 Datenspeicherung Absatz 2
  Die gespeicherten Daten dürfen nur durch das Kraftfahrt-Bundesamt und die zuständige Behörde und nur zum Zweck der Nachprüfung der Erfüllung der Voraussetzungen der Genehmigung und der mit der Genehmigung verbundenen Überwachungspflichten erhoben, gespeichert und verwendet werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in

allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind.

- AFGBV Anlage 1 Teil 1 Abschnitt 1.1 Generelle Kollisionsvermeidung
  Kollisionen mit anderen Verkehrsteilnehmenden und unbeteiligten Dritten müssen vermieden werden, sofern dies durch
  1. Notbremseingriffe oder
  2. andere Teilnehmende des umgebenden Verkehrs, andere unbeteiligte Dritte oder die Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nicht gefährdende Ausweichmanöver möglich ist. Kann eine Kollision zur Abwendung einer Gefährdung des Lebens der Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nur durch eine Gefährdung des Lebens anderer Teilnehmender des umgebenden Verkehrs oder unbeteiligter Dritter vermieden werden (unvermeidbare alternative Gefährdung von Menschenleben), darf der Schutz der anderen Teilnehmenden des umgebenden Verkehrs und der unbeteiligten Dritten nicht nachrangig gegenüber dem Schutz der Insassen des autonom fahrenden Kraftfahrzeugs erfolgen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.4 Reaktion auf Umweltbedingungen
  Wetter-, Umwelt- und Straßeninfrastrukturbedingungen (beispielsweise Regen, Sichtbehinderung durch Rauch, Schlaglöcher) werden im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Fahrpfad und Geschwindigkeit sind – bis hin zum Stillstand des Fahrzeugs – so zu wählen, daß die in den Nummern 1.1 bis 1.3 gestellten Anforderungen auch bei geänderten Umweltbedingungen erfüllt werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 2 Risikominimaler Zustand
  Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur Ausübung der Fahraufgabe gilt: Das Kraftfahrzeug kann nur auf Veranlassung der Technischen Aufsicht den risikominimalen Zustand verlassen.
- AFGBV Anlage 1 Teil 1 Abschnitt 3 Notfahrfunktion
  Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit einer Notfahrfunktion ausgestattet sein. Muß sich das Kraftfahrzeug im Falle eines Defekts am Kraftfahrzeug in den risikominimalen Zustand versetzen, muß dies mit der Notfahrfunktion erfolgen. Fahrten mit der Notfahrfunktion dürfen nur bei Schrittgeschwindigkeit und aktivierter Warnblinkanlage erfolgen. Der Übergang der autonomen Fahrfunktion aus der normalen Fahrt in die Fahrt mit der Notfahrfunktion ist von dieser Geschwindigkeitsbegrenzung ausgenommen, sofern ein Abbremsen erforderlich ist.
- AFGBV Anlage 1 Teil 1 Abschnitt 4 Manueller Fahrbetrieb
  Im manuellen Fahrbetrieb erfüllt eine fahrzeugführende Person die Fahraufgabe. Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit Vorrichtungen ausgestattet sein, die es einer fahrzeugführenden Person ermöglichen, die Fahraufgabe wahrzunehmen. Ist die Steuerung im manuellen Fahrbetrieb auf Geschwindigkeiten nicht höher als Schrittgeschwindigkeit begrenzt, ist es nicht erforderlich, daß die fahrzeugführende Person sich innerhalb des Kraftfahrzeugs mit autonomer Fahrfunktion aufhält. Die Steuerung kann in diesem Fall über eine im Nahfeld des Kraftfahrzeugs befindliche Fernsteuerung ausgeführt werden. Die maximale Distanz, über die eine Fernsteuerung möglich ist, beträgt 6 Meter, gemessen in gerader Verbindung. Die Einhaltung der maximalen Distanz ist vom Hersteller durch geeignete technische Mittel sicher zu stellen. Soll das Kraftfahrzeug mit autonomer Fahrfunktion im manuellen Fahrbetrieb mit Geschwindigkeiten höher als Schrittgeschwindigkeit gesteuert werden, muß es mit einem Sitzplatz für die fahrzeugführende Person ausgestattet sein. Der Sitzplatz ist entsprechend der geltenden Vorschriften zu gestalten.
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.1 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur dynamischen Ausübung der Fahraufgabe gilt:
  a) Zur dauerhaften Überwachung der technischen Ausrüstung werden nicht personenbezogene technische

Daten im Kraftfahrzeug erhoben und gespeichert.
b) Eine Beeinträchtigung der technischen Ausrüstung ist der Technischen Aufsicht unverzüglich anzuzeigen.

- AFGBV Anlage 1 Teil 1 Abschnitt 6 Übertragung von Daten an das Kraftfahrzeug
  Die zur selbstständigen Bewältigung der Fahraufgabe im autonomen Betrieb notwendigen Daten und Informationen von externen technischen Einheiten (beispielsweise Backends oder Server eines Anbieters, externe Sensoren, Smartphone) müssen vom Kraftfahrzeug sicher empfangen und verwendet werden können. Daten externer Einheiten können im Kraftfahrzeug zur Ausführung der autonomen Fahrfunktionen verwendet werden. Daten und Informationen können beispielsweise bei bestimmten Anwendungsfällen über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) von einer externen technischen Einheit an das Kraftfahrzeug und vom Kraftfahrzeug an eine technische Einheit übertragen werden. Die Übertragung solcher Daten muß insbesondere den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und nach dem aktuellen Stand der Technik abgesichert sein. Das Absicherungskonzept muß die in einer Bedrohungsanalyse identifizierten Risiken mit wirksamen Maßnahmen adressieren und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten. Zur Datenübertragung sollte eine zentrale sichere elektronische Steuereinheit (SECU) genutzt werden. Die SECU dient als Informationsgateway im Kraftfahrzeug. Die SECU kommuniziert intern an die Kommunikationsbusse des Kraftfahrzeugs und an den physischen On-Board-Diagnose II-Anschluß (OBD II) oder an eine proprietäre Schnittstelle eines Herstellers. Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung sind Teil 5 zu entnehmen. Die Integrität, Authentizität und Verfügbarkeit der Datenübertragung sind sicherzustellen. Die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen oder mit Infrastrukturkomponenten ist zulässig. Sie muß auf der Basis einer Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 insbesondere den Anforderungen an die Informationstechnik nach Teil 5 und damit den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen. Während des Betriebs in einer optionalen Testphase ist die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen und Infrastrukturkomponenten zu testen und gegebenenfalls anzupassen.
- AFGBV Anlage 1 Teil 1 Abschnitt 8 Sensorik
  Zur technischen Umsetzung der autonomen Fahrfunktion muß eine Sensorik verwendet werden, die alle für die sichere Erfüllung der Fahraufgabe erforderlichen Gegenstände, Daten oder Personen im Umfeld des Kraftfahrzeugs erfaßt und hinsichtlich der Verarbeitung personenbezogener Daten die Vorgaben der Verordnung (EU) 2016/679, des Bundesdatenschutzgesetzes und spezialgesetzlicher datenschutzrechtlicher Vorschriften beachtet. Zur Erfüllung des in Satz 1 genannten Zwecks und unter Einhaltung der genannten Vorgaben kann die Sensorik durch externe Systeme unterstützt werden. Beeinflussen Wetter-, Umwelt- und Infrastrukturbedingungen die Leistungsfähigkeit der Sensorik, werden von der technischen Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion Maßnahmen eingeleitet, um die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken auszugleichen. Die Sensorik ist in das Sicherheitskonzept des Kraftfahrzeugs mit autonomer Fahrfunktion nach Nummer 7.2 und in die permanente Systemüberwachung nach Nummer 5 einzubinden.

- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse
  - 1) Keine Datenspeicherung bei autonomer Fahrt im festgelegten Betriebsbereich

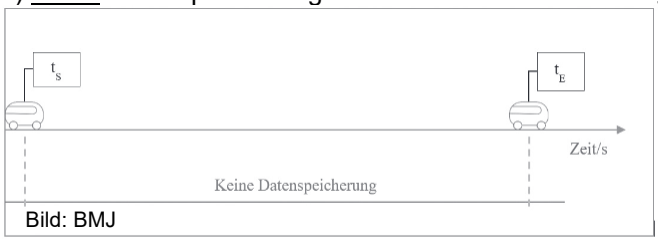


Bild: BMJ

  - 2) Datenspeicherung bei autonomer Fahrt im festgelegten Betriebsbereich mit Ereignis (bspw. Unfall)

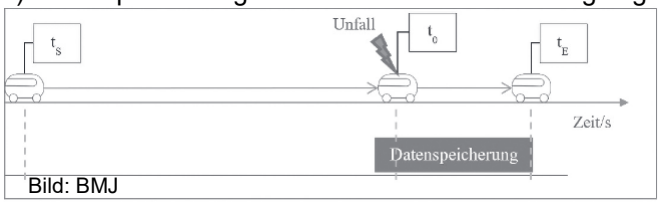


Bild: BMJ

  - 3) Datenspeicherung bei autonomer Fahrt im festgelegten Betriebsbereich mit Ereignis und anschließender Überführung des Kraftfahrzeuges in den risikominimalen Zustand

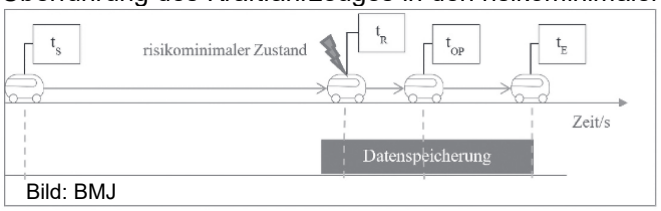


Bild: BMJ

  - Legende:
    t_S Zeitpunkt – Beginn der Fahrt (Starten des Kraftfahrzeuges)
    t_R Zeitpunkt – Auslösung des risikominimalen Zustands
    t_0 Zeitpunkt – Unfallereignis
    t_{0P} Zeitpunkt – Anforderung oder Eingabe der Technischen Aufsicht
    t_E Zeitpunkt – Ende der Fahrt
- AFGBV Anlage 1 Teil 3 Abschnitt 13.2 Technische Vorgaben für das Speichern, Auslesen und Übertragen von Daten
  Das System der Datenspeicherung darf nicht flüchtig sein. Die gespeicherten Daten müssen im stromlosen Zustand erhalten bleiben.
  Ergänzende technische Anforderungen für den Datenspeicher
  - a) Der Zugang zu den im Kraftfahrzeug mit autonomer Fahrfunktion gespeicherten Daten erfolgt über die normierte 16-polige On-Board-Diagnose-Schnittstelle (16-polige OBD-Schnittstelle) über ein Kommunikationsmodul nach ISO 22900-1:2008-03 Straßenfahrzeuge – Modulare Kommunikationsschnittstelle im Fahrzeug (MVCI) – Teil 1: Hardwaredesign Anforderungen unter Verwendung der proprietären Software des Herstellers oder über die proprietäre Schnittstelle. Ergänzend dazu müssen in bestimmten Situationen oder nach bestimmten Ereignissen die Daten direkt über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) an die zuständige staatliche Stelle gesendet werden.
  - b) Der Zugang und das Herunterladen der gespeicherten Daten über die normierte 16-polige OBD-Schnittstelle oder über die proprietäre Schnittstelle darf nur durch das Kraftfahrt-Bundesamt und die zuständige Behörde erfolgen, sofern dies für deren jeweilige Aufgabenerfüllung nach dieser Verordnung erforderlich ist.

- c) Im Reparaturfall erfolgt der Zugang zum Datenspeicher im Kraftfahrzeug mit autonomer Fahrfunktion über die normierte 16-polige OBD-Schnittstelle über ein Kommunikationsmodul nach ISO 22900 nur unter Verwendung der proprietären Software des Herstellers oder über die proprietäre Schnittstelle.
- d) Die Datenspeicherung und die Datenübermittlung an das Kraftfahrt-Bundesamt und die zuständige Behörde haben den Anforderungen an die Sicherheit im Bereich der Informationstechnologie (Teil 5) zu genügen. Insbesondere müssen die Daten dem Stand der Technik gemäß unter Beachtung der Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 vor Manipulation und mißbräuchlicher Verwendung geschützt werden.

- AFGBV Anlage 1 Teil 4 Abschnitt 14.1 Die Technische Aufsicht erteilt eine Fahrmanöverfreigabe an das Kraftfahrzeug mit autonomer Fahrfunktion
  Die technische Ausrüstung versetzt das Kraftfahrzeug in den risikominimalen Zustand, da die Fortsetzung der Fahrt aufgrund einer Verkehrssituation nicht fortgesetzt werden kann. Das Verlassen des risikominimalen Zustands erfolgt mit Unterstützung der Technischen Aufsicht. Folgendes ist hierbei zu beachten:
  a) Die autonome Fahrfunktion kann initial der Technischen Aufsicht mögliche Fahrmanöver zur Fortsetzung der Fahrt vorschlagen und ausreichend Daten zur Beurteilung der Situation liefern.
  b) Wird durch die Technische Aufsicht ein Fahrmanöver vorgegeben, so muß dieses durch die autonome Fahrfunktion validiert werden.
  Unabhängig von den Buchstaben a und b darf das Fahrmanöver nicht ausgeführt werden, wenn daraus eine Gefährdung der am Verkehr Teilnehmenden und unbeteiligter Dritter resultieren würde.
  Die sichere Ausführung oder Nichtausführung solcher Fahrmanöver obliegt weiterhin der autonomen Fahrfunktion mit systemseitiger Auswertung der aktuellen Verkehrssituation vor Ort.
  Hinweis:
  Der aktuelle Gesetzestext ist auf den ersten Blick korrekt, aber fatal beim zweiten Blick. Der menschliche Operator muß, insbesondere nach dem Überschreiten der Leistungsfähigkeitsgrenze eines Fahrzeugsystems, in der Lage sein das Fahrzeug zu steuern, ohne daß dieses durch das vorab bereits versagte System verhindert werden kann. Sonst hätte man einen Dead-Lock. Autonome, automatisierte oder KI-Anwendungen können menschliche Verantwortung nicht ersetzen. (Ethische Regeln haben Bestand).
- AFGBV Anlage 1 Teil 4 Abschnitt 14.2 Übernahme der Fahraufgabe durch manuelle Steuerung außerhalb des festgelegten Betriebsbereichs.
  Erreicht die autonome Fahrt die Grenzen des festgelegten Betriebsbereichs, muß das Kraftfahrzeug durch die autonome Funktion in den risikominimalen Zustand versetzt werden. Wird die Fahrt außerhalb der Grenzen des festgelegten Betriebsbereichs durch eine fahrzeugführende Person fortgesetzt, ist die fahrzeugführende Person mittels eines geeigneten Interaktionskonzepts zur Aktivität aufzufordern. Sofern das Stehenbleiben des Kraftfahrzeugs mit autonomer Fahrfunktion den umlaufenden Verkehr oder Dritte behindern würde, ist die Aufforderung durch einen entsprechenden Hinweis zu ergänzen. Die Aufforderung ist in ihrer Intensität fortlaufend zu steigern. Die Aufforderung kann beispielsweise durch Signaltöne in zunehmender Lautstärke oder durch Vibrationen mit zunehmender Intensität erfolgen.
- AFGBV Anlage 1 Teil 5 Abschnitt 15 Sicherheit in der Informationstechnologie
  Die vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie sind den Anforderungen der jeweils geltenden Fassung der UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems (ABl. L 83 vom 9.3.2021, S. 30) mit Maßgabe des Folgenden zu entnehmen: Die Anforderungen der Nummern 1, 3, 4, 5.3.1 bis 5.3.5 entfallen. Das Sicherheitskonzept muß den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten.
- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).

- AFGBV Anlage 2 Datenspeicherung
  Während des Betriebs sind bei den in § 1g Absatz 2 des Straßenverkehrsgesetzes genannten Anlässen im Kraftfahrzeug mit autonomer Fahrfunktion folgende Daten zu erfassen.

Fahrzeugidentifizierungsnummer	Alphanummerische Zeichen [A-Z; 0-9] Beispiel: AAAAAA654398GFRDE
Positionsdaten	Breiten- und Längengrad [±ddd.ddddd, Angabe in ± Graden (°) und Dezimalgraden, 5 Nachkommastellen] Höhenangaben in Meter Ausgabe im Globalen Positionsbestimmungssystem – Austauschformat als Abfolge von Punkten, in denen eine Änderung der Fortbewegungsrichtung erfolgt; Angabe des (Karten-)Bezugssystems.
Anzahl und Zeiten der Nutzung sowie der Aktivierung/Deaktivierung der autonomen Funktion	Datum (Jahr:Monat:Tag), Zeit (Stunde:Minute:Sekunde), Beispiel: 2019-07-16, 05:25:12
Anzahl und Zeit der Freigabe von alternativen Fahrmanöver.	Anzahl, Einzelzeiten (Stunde:Minute:Sekunde)
Systemüberwachungsdaten (Beginn/Ende) samt Softwarestand	Alphanummerische Zeichen [A-Z; 0-9] samt Erklärung Beispiel: P0601 Motorsteuergerät – Speicher Prüfsummenfehler
Umwelt- und Wetterbedingungen	Temperatur/°C, Helligkeit/Beleuchtungsstärke/lux, Stellung des Scheibenwischers an/aus.
Vernetzung	Vernetzungsparameter wie beispielsweise Übertragungslatenz und verfügbare Bandbreite
Name der aktivierten/deaktivierten passiven und aktiven Sicherheitssysteme, Zustand, auslösende Instanz (System oder extern)	Name des Systems, Zustand, Instanz Beispiel: Notbremssystem, aktiv, Systemfunktionsfähigkeit
Fahrzeugbeschleunigung in Längs- und Querrichtung	Nummerische Werte in Meter pro Sekunde zum Quadrat
Geschwindigkeit	Nummerischer Wert in Meter pro Sekunde
Status der lichttechnischen Einrichtungen	Beispiel: Blinken an/aus, Tagfahrlicht an/aus
Spannungsversorgung des autonomen Kraftfahrzeugs	Nummerischer Wert in Volt
Von extern an das Fahrzeug gesendete Befehle und Informationen	Gesendetes Format der Befehle sowie Metadaten zu Informationen: Dateigröße, Dateiformat, Quelle, Ziel, Übertragungszeit.

Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.
- BOStrab §3 Absatz 2
  Einrichtungen in Betriebsanlagen und Fahrzeugen, die für die Benutzung oder Betätigung durch Fahrgäste bestimmt sind, müssen gut erkennbar und leicht erreichbar sein. Ihre Handhabung muß sich sinnfällig erkennen lassen; Fehlbedienungen dürfen zu keiner Betriebsgefährdung führen.
  Hinweis:
  Einrichtungen (welche für die Nutzung durch Fahrgäste vorgesehen sind) müssen
  gut erkennbar (d.h. der Verwendungszweck muß eindeutig und leicht verständlich / logisch)
  und leicht erreichbar (behindertengerecht und für Kinder geeignet) sein.
- BOStrab §4 Absatz 4
  Durch betriebliche Vorkehrungen ist dafür zu sorgen, daß Betriebsstörungen zügig beseitigt werden, bei Unfällen und gefährlichen Ereignissen unverzüglich Hilfe geleistet wird und insbesondere bei Brandfällen die Möglichkeit zur Selbst- oder Fremdrettung von Personen oder eine Kombination von beidem in Abhängigkeit von den lokalen Verhältnissen besteht.

- BOStrab §7 Absatz 2
  Der Unternehmer ist verpflichtet, bei der Auswahl, Aus- und Fortbildung, Verwendung und Beaufsichtigung der Betriebsbediensteten die Sorgfalt anzuwenden, die eine sichere und ordnungsgemäße Beförderung von Personen erfordert.
- BOStrab §23 Absatz 1
  Für die Verständigung von Betriebsbediensteten mit Betriebsstellen müssen im betriebsnotwendigen Umfang nachrichtentechnische Anlagen vorhanden sein. Besonders wichtige Meldungen an zentrale Betriebsstellen sollen vorrangig übermittelt werden können.
- BOStrab §23 Absatz 3
  Bei Fahrbetrieb ohne Fahrzeugführer müssen nachrichtentechnische Anlagen vorhanden sein, die eine vorrangige Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle ermöglichen.
- BOStrab §43 Absatz 6
  Türen müssen in geschlossener Stellung festgehalten sein. Sie müssen jedoch von Fahrgästen im Notfall geöffnet werden können.
- BOStrab §46 Absatz 4
  Fahrzeuge müssen Einrichtungen für eine Sprechverbindung zwischen Fahrzeugführer und einer Betriebsstelle haben. Notfall-Informationen müssen vorrangig durchgegeben werden können.
- BOStrab §46 Absatz 5
  Personenfahrzeuge eines Zuges, die nicht mit Betriebsbediensteten besetzt sind, müssen ständig verfügbare Einrichtungen für eine Notfall-Sprechverbindung zwischen Fahrgästen und dem Fahrzeugführer haben. ➔ Die Technische Aufsicht (TA) der AD-Leitstelle ist der Fahrzeugführer im automatisierten *(Remote-Sicherheitsfahrer bei ≤ SAE 3)* / autonomen *(≥ SAE4)* Betrieb.
  Hinweis: Im konventionellen Betrieb befindet sich der Sicherheitsfahrer im Fahrzeug.
- BOStrab §46 Absatz 6
  Bei Fahrbetrieb ohne Fahrzeugführer müssen Personenfahrzeuge Einrichtungen für eine Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle haben. Absatz 4 Satz 2 gilt entsprechend.
- BOStrab §52 Absatz 3
  Betriebsanlagen oder Fahrzeuge, die ganz oder teilweise selbsttätig arbeiten oder fernbedient werden, müssen im Rahmen der betrieblichen Erfordernisse von Betriebsbediensteten auf einwandfreie Funktion überwacht werden.
- BOStrab §54 Absatz 3
  Personenzüge dürfen nur so beschleunigt und nur so gebremst werden, daß Fahrgäste nicht mehr als unvermeidbar gefährdet werden.

Einbindung juristischer Vorgaben auf straßengebundenen Verkehrssysteme.

- StGB § 34 Rechtfertigender Notstand
  Wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, handelt nicht rechtswidrig, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Dies gilt jedoch nur, soweit die Tat ein angemessenes Mittel ist, die Gefahr abzuwenden.

Gefahren nach HAZOP:

- Situation Fahrgast mit Hund an Leine:
  Die Person befindet sich bereits im Fahrzeug, das Tier jedoch noch nicht, d.h. es befindet sich noch außerhalb des Fahrzeuges, zu dem Zeitpunkt an dem die von der ÖV-Leitstelle geplante Fahrgastwechselzeit abgelaufen ist, woraufhin die Türschließung eingeleitet wird. Die Lichtschranke erkennt die Hundeleine nicht, somit werden die Türen geschlossen. Mit der Bestätigung, daß die Türen geschlossen sind, beginnt das autonome Fahrzeug die Fahrt mit der Konsequenz, daß das Tier mitgeschliffen würde, sofern im Fahrzeug nicht der Nothalt ausgelöst würde.
  ➔ Gegenmaßnahme (zur Vermeidung des Mitschleifens):
  Wird der Nothalt unmittelbar nach der Anfahrt betätigt führt das Fahrzeug einen sofortigen Nothalt durch, d.h. es sucht nicht erst nach einer geeigneten Anhalteposition.
  Hinweis:
  Die Anfangsgeschwindigkeit ist bei der Abfahrt / Anfahrt noch sehr gering.
- Situation Fahrgast mit Kinderwagen:

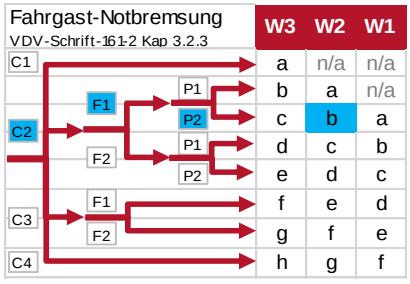
  Eine Person mit Kinderwagen hat den Kinderwagen bereits in das Fahrzeug hinein befördert (gehoben), befindet sich selbst aber noch außerhalb des Fahrzeuges (anders als der Kinderwagen), als die von der ÖV-Leitstelle geplante Fahrgastwechselzeit abgelaufen ist, woraufhin die Türschließung eingeleitet wird. Die Lichtschranke erkennt keine *(nicht)* Person im Türbereich (weil die Person noch außerhalb vom Fahrzeug steht und gerade zusteigen möchte), somit werden die Türen geschlossen. Mit der Bestätigung, daß die Türen geschlossen sind, beginnt das autonome Fahrzeug die Fahrt mit der Konsequenz, daß der Kinderwagen von seiner betreuenden Person getrennt wird, sofern nicht

außerhalb *(oder ggf. auch innerhalb von einem anderen Fahrgast)* vom Fahrzeug der Nothalt gedrückt wird.
➔ Gegenmaßnahme (zur Vermeidung der Trennung):
Wird der Nothalt unmittelbar nach der Anfahrt betätigt führt das Fahrzeug einen sofortigen Nothalt durch, d.h. es sucht nicht erst nach einer geeigneten Anhalteposition.

- Situation Fahrgast erkennt Gefahrensituation auf dem Fahrweg
  Fahrgast wird Zeuge eines schweren Unfalls, welcher weit voraus geschieht, (z.B. Bus/LKW kippt um oder ein Fahrzeug aus dem Gegenverkehr kreuzt die eigene Fahrbahn inkl. ggf. durchbricht die Mittelleitplanke auf der Kraftfahrstraße / Autobahn). Hier wird angenommen, daß die Sensorik des Fahrzeuges das Ereignis, im Gegensatz zum Fahrgast, aufgrund der Entfernung noch nicht erkannt hat, weshalb das Fahrzeug die Fahrt ohne erkennbares Abbremsen fortsetzt, woraufhin der Fahrgast in Angst / Panik gerät und den Notruf / Nothalt drückt.
- Situation Fahrgast erkennt medizinischen Notfall
  Der Fahrgast meldet einen medizinischen Notfall (per Notruf Knopf), dieser wird von der AD-Leitstelle angenommen sowie die geeigneten Maßnahmen durch diese eingeleitet.
  Hinweis:
  Im konventionellen Betrieb verifiziert der Fahrzeugführer, ob ein Notfall erkennbar ist, wobei ggf. beim Fahrgast nachgefragt wird. Das Fahrpersonal reagiert angemessen und hält ggf. an geeigneter Stelle um erste Hilfe zu leisten. Außerdem wird ggf. die ÖV-Leitstelle (es gibt keine AD-Leitstelle) informiert.
- Situation Fahrgast erkennt Unbehagen von einem anderen Fahrgast
  Ein Fahrgast ist sein Unbehagen (Übelkeit) anzusehen und dieser droht sich zu übergeben, (z.B. Aufgrund einer allgemeinem Reiskrankheit und der damit verbundenen Fahrübelkeit). Ein anderer Fahrgast bemerkt dieses und möchte sich schützen, weshalb er den Nothalt betätigt.

Diese Auflistung dient lediglich Anschaulichkeitszwecken und erhebt keinen Anspruch auf Vollständigkeit.

Risikograph (Nothalt im Haltestellenbereich):



≙ ASIL-A

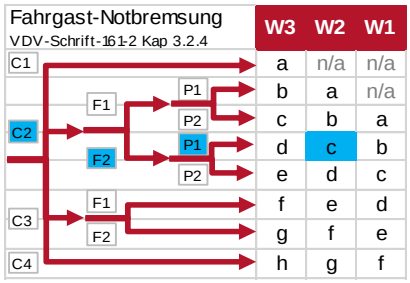
VDV-Schrift-161-2:
Die Betriebserfahrungen zeigen, daß die Betätigung der Fahrgast-Notbremse fast ausschließlich im Haltestellenbereich erfolgt.

Hinweis:
► *Situation Fahrgast mit Hündchen an Leine*
► *Situation Fahrgast mit Kinderwagen*

Begründung zur Wahl der Risikoparameter:

C2	Schwere irreversible Verletzung einer oder mehrerer Personen inkl. Tod einer einzigen Person durch den gefährlichen Vorfall. → *hier Tier, jedoch kann das Erlebnis schwere psychische Schäden insbesondere bei Kindern hervorrufen, deshalb von C1 auf C2 hochgestuft.*
F1	seltener bis öfterer Aufenthalt im gefährlichen Bereich.
P2	Möglichkeit der Vermeidung beinahe unmöglich.
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich.

Risikograph (Nothalt während der Fahrt):



≙ ASIL-A

VDV-Schrift-161-2:
Fahrgast-Notbremse nach Verlassen des Haltestellenbereiches im fahrerbesetzten Betrieb.

Hinweis:
- ► *Situation Fahrgast erkennt Gefahrensituation auf dem Fahrweg*
- ► *Situation Fahrgast erkennt medizinischen Notfall*
- ► *Situation Fahrgast erkennt Unbehagen von einem anderen Fahrgast*

Begründung zur Wahl der Risikoparameter:

C2	Schwere irreversible Verletzung einer oder mehrerer Personen inkl. Tod einer einzigen Person durch den gefährlichen Vorfall. *Hinweis:* *Gefahrensituation auf dem Fahrweg → Unfall* *medizinischen Notfall → Herzinfarkt* *Unbehagen eines anderen Fahrgast → Reiseübelkeit versus Hirninfarkt (Schlaganfall)*
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
P1	Möglichkeit der Vermeidung unter bestimmten Bedingungen.
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich.

Hinweis:
Ein Notfall im Fahrzeug hat keinen Einfluß auf die Anforderungen der Sicherheitsrelevanz für die UC-04 Fahrgastfahrt (ASIL-C) selbst.
Hinweis: Es gibt im autonomen Fahrbetrieb keinen Busfahrer, insofern kann dieser auch keinem medizinischen Notfall erliegen.

3.2.41 UC-41 Fahrzeug dauerhaft unerreichbar

Aufgrund eines dauerhaften Mobilfunkverlustes oder eines Fehlers im Fahrzeug ist keine automatische Datenkommunikation zwischen Fahrzeug und einer / beiden Leitstellen möglich.

- Sobald die Verbindung zwischen Fahrzeug und der Technischen Aufsicht (TA) der AD-Leitstelle für einen definierten Zeitraum (kurzzeitig, abhängig der Fahrzeuggeschwindigkeit, Reaktionszeit) abbricht wird ein Minimum Risk Manoeuvre (MRM) von AD-Bordsystem ausgelöst.
- Sofern der Verbindungsabbruch ausschließlich die Kommunikation zwischen ÖV-Bordrechner und ÖV-Leitstelle (über 3) oder zum BHMS (über 4) betrifft darf das Fahrzeug weiterfahren.
  Hinweis:
  In diesem Fall werden Informationen, welche die Sicherheit der Fahrt nicht gefährden können, nicht mehr aktualisiert, d.h. die Fahrgastinformation (im regulären Fahrgastbetrieb) bzw. die Fahrzeugpflegeablaufstatusinformationen (im BHMS) werden veraltet dargestellt.
  Hinweis:
  Die Kommunikation zwischen ÖV-Bordrechner und ÖV-Leitstelle unterliegt nicht der Systemüberwachung durch das AD-Bordsystem, es operiert eigenständig und rückwirkungsfrei, somit wird ein Verbindungsabbruch ÖV-seitig nicht vom AD-System erkannt oder behandelt.

Kontinuierlich wird automatisiert die Wiederherstellung der Kommunikation versucht.

- Sobald die Verbindung zwischen Fahrzeug und der Technischen Aufsicht (TA) der AD-Leitstelle nach einer Unterbrechung wiederhergestellt wurde, wird die Ursache der Unterbrechung untersucht.
- Sofern die Ursache
  - durch einen Defekt (z.B. Wackelkontakt) am Kraftfahrzeug ausgelöst wurde, muß die Fahraufgabe durch die Technische Aufsicht (TA) manuell übernommen werden.
  - (voraussichtlich) dauerhaft behoben wurde, kann die Technische Aufsicht (TA) die Beendigung des Minimum Risk Manoeuvres (MRM) veranlassen. Das Ergebnis der Untersuchung ist zu dokumentieren.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Überwachung der Fahrplanumsetzung auf Einhaltung der in UC-02 Umlaufanmeldung/-zuweisung übermittelten Fahrplandaten inklusive Pünktlichkeit im Fahrgastbetrieb. Informieren der Fahrgäste über Abweichungen gegenüber dem Fahrplan inklusive Unterstützung bei der Sicherstellung des reibungslosen Reiseablaufes der Fahrgäste, ggf. mittels FGI.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung).
BHMS	Überwachung der Umsetzung der Fahrzeugpflege im BHMS.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrzeugpflegeplandaten (Datenlieferung).
AD-Leitstelle	Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. Überprüfung (vor der Abfahrt), daß die Türen sicher verschlossen sind und während der Fahrt verschlossen bleiben.	Überwachung der autonomen Fahrt und angemessenes Eingreifen auf Basis der Störungsmeldung, sofern erforderlich.

Hinweis:
Das Betriebshofmanagementsystem (BHMS) umfaßt das Planungs- und Steuerungssystem für alle Vorgänge auf dem Betriebshof, z.B. Abstellen, Rangieren, Kuppeln, Waschen, Tanken, etc. von Bussen. → Das BHMS ist zuständig für die eigenständige Planung seiner Abläufe für Fahrzeugpflege (Service & Wartung) sowie verantwortlich für die Sicherstellung der Fahrzeugverfügbarkeit für den kommenden Betriebstag. Die ÖV-Leitstelle ist zuständig für die Berücksichtigung der Fahrzeugverfügbarkeit bei der Kapazitätsplanung der Fahrplanerstellung.

Hinweis:
Eine Fahrgastfahrt ist eine Fahrt, welche für die Nutzung durch Fahrgäste vorgesehen ist, unabhängig davon ob ein oder mehrere Fahrgäste davon Gebrauch machen.

Hinweis:
Fahrtänderungen für Service & Wartungsumläufe / -fahrten / -fahrwege / -fahraufträge / -missionen obliegen dem BHMS eigenständig.

Hinweis:
Die Eingriffsnotwendigkeit Technische Aufsicht (TA) kann sowohl im Regelbetrieb der Fahrgastbeförderung, als auch innerhalb des BHMS bei der Fahrzeugpflege (Service & Wartung) auftreten.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff

durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Ereignisfall (Besondere Situation / Ereignis → planbarer Regelbetrieb).

Aktionen:

- Das AD-Bordsystem überwacht kontinuierlich die autonome Fahrt über die Sensorik und die Peripherie des Fahrzeugs und sendet technische Informationen (über 8) an die AD-Leitstelle.
- Das AD-Bordsystem erkennt eine Störung → UC-12 Systemüberwachung und ggf. Störmeldung.
  Hinweis:
  Das AD-Bordsystem meldet informativ Störungen (über 14) an den ÖV-Bordrechner.
  Die Technische Aufsicht (TA) der AD-Leitstelle kann durch die Störung (AD-seitig) nicht benachrichtigt werden, aber die Technische Aufsicht (TA) erkennt die Störung eigenständig durch das Ausbleiben der kontinuierlichen Statusmeldungen, jedoch kann sie erst wieder Eingreifen, nachdem die Verbindung wiederhergestellt wurde.
  Allerdings kann sie (über 3) bei der ÖV-Leitstelle ein Ersatzfahrzeug anfordern und dieses zur letzten Position aussenden lassen.
  Hinweis:
  Die Kommunikation zwischen ÖV-Bordrechner und ÖV-Leitstelle unterliegt nicht der Systemüberwachung durch das AD-Bordsystem, es operiert eigenständig und rückwirkungsfrei, somit wird ein Verbindungsabbruch ÖV-seitig nicht vom AD-System erkannt oder behandelt.
- Die Systemüberwachung des AD-Bordsystems leitet stabilisierende Maßnahmen der Fehlerkorrektur, Stabilisierung, Robustheit ein und überprüft ob die Maßnahmen hinreichend wirksam sind.
  (Hinweis: Kontinuierlich wird automatisiert die Wiederherstellung der Kommunikation versucht).
  - Sobald die Verbindung zwischen dem Fahrzeug und der Technischen Aufsicht (TA) der AD-Leitstelle für einen definierten Zeitraum (kurzzeitig, abhängig der Fahrzeuggeschwindigkeit, Reaktionszeit) abbricht, wird automatisch ein Minimum Risk Manoeuvre (MRM) vom AD-Bordsystem ausgelöst.
  - Sofern die Verbindung zwischen dem Fahrzeug und der Technischen Aufsicht (TA) der AD-Leitstelle automatisiert wiederhergestellt werden konnte, wird die Ursache untersucht.
  - Sofern die Ursache
    - durch einen Defekt, der (noch) nicht nachhaltig beseitigt werden konnte, (z.B. Wackelkontakt) am Kraftfahrzeug ausgelöst wurde, muß die Fahraufgabe durch die Technische Aufsicht (TA) manuell übernommen werden.
    - (voraussichtlich) dauerhaft behoben wurde, kann die Technische Aufsicht (TA) die Beendigung des Minimum Risk Manoeuvres (MRM) veranlassen. Das Ergebnis der Untersuchung ist zu dokumentieren.
- Sofern der Verbindungsabbruch ausschließlich die Kommunikation zwischen ÖV-Bordrechner und ÖV-Leitstelle (über 3) oder zum BHMS (über 4) betrifft, darf das Fahrzeug weiterfahren.
  Hinweis:
  In diesem Fall werden Informationen, welche die Sicherheit der Fahrt nicht gefährden können, nicht mehr aktualisiert, d.h. die Fahrgastinformationen (im regulären Fahrgastbetrieb) bzw. die Fahrzeugpflegeablaufstatusinformationen (im BHMS) werden veraltet dargestellt.
- Sofern die ÖV-Leitstelle den Verbindungsabbruch bemerkt, kann diese (über 3) mit der AD-Leitstelle kommunizieren und den Austausch des Fahrzeuges veranlassen → UC-27 Ersatzfahrzeug bereitstellen.
  Hinweis:
  Die Kommunikation zwischen ÖV-Bordrechner und ÖV-Leitstelle unterliegt nicht der Systemüberwachung durch das AD-Bordsystem, es operiert eigenständig und rückwirkungsfrei.
- Sofern der Defekt auf dem Betriebshof stattgefunden hat, ist das BHMS statt der ÖV-Leitstelle zuständig.
  Hinweis:
  In diesem Fall muß kein Ersatzfahrzeug gestellt werden, stattdessen bergen die Service & Wartungskräfte des BHMS das Fahrzeug und bringen es zur Instandsetzung.

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.

- AFGBV §12 Anforderungen an den Hersteller Absatz 1 Punkt 2
  Der Hersteller eines Kraftfahrzeugs mit autonomer Fahrfunktion hat
  ein Sicherheitskonzept zur funktionalen Sicherheit nach Anlage I Nummer 7.2 zu erstellen, und dabei
  a) auf Basis dieses Sicherheitskonzeptes eine Gefährdungsanalyse nach Anlage I Ziffer 7.2.1 durchzuführen,
  b) das Sicherheitskonzept nach Anlage III Ziffer 3 zu dokumentieren,
  c) die Sicherheit der autonomen Fahrfunktion entsprechend dieses Sicherheitskonzepts zu überprüfen und die Sicherheit gegenüber dem Kraftfahrt-Bundesamt nach den Anforderungen nach Anlage I Ziffer 10 nachzuweisen.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 3
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihnen anvertrauten Aufgaben zuverlässig sind; zur Beurteilung ihrer Zuverlässigkeit sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde sowie, bei Einsatz für die Durchführung von Fahrten im manuellen Betrieb, eine Auskunft aus dem Fahrerlaubnisregister vorzulegen; § 8 Absatz 3 gilt entsprechend.
- AFGBV §13 Anforderungen an den Halter Absatz 5
  Die Anforderungen zur Dokumentenverwaltung für die Anweisungen nach Absatz 3 und der Berichte nach Absatz 4 müssen dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik wird vermutet, wenn die Vorgaben der ISO 9001:2015 Qualitätsmanagementsysteme – Grundlagen und Begriffe erfüllt werden. Darüber hinaus muß die Dokumentenverwaltung den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 genügen.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 1
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach §1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie in der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik, Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik über einen Abschluß verfügt als
  - ► Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert),
  - ► Bachelor, Master oder
  - ► staatlich geprüfter Techniker.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 2
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie eine entsprechende Schulung in Bezug auf das Kraftfahrzeug mit autonomer Fahrfunktion beim Hersteller dieses Kraftfahrzeugs erfolgreich abgeschlossen hat.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 3
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muß, und
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 1 Punkt 4
  Die als Technische Aufsicht eingesetzte natürliche Person muß für die Wahrnehmung ihrer Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sein. Sie ist geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihr anvertrauten Aufgaben nach § 1f Absatz 2 des Straßenverkehrsgesetzes zuverlässig ist.
  Zur Beurteilung der Zuverlässigkeit im Sinne des Satzes 2 Nummer 4 sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde, eine Auskunft aus dem Fahrerlaubnisregister sowie eine Auskunft über Eintragungen aus dem Fahreignungsregister vorzulegen. Sofern in dem Fahrerlaubnisregister mehr als drei Punkte eingetragen sind, ist die Zuverlässigkeit nicht gegeben. § 8 Absatz 3 gilt bezüglich Satz 3 entsprechend.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 2
  Die als Technische Aufsicht eingesetzte natürliche Person darf sich mit Zustimmung des Halters zur Erfüllung ihrer Pflichten weiterer geeigneter natürlicher Personen bedienen, die über mindestens drei Jahre Berufserfahrung im Bereich des Verkehrs- oder Kraftfahrzeugwesens verfügen. Die eingesetzten natürlichen Personen müssen wiederkehrend, mindestens jedoch jährlich beim Hersteller in Bezug auf den Umgang mit dem Kraftfahrzeug sowie wesentliche Veränderungen am Kraftfahrzeug oder der autonomen Fahrfunktion

geschult werden. Die Schulung ist mit einer praktischen Prüfung einschließlich der Bewältigung simulierter Betriebsstörungen abzuschließen. Der erfolgreiche Abschluß der Schulung von eingesetzten natürlichen Personen ist von der Technischen Aufsicht zu dokumentieren. Sollen die eingesetzten natürlichen Personen Fahrten im manuellen Fahrbetrieb übernehmen oder Fahrmanöver freigeben, müssen diese Personen eine gültige Fahrerlaubnis besitzen. Die Klasse der Fahrerlaubnis muß der des Fahrzeugs mit autonomer Fahrfunktion entsprechen.

- AFGBV §14 Anforderungen an die Technische Aufsicht (TA) Absatz 3
  Befindet sich das Kraftfahrzeug mit autonomer Fahrfunktion im risikominimalen Zustand im Sinne des § 1d Absatz 4 des Straßenverkehrsgesetzes, hat die als Technische Aufsicht eingesetzte natürliche Person eine Untersuchung der Auslösung und der Notwendigkeit des risikominimalen Zustands durchzuführen, bevor sie dessen Beendigung veranlassen darf. Das Ergebnis der Untersuchung ist zu dokumentieren. Wurde der risikominimale Zustand durch einen Defekt am Kraftfahrzeug ausgelöst, muß nach Erreichen des risikominimalen Zustands die Fahraufgabe durch die als Technische Aufsicht eingesetzte natürliche Person unter Einhaltung der Anforderungen der Anlage 1 Nummer 4 manuell übernommen werden, bis der auslösende Defekt nachhaltig beseitigt worden ist.
  Sofern der risikominimale Zustand zu einer Gefährdung der Sicherheit und Leichtigkeit des Verkehrs führt, ist ungeachtet der Sätze 1 und 3 das Kraftfahrzeug mit autonomer Fahrfunktion unverzüglich aus dem Straßenraum zu entfernen. In diesen Fällen erfolgt die Untersuchung der Technischen Aufsicht gemäß Satz 1 im Nachgang des Abtransports auf Grundlage der gespeicherten Fahrdaten.
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV §15 Datenspeicherung Absatz 2
  Die gespeicherten Daten dürfen nur durch das Kraftfahrt-Bundesamt und die zuständige Behörde und nur zum Zweck der Nachprüfung der Erfüllung der Voraussetzungen der Genehmigung und der mit der Genehmigung verbundenen Überwachungspflichten erhoben, gespeichert und verwendet werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 2 Risikominimaler Zustand
  Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur Ausübung der Fahraufgabe gilt: Das Kraftfahrzeug kann nur auf Veranlassung der Technischen Aufsicht den risikominimalen Zustand verlassen.
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.
- AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse
  siehe Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV Anlage 1 Teil 1 Abschnitt 3 Notfahrfunktion
  Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit einer Notfahrfunktion ausgestattet sein. Muß sich das Kraftfahrzeug im Falle eines Defekts am Kraftfahrzeug in den risikominimalen Zustand versetzen, muß dies mit der Notfahrfunktion erfolgen. Fahrten mit der Notfahrfunktion dürfen nur bei Schrittgeschwindigkeit und aktivierter Warnblinkanlage erfolgen. Der Übergang der autonomen Fahrfunktion aus der normalen Fahrt in die Fahrt mit der Notfahrfunktion ist von dieser Geschwindigkeitsbegrenzung ausgenommen, sofern ein Abbremsen erforderlich ist.
- AFGBV Anlage 1 Teil 1 Abschnitt 4 Manueller Fahrbetrieb
  Im manuellen Fahrbetrieb erfüllt eine fahrzeugführende Person die Fahraufgabe. Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit Vorrichtungen ausgestattet sein, die es einer fahrzeugführenden Person ermöglichen, die Fahraufgabe wahrzunehmen. Ist die Steuerung im manuellen Fahrbetrieb auf Geschwindigkeiten nicht höher als Schrittgeschwindigkeit begrenzt, ist es nicht erforderlich, daß die fahrzeugführende Person sich innerhalb des Kraftfahrzeugs mit autonomer Fahrfunktion aufhält. Die Steuerung kann in diesem Fall über eine im Nahfeld des Kraftfahrzeugs befindliche Fernsteuerung ausgeführt werden. Die maximale Distanz, über die eine Fernsteuerung möglich ist, beträgt 6 Meter, gemessen in gerader Verbindung. Die Einhaltung der maximalen Distanz ist vom Hersteller durch geeignete technische

Mittel sicher zu stellen. Soll das Kraftfahrzeug mit autonomer Fahrfunktion im manuellen Fahrbetrieb mit Geschwindigkeiten höher als Schrittgeschwindigkeit gesteuert werden, muß es mit einem Sitzplatz für die fahrzeugführende Person ausgestattet sein. Der Sitzplatz ist entsprechend der geltenden Vorschriften zu gestalten.

- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.1 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur dynamischen Ausübung der Fahraufgabe gilt:
  a) Zur dauerhaften Überwachung der technischen Ausrüstung werden nicht personenbezogene technische Daten im Kraftfahrzeug erhoben und gespeichert.
  b) Eine Beeinträchtigung der technischen Ausrüstung ist der Technischen Aufsicht unverzüglich anzuzeigen.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.2 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und mit konventionellen Vorrichtungen zur Ausübung der Fahraufgabe gilt:
  Die autonome Fahrfunktion darf nicht erneut aktivierbar sein, solange eine Beeinträchtigung der technischen Ausrüstung besteht.
- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).

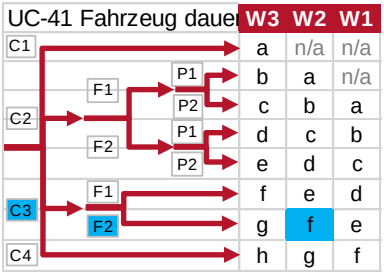
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

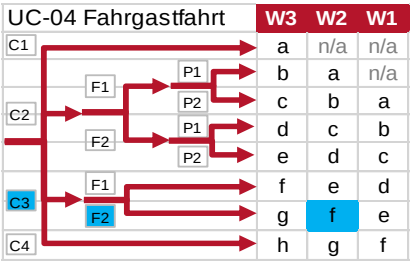
Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.
- Die IT-Infrastruktur ist so aufzusetzen, daß die Verfügbarkeit der Mobilfunkverbindung, möglichst redundant abgesichert, permanent funktional nutzungsbereit ist.
  Hinweis:
  Es dürfen keine vorhersehbaren negativen Effekte auftreten können, d.h. ISP-Verträge mit eingeschränkter Verfügbarkeit (Datenvolumenbegrenzung / Drosselung) sind nicht zulässig.
  - ► Die Sicherheit der Funkverbindung ist abzusichern mittels Gefahrenabwehr / -minderung, gemäß BSI Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2023-01.

Risikograph:



≙ ASIL-C ←



← ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall.
F2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich.
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.42 UC-42 Parameter für LSA Beeinflussung setzen

Üblicherweise kommuniziert das Fahrzeug direkt mit der LSA-Steuerung. Jedoch kann der Disponent von der Leitstelle aus die LSA-Beeinflussung aktivieren bzw. deaktivieren oder den Schwellenwert (ab x min Verspätung) der Signalanforderung ändern.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Überwachung des Fahrweges des Fahrzeuges / Platoon gemäß den Fahrplandaten sowie sofern notwendig / sinnvoll, daß Ergreifen von Maßnahmen, z.B. Lichtsignalanlagenbeeinflussung (LSA) um die Pünktlichkeit wiederherzustellen, die mitreisenden und potentiellen Fahrgäste über Einhaltung / Abweichung der Pünktlichkeit zu informieren, sowie um Unterstützung bei der Sicherstellung des zeitgerechten Erreichens bei Anschlüssen der Fahrt zu leisten.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung).
BHMS	keine	keine
AD-Leitstelle	keine	keine

Hinweis:
Eine Fahrgastfahrt ist eine Fahrt, welche für die Nutzung durch Fahrgäste vorgesehen ist, unabhängig davon ob ein oder mehrere Fahrgäste davon Gebrauch machen.

Hinweis:
Die LSA-Beeinflussung gehört zu den dispositiven Maßnahmen der ÖV-Leitstelle.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Fahrplan / Fahrrouten Aktualisierung (Regelbetrieb).

Aktionen:

- Der Disponent der ÖV-Leitstelle erkennt eine Fahrplanabweichung, welche eine Aktualisierung der Parameter der LSA-Beeinflussung für das Fahrzeug mit der ID erfordert.
- Der Disponent der ÖV-Leitstelle ändert den Parametersatz für das betroffene Fahrzeug und sendet diese (über 7) an den ÖV-Bordrechner.
- Der ÖV-Bordrechner speichert die Parameter und verwendet diese.

Juristische Anforderungen:

- AFGBV Anlage 1 Teil 1 Abschnitt 1.3 Planung der Fahrpfade und Geschwindigkeiten
  Bei Geschwindigkeitsanpassungen kommt es zu keiner vermeidbaren Beeinträchtigung von Insassen, anderen Verkehrsteilnehmenden und unbeteiligten Dritten. Es gelten folgende Anforderungen:
  a) Geschwindigkeitsbeschränkungen und Änderungen der Geschwindigkeitsbeschränkung werden erkannt und die Geschwindigkeit wird entsprechend angepaßt.
  b) Besondere Anforderungen an die Geschwindigkeit werden erkannt und im Geschwindigkeits- und Fahrtverlauf befolgt (beispielsweise in Bereichen vor Schulen und an Arbeitsstellen an Straßen, an Bushaltestellen, Bahnübergängen, in engen Kurvenradien oder bei Gefällen, in Engstellen, in denen der eigene Fahrstreifen vom Gegenverkehr mitbenutzt werden muß).

c) Zeichen und Weisungen der Polizeibeamten gemäß § 36 der Straßenverkehrs-Ordnung, Wechsellichtzeichen gemäß § 37 der Straßenverkehrs-Ordnung, sonstige Zeichen gemäß der §§ 39 bis 42 der Straßenverkehrs-Ordnung sowie Verkehrseinrichtungen gemäß § 43 der Straßenverkehrs-Ordnung werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
d) Situationen, in denen die Vorfahrt anderen gewährt werden muß (beispielsweise vor Fußgängerüberwegen, in Kreuzungsbereichen oder Einmündungen), werden erkannt und ohne Gefährdung oder Behinderung der Vorfahrtberechtigten bewältigt. Es ist eine berechnete Zeit bis zum Aufprall von mehr als drei Sekunden bezüglich des Vorfahrtberechtigen einzuhalten. Wird von diesen Werten abgewichen, muß dies ausreichend begründet und auf Basis von systematischen Sicherheitsbewertungen nach dem Stand der Technik dokumentiert werden. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO 26262:2018-12 Straßenfahrzeuge – Funktionale Sicherheit1 erfüllt werden.
e) Bauliche Straßengestaltungen mit Auswirkung auf das Verhaltensrecht (beispielsweise bis zu 5 Meter vom Fahrbahnrand einer vorfahrtberechtigten Straße abgesetzte Radwege nach § 9 Absatz 3 der Straßenverkehrs-Ordnung oder abgesenkte Bordsteine nach § 10 der Straßenverkehrs-Ordnung) werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
f) Arbeitsstellen an Straßen, temporär veränderte Fahrbahnverläufe oder Fahrbahnmarkierungen werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
g) Defizite am Zubehör, insbesondere der Verkehrseinrichtungen (zum Beispiel verschlissene, beschädigte, fehlende oder defekte temporäre oder dauerhafte Fahrbahnmarkierungen und Verkehrszeichen, Phantommarkierungen) und der Straßenausstattung, insbesondere solcher nach vorstehenden Buchstaben a bis f werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Dies gilt insbesondere nach Sturm- und sonstigen Witterungsereignissen.

Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.
- Dieser UseCase hat keinen direkten Einfluß auf die Fahrt (UC-03 / UC-04 / UC-44).
  Es wird die Lichtsignalanlage z.B. Ampel beeinflußt, welche indirekt über die Sensorik erfaßt und angewendet wird. Das AD Bordsystem muß ein plötzlich auftretendes unerwartetes Ereignis (z.B. veränderte Signale einer Ampelanlage) erkennen und die Anpassung des Fahrpfades und der Parameter (z.B. Geschwindigkeit / Halt) im Rahmen des Betriebsbereiches (z.B. Stadtfahrt, Überlandfahrt) der dynamischen Fahraufgabe anpassen, wobei statistische Handlungsoptionen (aus der Vergangenheit), KI gestützt, in dem Auswahlprozeß (Lernen aus der Vergangenheit) der verfügbaren Optionsmöglichkeiten mit berücksichtigt werden können.

Risikograph:

n/a → QM

3.2.43 UC-43 Parken

Das Fahrzeug soll zwischen zwei Fahrten (außerhalb des Betriebshofs) ohne Fahrgäste abgestellt werden. Solange das Fahrzeug parkt, wird auf dem Außenanzeiger ein entsprechender Text angezeigt, oder (nicht im Diagramm beschrieben) dieser ganz abgeschaltet.

Es wird davon ausgegangen, daß sowohl unmittelbar vor als auch nach der Abstellung eine Leerfahrt (an den bzw. vom Abstellort) stattfindet. Soll eine Fahrgast-fahrt direkt am Abstellort enden oder dort beginnen, müssen die im UC Leerfahrt beschriebenen Abläufe entsprechend durchgeführt werden, insbesondere (vor Beginn dieses UC) die Prüfung, daß sich keine Personen mehr im Fahrzeug befinden, bzw. (am Ende des UC) die Freigabe der Türen (siehe UC Regelhalt).

Konventioneller Betrieb:
Der Fahrer stellt das Fahrzeug ab und stellt die Außenanzeige des Fahrzeugs über den ÖV-Bordrechner ein.

Automatisierter Betrieb:
Der ÖV-Bordrechner muss selbständig erkennen, welchen Text er auf dem Außenanzeiger schalten muss, z. B. anhand der Tatsache, daß er auf keiner Fahrt angemeldet ist und die Türen nicht freigegeben sind.

Wie oben beschrieben, muß ggf. vor und/oder nach der Abstellung eine Pseudo-Leerfahrt ohne Fahrtstrecke eingefügt werden, um sicherzustellen, daß sich während des Parkens keine Fahrgäste mehr im Fahrzeug befinden bzw. daß zu Beginn der folgenden Fahrgastfahrt ein Fahrgastwechsel stattfindet.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Überwachung des Fahrweges des Fahrzeuges / Platoon gemäß den Fahrplandaten plus sofern notwendig / sinnvoll, das Ergreifen von Maßnahmen, z.B. Lichtsignalanlagenbeeinflussung (LSA) um die Pünktlichkeit wiederherzustellen plus die mitreisenden und potentiellen Fahrgäste über Einhaltung / Abweichung der Pünktlichkeit zu informieren, sowie Unterstützung bei der Sicherstellung des zeitgerechten Erreichens bei Anschlüssen der Fahrt.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung).
BHMS	keine	keine
AD-Leitstelle	keine	keine

Hinweis:
Ein Umlauf ist eine Sequenz von Fahrten, vom Ausrücken aus dem Betriebshof bis zum Einrücken in den Betriebshof, d. h. die Menge von Fahrten, die von einem Fahrzeug an einem (Teil des) Betriebstag(s) durchgeführt werden. Die Identifikation erfolgt über den Betriebstag sowie eine Umlaufnummer.

Hinweis:
Die Fahrt entspricht der Bewegung eines Fahrzeugs vom Startpunkt bis zum Endpunkt eines Fahrwegs und wird über den Umlauf bzw. Kurs und die Fahrtnummer identifiziert.

Hinweis:
Der Fahrweg ist eine für eine Fahrt genutzte Route. Diese ist definiert durch eine geordnete Folge geplanter Haltepunkte (bei Leerfahrten nur Start- und Zielpunkt) und ggf. Zwischenpunkte, die den Streckenverlauf eindeutig festlegen.

Hinweis:
Der Fahrauftrag definiert als Oberbegriff eine Vorgabe für die Bewegung eines Fahrzeugs. Die Quelle von Fahraufträgen kann vielfältig sein: Fahrplan, dispositive Maßnahme der Leitstelle, Betriebshof- und Werkstattmanagement etc. Entsprechend ist die Granularität eines Fahrauftrages sehr unterschiedlich, er kann von einer kurzen (Rangier-)Bewegung bis zu einer komplexen Folge von Einsetz- / Fahrplan- / Aussetz-Fahrten reichen.

Hinweis:
Die Mission beschreibt einen Teil einer Fahrt zwischen zwei Haltepunkten / Haltestellen und beinhaltet Angaben zu
- dem Fahrgastwechsel (möglich / nicht möglich, d.h. die Türen werden am Ziel geöffnet bzw. nicht geöffnet)
- der Zeitspanne des Haltens (für den potentiellen Fahrgastwechsel / für das Laden des Fahrzeuges / …)
- der Umlaufnummer inklusive Angaben zum vorgegebenen Fahrweg (Wegpunkte, Route) zum Zielpunkt gemäß Fahrwegplanung der ÖV-Leitstelle
plus optional
- den Informationen zur Haltebucht
- der geplanten Fahrzeit zur Umsetzung der Mission gemäß Fahrwegplanung der ÖV-Leitstelle.

Hinweis:
Die Mission zum Aus- und Einrücken in den Betriebshof gehört in den Umlauf und unterliegt der Verantwortung der ÖV-Leitstelle auch wenn der erste bzw. letzte Teil auf dem Betriebshof stattfindet, wo offiziell der BHMS zuständig und verantwortlich ist. Der Übergabepunkt ist hier der Abfahrtpunkt oder der Parkplatz zum Ausrücken (nach der Umlaufanmeldung der ÖV-Fahrplandaten durch das BHMS) sowie beim wieder Einrücken der vom BHMS zugewiesene Rückkehrabstellplatz, welcher bei der Umlaufanmeldung vom BHMS zugewiesen wurde.

Hinweis:
Fahrtänderungen für Service & Wartungsumläufe / -fahrten / -fahrwege / -fahraufträge / -missionen obliegen dem BHMS eigenständig.

Betriebsschutz:
Der Zugang zum Fahrzeug ist gesperrt, vor dem Parken ist durch die AD-Leitstelle zu verifizieren, daß sich keine Person im Fahrzeug (Sicherheitszone) befindet.

Situation:
Parken (Regelbetrieb).

Aktionen:

- Der ÖV-Bordrechner trackt den Ablauf / Umsetzung des Fahrplanes gemäß dem hinterlegten Umlauf. Sobald nach einem Missionswechsel eine Mission zum Parken dran ist, wird über UC-18 Zielbeschilderung außen und innen ändern der Außenanzeiger auf „Parken“ oder ähnlich gesetzt.
- Die Technische Aufsicht der AD-Leitstelle verifiziert über die Innenraumkamera (über UM0.15.3 CamaraImage), daß sich kein Fahrgast im Fahrzeug befindet, andernfalls → UC-22 Problem mit Fahrgast (störendes Verhalten).

Juristische Anforderungen:

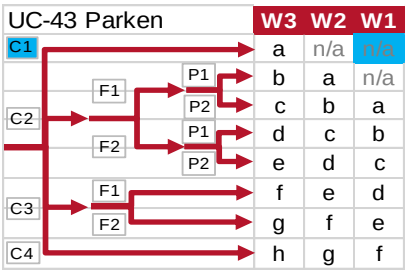
- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.

  Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.
- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

Gefahren nach HAZOP:

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert. Dazu zählen auch Vorgaben zur Entscheidungsbefugnis der Technischen Aufsicht (TA) der AD-Leitstelle. Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.
  Hinweis:
  Die Betriebsprozesse beinhalten auch die festgelegten Regeln für das effiziente und reibungslose Zusammenspiel der Organisationseinheiten BHMS, AD-Leitstelle und ÖV-Leitstelle.

Risikograph:



≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzungen durch den gefährlichen Vorfall.
✖	
✖	
W1	Eine sehr geringe Auftretenswahrscheinlichkeit und nur wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.44 UC-44 Fahrt im Depot

Nachdem das Fahrzeug für die autonome Fahrt (inklusive der Fahrplandaten) konfiguriert wurde *(UC-02 → UC-44)* wird in Abhängigkeit des aufrufenden Use Cases über die zugehörige Mission (aus dem BH-Umlauf) der spezifische Ablauf der Fahrt umgesetzt.

Hinweis:
Fahrt = Bewegung eines Fahrzeuges von Startpunkt zum Zielpunkt eines Fahrwegs, welches über den Umlauf bzw. Kurs und die Fahrtnummer identifiziert wird.

Eine Fahrt aus dem Depot kann aufgerufen werden von

- UC-01 Fahrzeug aufrüsten zur Umsetzung der Probefahrt der erweiterten Abfahrkontrolle
- UC-02 Umlaufanmeldung/-zuweisung zur Umsetzung der Fahrt für das Ausrücken (Betriebsaufnahme) und dem Wiedereinrücken in den Betriebshof (Fahrt zum Sammelplatz der Abrüstung → UC-43 Parken)
- UC-15 Neuen Umlauf hinzufügen um beliebige Fahrten innerhalb des Betriebshofes zu adressieren
- UC-25 Waschvorgang
- UC-26 Lademanagement

Im ersten Fall absolviert das Fahrzeug autonom mit Überwachung durch die Technische Aufsicht (TA) der AD-Leitstelle die Probefahrt und kehrt dann zur Station für die Prüfung der sicherheitsrelevanten elektronisch geregelten und mechanischen Fahrzeugsysteme, gemäß der Planung vom BHMS, zurück um die in AFGBV §13 Anforderungen an den Halter Absatz 7 definierten Bereiche zu überprüfen. Die Prüfung ist zu dokumentieren → UC-01 Fahrzeug aufrüsten.

Sofern die erweiterte Abfahrkontrolle ohne Mängel abgeschlossen wurde und das Fahrzeug (im zweiten Durchlauf von UC-02) zur autonomen Fahrt der Betriebsaufnahme konfiguriert wurde, ist es zum Ausrücken betriebsbereit.

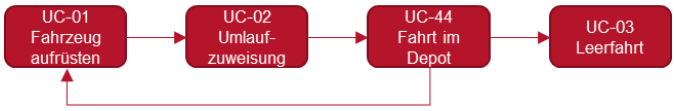


Abbildung 7 Ablauf vor dem Ausrücken

In diesem Fall fährt das Fahrzeug autonom mit Überwachung durch die Technische Aufsicht (TA) der AD-Leitstelle zur Ausfahrt des Betriebshofes gemäß dem Fahrauftrag der ÖV-Leitstelle aus UC-02 Umlaufanmeldung/-zuweisung. Entsprechendes gilt für das Wiedereinrücken in den Betriebshof. Mit der Übergabe (zum Betriebsende ÖV) des Fahrzeuges von der ÖV-Leitstelle an das BHMS startet der Umlauf Fahrzeugpflege (Service, Reinigung und Wartung), welcher vom BHMS selbständig geplant und umgesetzt wird über die zugehörigen Use Cases (siehe oben).

Hinweis:
Im Anschluß an den BH-Umlauf Fahrzeugpflege (Service & Wartung) erfolgt das UC-07 Fahrzeug abrüsten.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	keine	keine
BHMS	Planung und Aussteuerung der jeweiligen Fahrt zu den einzelnen Stationen des Ablaufes (Umlaufes) Fahrzeugpflege (Service & Wartung). Sicherstellen, daß sich zu Fahrtbeginn der autonomen Fahrt keine Personen im Fahrzeug aufhalten.	Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung). Sicherstellung, daß die Fahrzeuge an den Stationen des BHMS zeitgerecht verfügbar sind damit die BHMS-Betriebsabläufe reibungslos, verzögerungs-frei umgesetzt werden können.
AD-Leitstelle	Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle.	Überwachung der autonomen Fahrt

Hinweis:
Das Betriebshofmanagementsystem (BHMS) umfaßt das Planungs- und Steuerungssystem für alle Vorgänge auf dem Betriebshof, z.B. Abstellen, Rangieren, Kuppeln, Waschen, Tanken, etc. von Bussen. → Das BHMS ist zuständig für die eigenständige Planung seiner Abläufe für Fahrzeugpflege (Service & Wartung) sowie verantwortlich für die Sicherstellung der Fahrzeugverfügbarkeit für den kommenden Betriebstag. Die ÖV-Leitstelle ist zuständig für die Berücksichtigung der Fahrzeugverfügbarkeit bei der Kapazitätsplanung der Fahrplanerstellung.

Hinweis:
Eine Fahrgastfahrt ist eine Fahrt, welche für die Nutzung durch Fahrgäste vorgesehen ist, unabhängig davon ob ein oder mehrere Fahrgäste davon Gebrauch machen (hier) können.

Hinweis:
Fahrtänderungen für Service & Wartungsumläufe / -fahrten / -fahrwege / -fahraufträge / -missionen obliegen dem BHMS eigenständig.

Betriebsschutz:
Zugang zum Betriebshof (Sicherheitszone) haben nur ausgebildete und (sicherheitstechnisch) geschulte Mitarbeiter, Fahrgäste haben keinen Zugang.

Situation:
Fahrzeug ist bereit zur Fahrt im Depot inkl.

- der Umsetzung der erweiterten Abfahrkontrolle / Probefahrt (Regelbetrieb)
- dem Aus- / Einrücken (Regelbetrieb)
- den Rangierfahrten (Regelbetrieb) zwischen den einzelnen Stationen der Fahrzeugpflege (Service & Wartung).

Aktionen:

- Das BHMS meldet (über 4) die Abfahrbereitschaft an die AD-Leitstelle.
  Die aktuellen Fahrplandaten (Fahrten, Fahraufträge und die Missionen des Umlaufes) wurden in den ÖV-Bordrechner und das AD-Bordsystem geladen und sind jeweils verifiziert.
  Das Fahrzeug ist gemäß der Umlaufdaten abfahrbereit
  - zur erweiterten Abfahrkontrolle (Probefahrt),
  - zum Ausrücken (Betriebsaufnahme),
  - zum Einrücken (Ausrückfahrt zum Betriebsende),
  - zu den jeweiligen Rangierfahrten zwischen den Stationen des BHMS,
  - zur Fahrt zum UC-07 Fahrzeug abrüsten und UC-43 Parken.
- Die AD-Leitstelle startet (über 8) durch das AD-Bordsystem die autonome Fahrt, welche von der Technischen Aufsicht (TA) überwacht wird.
  - Der Umlauf erweiterte Abfahrkontrolle (Probefahrt) kann mehrere Missionen enthalten, welche Leerfahrten und Fahrgastfahrten (ohne Fahrgast), in beliebiger Reihenfolge, mit/ohne Türöffnung und andere Situationen umsetzen kann. Zum Testende der Probefahrt fährt das Fahrzeug zur Prüfstation für die vorgeschriebenen Prüfungen, gemäß der definierten Bereiche in AFGBV §13 Anforderungen an den Halter Absatz 7, welche in UC-01 Fahrzeug aufrüsten dokumentiert werden.
  - Der klassische Umlauf (Betrieb) enthält die Fahrplandaten der ÖV-Leitstelle. Dieser beginnt mit dem Verlassen des Depots über UC-44, gefolgt von Leer- und Fahrgastfahrten (mit/ohne Fahrgäste) in beliebiger Reihenfolge über UC-45 MissionCtrl gesteuert, bis hin zum Wiedereinrücken in das Depot über UC-44.
  - Der Umlauf Fahrzeugpflege (Service & Wartung) steuert den Ablauf der UC-24 Fundsachen und Sauberkeit im Fahrzeug, UC-25 Waschvorgang, UC-26 Lademanagement, UC-43 Parken und letztendlich den UC-07 Fahrzeug abrüsten, welcher UC-09 Datenentsorgung initiiert.
    Hinweis:
    Der Umlauf wird gemäß der Prozesse und Verfahren des BHMS, eigenständig vom BHMS geplant und umgesetzt. Dieses kann sein z.B. Waschen außen, dann Reinigung innen, gefolgt von Laden und letztendlich Abrüsten. Die zuständige ÖV-Leitstelle erhält die Rückmeldung der Fahrzeugverfügbarkeit vom BHMS zur Berücksichtigung bei der Kapazitätsplanung. Durch die Steuerung des Fahrzeuges über Missionen ist ein standardisierter, diskriminierungsfreier Zugang gegeben, wobei unterschiedliche fahrzeugspezifische Abläufe der Serviceroutinen gemäß der Vorgabe der Fahrzeughersteller (OEM) berücksichtigt werden können.
- Der ÖV-Bordrechner berichtet (informiert) den Fahrtfortschritt in Form von zurückgelegtem Weg mittels der logischen Ortung über GPS (über 6) an das BHMS.

Juristische Anforderungen:

- AFGBV §5 Absatz 5
  Die Hersteller und die Halter von Kraftfahrzeugen mit autonomer Fahrfunktion sind verpflichtet
  ► das Kraftfahrt-Bundesamt bei der Durchführung der Marktüberwachungstätigkeiten zu unterstützen und
  ► dem Kraftfahrt-Bundesamt auf Verlangen die für die Marktüberwachung erforderlichen Unterlagen und Informationen sowie andere technische Spezifikationen unentgeltlich bereitzustellen, wobei die Hersteller auf Verlangen auch einen Zugang zu Software und Algorithmen ermöglichen müssen.
- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.

- AFGBV §12 Anforderungen an den Hersteller Absatz 1
  Der Hersteller eines Kraftfahrzeugs mit autonomer Fahrfunktion hat Reparatur- und Wartungsinformationen für das Kraftfahrzeug nach Anlage 3 Nummer 2.3 und 2.6 dieser Verordnung zu erstellen.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 1
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen die Fahrzeugsysteme für die aktive und passive Sicherheit des Kraftfahrzeugs mit autonomer Fahrfunktion regelmäßig überprüft werden.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 2
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß täglich vor Betriebsbeginn eine erweiterte Abfahrkontrolle nach Absatz 7 durchgeführt wird.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 3
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen ab dem Tag der Zulassung zum Straßenverkehr alle 90 Tage eine Gesamtprüfung nach den Vorgaben des Betriebshandbuchs für das Kraftfahrzeug mit autonomer Fahrfunktion durchgeführt wird.
- AFGBV §13 Anforderungen an den Halter Absatz 1 Punkt 4
  Der Halter hat zur Erfüllung der Pflichten nach § 1f Absatz 1 des Straßenverkehrsgesetzes während des Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten, daß die Ergebnisse der Gesamtprüfungen nach Nummer 3 einschließlich einer Beschreibung aller festgestellten Mängel und durchgeführter Instandsetzungen in einem Bericht dokumentiert und dem Kraftfahrt-Bundesamt sowie der zuständigen Behörde auf Verlangen unverzüglich übermittelt werden, sofern dies erforderlich ist.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 1
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie eine Meisterprüfung im Kraftfahrzeugmechaniker-Handwerk erfolgreich bestanden haben; diesem Abschluß steht der Abschluß als Diplom-Ingenieur, Diplom-Ingenieur (FH), Ingenieur (graduiert), Bachelor, Master oder der staatlich geprüfte Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik/Luftfahrzeugtechnik gleich, sofern die betreffende Person nachweislich im Kraftfahrzeugbereich tätig ist und eine mindestens dreijährige Tätigkeit nachweisen kann.
- AFGBV §13 Anforderungen an den Halter Absatz 2 Punkt 3
  Der Halter hat sicherzustellen, daß bei der Durchführung von Maßnahmen nach Absatz 1 jede Person geeignet im Sinne von Satz 2 ist. Die für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlichen Personen sind geeignet, wenn sie im Hinblick auf die Wahrnehmung der ihnen anvertrauten Aufgaben zuverlässig sind; zur Beurteilung ihrer Zuverlässigkeit sind im Rahmen des Verfahrens nach den §§ 7 und 8 Absatz 2 jeweils ein Führungszeugnis zur Vorlage bei einer Behörde sowie, bei Einsatz für die Durchführung von Fahrten im manuellen Betrieb, eine Auskunft aus dem Fahrerlaubnisregister vorzulegen; § 8 Absatz 3 gilt entsprechend.
- AFGBV §13 Anforderungen an den Halter Absatz 3
  Der Halter muß sicherstellen, daß Anweisungen zur ordnungsgemäßen Durchführung der Wartungsarbeiten, der Gesamtprüfungen, weiterer Untersuchungen und Fahrten im manuellen Fahrbetrieb vorliegen und daß diese Anweisungen befolgt werden. Die Anweisungen sind zu dokumentieren.
- AFGBV §13 Anforderungen an den Halter Absatz 4
  Berichte über die Durchführung von Wartungsarbeiten, von Gesamtprüfungen und von weiteren Untersuchungen müssen durch den Halter oder die verantwortliche Person unverzüglich schriftlich oder elektronisch erstellt werden. Die Berichte sind zu unterzeichnen. Die Berichte sind zu dokumentieren und vom Halter oder von der für die Technische Aufsicht verantwortlichen Person sechs Monate lang aufzubewahren und nach Ablauf dieser Frist unverzüglich, bei elektronischer Speicherung automatisiert, zu löschen.
- AFGBV §13 Anforderungen an den Halter Absatz 5
  Die Anforderungen zur Dokumentenverwaltung für die Anweisungen nach Absatz 3 und der Berichte nach Absatz 4 müssen dem Stand der Technik entsprechen. Das Erfordernis des Stands der Technik wird vermutet, wenn die Vorgaben der ISO 9001:2015 Qualitätsmanagementsysteme – Grundlagen und Begriffe erfüllt werden. Darüber hinaus muß die Dokumentenverwaltung den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 genügen.
- AFGBV §13 Anforderungen an den Halter Absatz 6
  Soweit der Halter die Aufgaben der Technischen Aufsicht selbst wahrnimmt, muß er gemäß den Voraussetzungen nach § 14 dafür geeignet sein. Sofern er die Aufgaben der Technischen Aufsicht nicht selbst wahrnimmt, muß er eine nach § 14 geeignete natürliche Person hierfür bestellen. Der Halter hat die zur Wahrnehmung der Pflichten der Technischen Aufsicht notwendigen sachlichen Voraussetzungen zur Verfügung zu stellen; dies erfordert insbesondere die Bereitstellung und Einrichtung von Räumlichkeiten

sowie informationstechnischen Systemen, die für die Wahrnehmung der Pflichten der Technischen Aufsicht nach § 1f Absatz 2 des Straßenverkehrsgesetzes geeignet sind.

- AFGBV §13 Anforderungen an den Halter Absatz 7
  Die erweiterte Abfahrkontrolle im Sinne des Absatzes 1 Nummer 2 beginnt mit einer Probefahrt, um die Systeme zu aktivieren. Im Anschluß an die Probefahrt werden folgende Bereiche überprüft:
  - Bremsanlage,
  - Lenkanlage,
  - Lichtanlage,
  - Reifen/Räder,
  - Fahrwerk,
  - sicherheitsrelevante elektronisch geregelte Fahrzeugsysteme sowie die Sensorik zur Erfassung externer und interner Parameter und
  - mechanische Fahrzeugsysteme für die aktive und passive Sicherheit.
- AFGBV §14 Anforderungen an die Technische Aufsicht (TA)
  → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV §15 Datenspeicherung Absatz 1
  Für den Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion regelt Anlage 2 zu dieser Verordnung Näheres zu den genauen Zeitpunkten der Datenspeicherung, zu den Parametern der Datenkategorien und zu den Datenformaten.
- AFGBV Anlage 1 Teil 1 Funktionale Anforderungen an Kraftfahrzeuge mit autonomer Fahrfunktion
  Kraftfahrzeuge mit autonomer Fahrfunktion müssen die im Folgenden dargestellten funktionalen Anforderungen erfüllen. Die geforderten Funktionen können vom Hersteller oder vom Halter oder von beiden in einer möglichen, so genannten Testphase des Kraftfahrzeugs mit autonomer Fahrfunktion ohne Fahrgäste im festgelegten Betriebsbereich nachgewiesen werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 1 Dynamische Fahraufgabe
  Das Kraftfahrzeug muß in der Lage sein, durch geeignete Wahl von Fahrpfad und Geschwindigkeit selbstständig und stetig anpassend die Fahraufgabe in dem genehmigten festgelegten Betriebsbereich in allen Situationen sicher zu erfüllen. Dies beinhaltet die Ausrichtung des Fahrverlaufs am veränderlichen Umfeld des Kraftfahrzeugs mit autonomer Fahrfunktion und die Sicherstellung der Übereinstimmung mit gesetzlichen Vorgaben. Der Sicherheit aller Verkehrsteilnehmenden, aller unbeteiligten Dritten und aller Fahrzeuginsassen muß die höchste Priorität bei der Erfüllung der Fahraufgabe eingeräumt werden. Auf unerwartete Ereignisse, auch wenn diese plötzlich auftreten, muß das Kraftfahrzeug mit autonomer Fahrfunktion angemessen reagieren.
  Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten. In Abhängigkeit von überprüfbaren Einflußfaktoren auf die Gefährdung von Fahrzeuginsassen und anderen Verkehrsteilnehmenden und unbeteiligter Dritte kann es erforderlich sein, diese Grenze zu überschreiten. Dies kann beispielsweise der Fall sein, wenn sich nur angeschnallte, nicht aber stehende Fahrzeuginsassen im Inneren des Fahrzeugs aufhalten.
  Das Kraftfahrzeug mit eingeschalteter autonomer Fahrfunktion muß zur Erfüllung der Fahraufgabe mindestens die Anforderungen erfüllen, die in den folgenden Nummern 1.1 bis 1.4 genannt sind.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.1 Generelle Kollisionsvermeidung
  Kollisionen mit anderen Verkehrsteilnehmenden und unbeteiligten Dritten müssen vermieden werden, sofern dies durch
  1. Notbremseingriffe oder
  2. andere Teilnehmende des umgebenden Verkehrs, andere unbeteiligte Dritte oder die Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nicht gefährdende Ausweichmanöver möglich ist. Kann eine Kollision zur Abwendung einer Gefährdung des Lebens der Insassen des Kraftfahrzeugs mit autonomer Fahrfunktion nur durch eine Gefährdung des Lebens anderer Teilnehmender des umgebenden Verkehrs oder unbeteiligter Dritter vermieden werden (unvermeidbare alternative Gefährdung von Menschenleben), darf der Schutz der anderen Teilnehmenden des umgebenden Verkehrs und der unbeteiligten Dritten nicht nachrangig gegenüber dem Schutz der Insassen des autonom fahrenden Kraftfahrzeugs erfolgen.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.2 Interaktion mit anderen Verkehrsteilnehmenden
  a) Vorausfahrende Verkehrsteilnehmende auf der Fahrbahn werden erkannt. Es wird jederzeit in jedem Geschwindigkeitsbereich und in jeder möglichen Fahrsituation ein angemessener Sicherheitsabstand eingehalten. Der einzuhaltende Sicherheitsabstand bestimmt sich nach § 4 der Straßenverkehrs-Ordnung.
  b) Der Fahrstreifenwechsel vorausfahrender oder nachfolgender Fahrzeuge, der von einem benachbarten Fahrstreifen in den eigenen Fahrstreifen oder aus dem eigenen Fahrstreifen heraus in einen benachbarten Fahrstreifen erfolgt, wird erkannt und bei der Fahraufgabe entsprechend berücksichtigt.
  c) Situationen, welche einen Fahrstreifenwechsel bedingen (beispielsweise anhaltende oder langsame Fahrzeuge auf der Fahrbahn, Ende eines Fahrstreifens), werden erkannt und geeignete Manöver zum Fahrstreifenwechsel werden sicher durchgeführt.
  d) Einsatzfahrzeuge werden erkannt und geeignete Fahrmanöver sicher durchgeführt.
- AFGBV Anlage 1 Teil 1 Abschnitt 1.3 Planung der Fahrpfade und Geschwindigkeiten
  Bei Geschwindigkeitsanpassungen kommt es zu keiner vermeidbaren Beeinträchtigung von Insassen, anderen Verkehrsteilnehmenden und unbeteiligten Dritten. Es gelten folgende Anforderungen:

a) Geschwindigkeitsbeschränkungen und Änderungen der Geschwindigkeitsbeschränkung werden erkannt und die Geschwindigkeit wird entsprechend angepaßt.
b) Besondere Anforderungen an die Geschwindigkeit werden erkannt und im Geschwindigkeits- und Fahrtverlauf befolgt (beispielsweise in Bereichen vor Schulen und an Arbeitsstellen an Straßen, an Bushaltestellen, Bahnübergängen, in engen Kurvenradien oder bei Gefällen, in Engstellen, in denen der eigene Fahrstreifen vom Gegenverkehr mitbenutzt werden muß).
c) Zeichen und Weisungen der Polizeibeamten gemäß § 36 der Straßenverkehrs-Ordnung, Wechsellichtzeichen gemäß § 37 der Straßenverkehrs-Ordnung, sonstige Zeichen gemäß der §§ 39 bis 42 der Straßenverkehrs-Ordnung sowie Verkehrseinrichtungen gemäß § 43 der Straßenverkehrs-Ordnung werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
d) Situationen, in denen die Vorfahrt anderen gewährt werden muß (beispielsweise vor Fußgängerüberwegen, in Kreuzungsbereichen oder Einmündungen), werden erkannt und ohne Gefährdung oder Behinderung der Vorfahrtberechtigten bewältigt. Es ist eine berechnete Zeit bis zum Aufprall von mehr als drei Sekunden bezüglich des Vorfahrtberechtigen einzuhalten. Wird von diesen Werten abgewichen, muß dies ausreichend begründet und auf Basis von systematischen Sicherheitsbewertungen nach dem Stand der Technik dokumentiert werden. Das Erfordernis des Stands der Technik gilt als erfüllt, wenn die Vorgaben der ISO 26262:2018-12 Straßenfahrzeuge – Funktionale Sicherheit erfüllt werden.
e) Bauliche Straßengestaltungen mit Auswirkung auf das Verhaltensrecht (beispielsweise bis zu 5 Meter vom Fahrbahnrand einer vorfahrtberechtigten Straße abgesetzte Radwege nach § 9 Absatz 3 der Straßenverkehrs-Ordnung oder abgesenkte Bordsteine nach § 10 der Straßenverkehrs-Ordnung) werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
f) Arbeitsstellen an Straßen, temporär veränderte Fahrbahnverläufe oder Fahrbahnmarkierungen werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt.
g) Defizite am Zubehör, insbesondere der Verkehrseinrichtungen (zum Beispiel verschlissene, beschädigte, fehlende oder defekte temporäre oder dauerhafte Fahrbahnmarkierungen und Verkehrszeichen, Phantommarkierungen) und der Straßenausstattung, insbesondere solcher nach vorstehenden Buchstaben a bis f werden erkannt und im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Dies gilt insbesondere nach Sturm- und sonstigen Witterungsereignissen.

- AFGBV Anlage 1 Teil 1 Abschnitt 1.4 Reaktion auf Umweltbedingungen
  Wetter-, Umwelt- und Straßeninfrastrukturbedingungen (beispielsweise Regen, Sichtbehinderung durch Rauch, Schlaglöcher) werden im Geschwindigkeits- und Fahrtverlauf berücksichtigt. Fahrpfad und Geschwindigkeit sind – bis hin zum Stillstand des Fahrzeugs – so zu wählen, daß die in den Nummern 1.1 bis 1.3 gestellten Anforderungen auch bei geänderten Umweltbedingungen erfüllt werden.
- AFGBV Anlage 1 Teil 1 Abschnitt 3 Notfahrfunktion
  Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit einer Notfahrfunktion ausgestattet sein. Muß sich das Kraftfahrzeug im Falle eines Defekts am Kraftfahrzeug in den risikominimalen Zustand versetzen, muß dies mit der Notfahrfunktion erfolgen. Fahrten mit der Notfahrfunktion dürfen nur bei Schrittgeschwindigkeit und aktivierter Warnblinkanlage erfolgen. Der Übergang der autonomen Fahrfunktion aus der normalen Fahrt in die Fahrt mit der Notfahrfunktion ist von dieser Geschwindigkeitsbegrenzung ausgenommen, sofern ein Abbremsen erforderlich ist.
- AFGBV Anlage 1 Teil 1 Abschnitt 4 Manueller Fahrbetrieb
  Im manuellen Fahrbetrieb erfüllt eine fahrzeugführende Person die Fahraufgabe. Das Kraftfahrzeug mit autonomer Fahrfunktion muß mit Vorrichtungen ausgestattet sein, die es einer fahrzeugführenden Person ermöglichen, die Fahraufgabe wahrzunehmen. Ist die Steuerung im manuellen Fahrbetrieb auf Geschwindigkeiten nicht höher als Schrittgeschwindigkeit begrenzt, ist es nicht erforderlich, daß die fahrzeugführende Person sich innerhalb des Kraftfahrzeugs mit autonomer Fahrfunktion aufhält. Die Steuerung kann in diesem Fall über eine im Nahfeld des Kraftfahrzeugs befindliche Fernsteuerung ausgeführt werden. Die maximale Distanz, über die eine Fernsteuerung möglich ist, beträgt 6 Meter, gemessen in gerader Verbindung. Die Einhaltung der maximalen Distanz ist vom Hersteller durch geeignete technische Mittel sicher zu stellen. Soll das Kraftfahrzeug mit autonomer Fahrfunktion im manuellen Fahrbetrieb mit Geschwindigkeiten höher als Schrittgeschwindigkeit gesteuert werden, muß es mit einem Sitzplatz für die fahrzeugführende Person ausgestattet sein. Der Sitzplatz ist entsprechend der geltenden Vorschriften zu gestalten.
- AFGBV Anlage 1 Teil 1 Abschnitt 5 Dauerhafte Selbstüberwachung
  Die zur Wahrnehmung der Fahraufgabe nötige technische Ausrüstung muß vom Kraftfahrzeug mit autonomer Fahrfunktion selbstständig dauerhaft auf ihre Funktionalität hin überwacht werden. Die Überwachung ist so auszuführen, daß eine Beeinträchtigung der technischen Ausrüstung, die zur sicheren Teilnahme des Kraftfahrzeugs mit autonomer Fahrfunktion am Straßenverkehr nötig ist, in den risikominimalen Zustand führt.
- AFGBV Anlage 1 Teil 1 Abschnitt 5.1 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und ohne konventionelle Vorrichtungen zur dynamischen Ausübung der Fahraufgabe gilt:
  a) Zur dauerhaften Überwachung der technischen Ausrüstung werden nicht personenbezogene technische Daten im Kraftfahrzeug erhoben und gespeichert.
  b) Eine Beeinträchtigung der technischen Ausrüstung ist der Technischen Aufsicht unverzüglich anzuzeigen.

- AFGBV Anlage 1 Teil 1 Abschnitt 5.2 Dauerhafte Selbstüberwachung – Für Kraftfahrzeuge mit autonomer Fahrfunktion und mit konventionellen Vorrichtungen zur Ausübung der Fahraufgabe gilt:
  Die autonome Fahrfunktion darf nicht erneut aktivierbar sein, solange eine Beeinträchtigung der technischen Ausrüstung besteht.
- AFGBV Anlage 1 Teil 1 Abschnitt 6 Übertragung von Daten an das Kraftfahrzeug
  Die zur selbstständigen Bewältigung der Fahraufgabe im autonomen Betrieb notwendigen Daten und Informationen von externen technischen Einheiten (beispielsweise Backends oder Server eines Anbieters, externe Sensoren, Smartphone) müssen vom Kraftfahrzeug sicher empfangen und verwendet werden können. Daten externer Einheiten können im Kraftfahrzeug zur Ausführung der autonomen Fahrfunktionen verwendet werden. Daten und Informationen können beispielsweise bei bestimmten Anwendungsfällen über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) von einer externen technischen Einheit an das Kraftfahrzeug und vom Kraftfahrzeug an eine technische Einheit übertragen werden. Die Übertragung solcher Daten muß insbesondere den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen und nach dem aktuellen Stand der Technik abgesichert sein. Das Absicherungskonzept muß die in einer Bedrohungsanalyse identifizierten Risiken mit wirksamen Maßnahmen adressieren und eine Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 beinhalten. Zur Datenübertragung sollte eine zentrale sichere elektronische Steuereinheit (SECU) genutzt werden. Die SECU dient als Informationsgateway im Kraftfahrzeug. Die SECU kommuniziert intern an die Kommunikationsbusse des Kraftfahrzeugs und an den physischen On-Board-Diagnose II-Anschluß (OBD II) oder an eine proprietäre Schnittstelle eines Herstellers. Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung sind Teil 5 zu entnehmen. Die Integrität, Authentizität und Verfügbarkeit der Datenübertragung sind sicherzustellen. Die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen oder mit Infrastrukturkomponenten ist zulässig. Sie muß auf der Basis einer Datenschutzfolgeabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 insbesondere den Anforderungen an die Informationstechnik nach Teil 5 und damit den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechen. Während des Betriebs in einer optionalen Testphase ist die Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Fahrzeugen und Infrastrukturkomponenten zu testen und gegebenenfalls anzupassen.
- AFGBV Anlage 1 Teil 1 Abschnitt 7.1 Betriebshandbuch
  Zweck des Betriebshandbuchs ist es, mittels detaillierter Vorgaben den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten und der Technischen Aufsicht die richtige Reaktion auf Fehlerfälle zu ermöglichen.
- AFGBV Anlage 1 Teil 1 Abschnitt 8 Sensorik
  Zur technischen Umsetzung der autonomen Fahrfunktion muß eine Sensorik verwendet werden, die alle für die sichere Erfüllung der Fahraufgabe erforderlichen Gegenstände, Daten oder Personen im Umfeld des Kraftfahrzeugs erfaßt und hinsichtlich der Verarbeitung personenbezogener Daten die Vorgaben der Verordnung (EU) 2016/679, des Bundesdatenschutzgesetzes und spezialgesetzlicher datenschutzrechtlicher Vorschriften beachtet. Zur Erfüllung des in Satz 1 genannten Zwecks und unter Einhaltung der genannten Vorgaben kann die Sensorik durch externe Systeme unterstützt werden. Beeinflussen Wetter-, Umwelt- und Infrastrukturbedingungen die Leistungsfähigkeit der Sensorik, werden von der technischen Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion Maßnahmen eingeleitet, um die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken auszugleichen. Die Sensorik ist in das Sicherheitskonzept des Kraftfahrzeugs mit autonomer Fahrfunktion nach Nummer 7.2 und in die permanente Systemüberwachung nach Nummer 5 einzubinden.
- AFGBV Anlage 1 Teil 1 Abschnitt 9 Alterung und Abnutzung des Systems
  Das Kraftfahrzeug muß die funktionalen Anforderungen auch bei Alterung und Abnutzung der relevanten Systemkomponenten erfüllen. Beeinflussen Alterungserscheinungen die Leistungsfähigkeit, beispielsweise der Sensorik, gleicht die technische Ausrüstung des Kraftfahrzeugs mit autonomer Fahrfunktion die aus der verminderten Leistungsfähigkeit der Sensorik resultierenden Risiken durch geeignete Maßnahmen aus.
- AFGBV Anlage 1 Teil 2 Test- und Validierungsmethoden für Fahrzeuge mit autonomer Fahrfunktion (Abschnitt 10 bis 12) → *Definiert Test- und Validierungsmethoden, welche bei der Implementierung und Validierung anzuwenden sind.*
- AFGBV Anlage 1 Teil 3 Digitaler Datenspeicher Abschnitt 13 Allgemeine Anforderungen an den Datenspeicher
  Im Kraftfahrzeug mit autonomer Fahrfunktion muß ein den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datenspeicher integriert sein, der ereignisbasiert und während des Betriebs nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfaßt, speichert und verwendet. Die zu erfassenden Daten sind in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt. Der Datenspeicher ist entsprechend den in § 1g des Straßenverkehrsgesetzes und den in dieser Verordnung enthaltenen Datenschutz- und den Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 entsprechender Datensicherheitsvorschriften gemäß dem Stand der Technik auszugestalten. Ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren sind entsprechend der einschlägigen Technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vorzusehen. Das Bundesamt für die Sicherheit in der Informationstechnik ist in die konkrete

Ausgestaltung der Vorgaben einzubeziehen. Wesentliche Anforderungen an den Datenspeicher sind nachfolgend dargestellt.

- AFGBV Anlage 1 Teil 3 Abschnitt 13.1 Zu speichernde Ereignisse → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).
- AFGBV Anlage 1 Teil 5 Abschnitt 16 Sicherheit der Funkverbindung
  Die Verbindungen sind so auszuführen, daß der Schutz gegen einen unerlaubten Zugriff auf die Verbindungen die Vorgaben der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 umsetzt. Der Aufbau der Verbindung und die Datenübertragung sind nach dem Stand der Technik mit der Nutzung offener und etablierter Standards zu sichern und zu verschlüsseln (beispielsweise mit TLS 1.3 wie in der Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik im Januar 2020 und auf der Internetseite des Bundesamt für Sicherheit in der Informationstechnik (BSI).
- AFGBV Anlage 2 Datenspeicherung → Anforderungen aus Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).

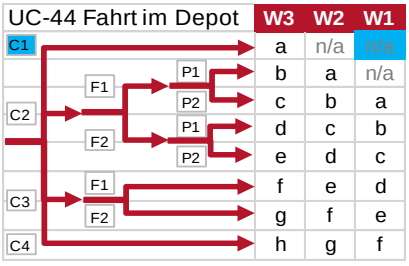
Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.
- BOStrab §46 Absatz 6
  Bei Fahrbetrieb ohne Fahrzeugführer müssen Personenfahrzeuge Einrichtungen für eine Sprechverbindung zwischen Fahrgästen und einer Betriebsstelle haben. Absatz 4 Satz 2 gilt entsprechend.
- BOStrab §52 Absatz 3
  Betriebsanlagen oder Fahrzeuge, die ganz oder teilweise selbsttätig arbeiten oder fernbedient werden, müssen im Rahmen der betrieblichen Erfordernisse von Betriebsbediensteten auf einwandfreie Funktion überwacht werden.

Gefahren nach HAZOP (Fahrt im Depot – Ausrückfahrt und Einrückfahrt):

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert.
  - ► Gefahr eines Unfalles, das autonom fahrende Fahrzeug erkennt einen Fußgänger nicht, weshalb es zu einem Unfall kommt ➔ geringe Auswirkung, wegen Geschwindigkeitsbegrenzung auf dem Firmengelände.
  - ► Sonderfall:
    BH-Mitarbeiter hält sich nicht an die Arbeitsvorschrift und nutzt das Fahrzeug zur Fahrt zum Ausgang des BH. → Unautorisierte UC-04 Fahrgastfahrt.

Risikograph (Fahrt im Depot – Ausrückfahrt und Einrückfahrt):



UC-44 Fahrt im Depot	W3	W2	W1
C1	a	n/a	n/a
C2 F1 P1	b	a	n/a
C2 F1 P2	c	b	a
C2 F2 P1	d	c	b
C2 F2 P2	e	d	c
C3 F1	f	e	d
C3 F2	g	f	e
C4	h	g	f

≙ QM per Restriktion, daß Fahrten im Betriebshof auf v≤6km/h begrenzt sind.

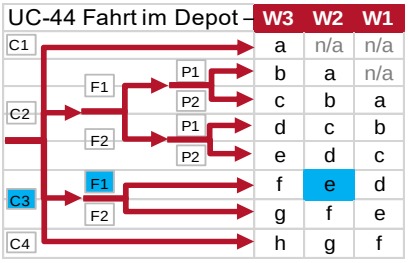
Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzung (Akzeptiertes Standardrisiko beim Arbeiten z.B. Fahrzeug Reinigung, Waschen, Parken und Laden, sowie der allgemeinen Fahrzeugnutzung unter der Randbedingung (Restriktion) Geschwindigkeitsbegrenzung ≤6km/h auf dem Betriebshof).
✖	
✖	
W1	Die angenommene Auswirkung kann unmittelbar eintreten, wenn das Fahrzeug in Betrieb genommen wird. Die Gefahr entspricht der normalen, typischen Teilnahme am Straßenverkehr, jedoch gilt auf dem Betriebshof, daß Fahrten in Schrittgeschwindigkeit (≤6km/h) auszuführen sind, welches als getroffene Gegenmaßnahme, schwere Verletzungen praktisch ausschließt. Somit ergibt sich eine Bewertung von W1.

Gefahren nach HAZOP (Fahrt im Depot – Abfahrkontrolle / Probefahrt):

- Die potentiellen Gefahren werden auf Basis der Betriebsprozesse ermittelt und bewertet sowie durch eine daraus resultierende Arbeitsvorschrift des ÖPNV-Unternehmens auf ein verbleibendes, akzeptables Risiko reduziert, jedoch müssen Kraftfahrzeuge mit autonomer Fahrfunktion mit im realen Betrieb vorkommenden Situationen realistisch auf die korrekte Arbeitsweise der Funktionen überprüft werden.
  - Gefahr eines simulierten Unfalles,
    das autonom fahrende Fahrzeug muß die juristisch geforderten Tests, insbesondere die dynamische Fahraufgabe und generelle Kollisionsvermeidung beanstandungsfrei absolvieren
    ➔ Nicht Einhaltung der Tests könnte im Real-Fall zu Verletzungen und Tod von Personen führen.
  - Nicht Funktionalität des Einklemmschutzes (Türkontrolle)
    ➔ Verletzungen könnten im Real-Fall eintreten, medizinische Versorgung könnte erforderlich werden.
  - Nicht Einhaltung von „Türen während der Fahrt geschlossen halten“
    (Türen können während der Fahrt geöffnet werden, oder öffnen verfrüht, oder schließen zu spät).
    ➔ Fahrgäste könnten im Real-Fall während der Fahrt aus dem Fahrzeug stürzen, was zu Verletzungen und Tod führen kann.
  - Nicht Einhaltung von Grenzwerten, z.B. Kraftfahrzeuge mit autonomer Fahrfunktion, die zur Beförderung von stehenden oder nicht angegurteten Fahrzeuginsassen eingesetzt werden, dürfen im Regelbetrieb eine Beschleunigung von 2,4 Meter pro Sekunde-Quadrat in der Ebene nicht überschreiten.
    ➔ Fahrgäste könnten im Real-Fall während der Fahrt Verletzungen bis hin zum Tod erleiden.

Risikograph (Fahrt im Depot – Abfahrkontrolle / Probefahrt):



≙ ASIL-C

Begründung zur Wahl der Risikoparameter:

C3	Tod mehrerer Personen bei einem schweren Unfall.
F1	seltener bis öfterer Aufenthalt im gefährlichen Bereich, hier Unfallschwerpunkte im realen Betrieb im öffentlichen Straßennetz
✖	
W2	Eine geringe Auftretenswahrscheinlichkeit und wenige unerwünschte Ereignisse sind wahrscheinlich.

3.2.45 UC-45 MissionCtrl

Steuerung (Umschalter), welche zwischen UC-03 Leerfahrt und UC-04 Fahrzeugfahrt, bzw. UC-44 Fahrt im Depot den Missionswechsel steuert.

Referenzmodell	Beschreibung der Aktivität	Verantwortlichkeit
ÖV-Leitstelle	Status Missionswechsel entgegennehmen sofern sich das Fahrzeug außerhalb des Betriebshofes befindet.	keine
BHMS	Status Missionswechsel entgegennehmen sofern sich das Fahrzeug innerhalb des Betriebshofes befindet.	keine
AD-Leitstelle	Die Systemüberwachung des AD-Bordsystems überwacht den Missionsablauf und wechselt automatisiert (bzw. aktiviert) die nächste Mission aus dem Umlauf, sobald die bisherige Mission beendet ist.	Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. Das AD-Bordsystem ist für die Umschaltung der Missionen zuständig. (Wechsel zwischen UC-03, UC-04 und UC-44).

Hinweis:
Das AD-Bordsystem ist zuständig, den automatisierten Missionswechsel umzusetzen

Hinweis:
Fahrtänderungen für Service & Wartungsumläufe / -fahrten / -fahrwege / -fahraufträge / -missionen obliegen dem BHMS eigenständig.

Hinweis:
Die Mission beschreibt einen Teil einer Fahrt zwischen zwei Haltepunkten / Haltestellen und beinhaltet Angaben zu
- dem Fahrgastwechsel (möglich / nicht möglich, d.h. die Türen werden am Ziel geöffnet bzw. nicht geöffnet)
- der Zeitspanne des Haltens (für den potentiellen Fahrgastwechsel / für das Laden des Fahrzeuges / …)
- der Umlaufnummer inklusive Angaben zum vorgegebenen Fahrweg (Wegpunkte, Route) zum Zielpunkt gemäß Fahrwegplanung der ÖV-Leitstelle
plus optional
- den Informationen zur Haltebucht
- der geplanten Fahrzeit zur Umsetzung der Mission gemäß Fahrwegplanung der ÖV-Leitstelle.

Betriebsschutz:
Fahrgäste dürfen nur Zugang zu Bedienelementen haben, welche zur Benutzung durch den Fahrgast vorgesehen sind. Der Zugang zu den Fahrzeugsystemen, insbesondere AD-Bordsystem und ÖV-Bordrechner (Sicherheitszone) ist durch angemessene Schutzmaßnahmen (Login + ggf. 2FA) gegen unautorisierten Zugriff durch geeignete sicherheitstechnische Verfahren (gegen Fremdzugriff und Manipulation) zu schützen, insbesondere Fahrgäste dürfen keinen Zugang erhalten können.

Situation:
Ablaufsteuerung (Regelbetrieb).

Aktionen:

- Die Systemüberwachung des AD-Bordsystems überwacht den Missionsablauf und wechselt automatisiert zur nächsten Mission sobald die bisherige Mission beendet ist.
- Das AD-Bordsystem informiert über die Aktivierung der nachfolgenden Mission aus dem Umlauf der ÖV-Leitstelle den ÖV-Bordrechner (über 14) sowie (über 8) die Technische Aufsicht (TA) der AD-Leitstelle.
- Der ÖV-Bordrechner informiert (über 7) die ÖV-Leitstelle.

Juristische Anforderungen:

- AFGBV §9 Absatz 2 Punkt 3
  Ein Betriebsbereich ist geeignet, wenn die zuständige Behörde feststellt, daß durch den Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion in diesem Betriebsbereich weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet werden.

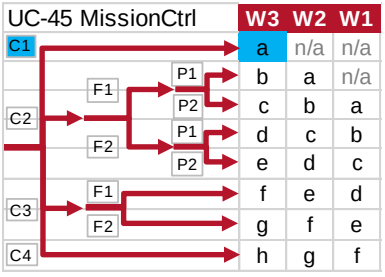
  Übertragung der Erfahrungen aus dem Schienenverkehr auf straßengebundenen Verkehrssysteme gemäß GVB.

- BOStrab §3 Absatz 1
  Betriebsanlagen und Fahrzeuge müssen so gebaut sein, daß ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet oder behindert.

Gefahren nach HAZOP:

- Die Aktivierung (selbst) der Folgemission hat keinen direkten Einfluß auf die Sicherheit, weil die Sicherheit durch die drei UseCases (Leerfahrt, Fahrgastfahrt mit/ohne Fahrgäste im Fahrzeug und Fahrt im Depot) behandelt werden. Eine Leerfahrt ist eine Fahrt ohne Fahrgäste (Verbot) außerhalb des Depots. Eine Fahrt im Depot ist eine Fahrt ohne Fahrgäste (Verbot) im Depot. Das Verbot von Fahrgästen ist nicht der Sicherheit, sondern der Security (Schutz durch unberechtigten Zugang zu Sicherheitszonen) geschuldet, weshalb bei diesen beiden UseCases vor Abfahrt eine Überprüfung des Innenraumes erfolgt um sicherzustellen, daß sich keine Person im Fahrzeug befindet.

Risikograph:



UC-45 MissionCtrl	W3	W2	W1
C1	a	n/a	n/a
C2 F1 P1	b	a	n/a
C2 F1 P2	c	b	a
C2 F2 P1	d	c	b
C2 F2 P2	e	d	c
C3 F1	f	e	d
C3 F2	g	f	e
C4	h	g	f

≙ QM

Begründung zur Wahl der Risikoparameter:

C1	Geringe Verletzungen durch den gefährlichen Vorfall.
✖	
✖	
W3	Eine relativ hohe Auftretenswahrscheinlichkeit und häufige unerwünschte Ereignisse sind wahrscheinlich. Hinweis: Es gibt eine sehr hohe Auftretenswahrscheinlichkeit, aber unerwünschte Ereignisse sind unwahrscheinlich.

3.3 Anforderungen zur Absicherung der operativen Situationen (Use Cases)

3.3.1 Zuordnung der Verantwortlichkeit mit Sicherheitsrelevanz (Matrix)

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-01 Fahrzeug aufrüsten	QM	V	V	A	V	A
■ Sicherstellung der Einsatzbereitschaft / Betriebsbereitschaft der Fahrzeuge inklusive Nachweis der Gewährleistung der Einhaltung der Reparatur- und Wartungsinformationen der Fahrzeugsysteme gemäß den Vorgaben des Herstellers. ■ Nachweis der Durchführung der täglichen vor Betriebsbeginn umzusetzenden erweiterten Abfahrkontrolle nach Absatz 7. ► Bremsanlage, ► Lenkanlage, ► Lichtanlage, ► Reifen/Räder, ► Fahrwerk, ► sicherheitsrelevante elektronisch geregelte Fahrzeugsysteme sowie die Sensorik zur Erfassung externer und interner Parameter und ► mechanische Fahrzeugsysteme für die aktive und passive Sicherheit. Hinweis: Die in Absatz 7 geforderte Probefahrt wird umgesetzt in UC-44 Fahrt im Depot mit der dort gültigen Sicherheitsrelevanz. ■ Nachweis der umgesetzten Gesamtprüfung alle 90 Tage. ■ Nachweis der Eignung der maßnahmenumsetzenden Mitarbeiter des BHMS.	QM	V	I	A	I	A
■ Disposition inklusive Fahrpläne (Umläufe), Kapazitätsplanung und Einsatzplanung.	QM	I	V	A	I	A
■ Fahrzeuganmeldung entgegennehmen und Fahrzeugstatus erfassen. ■ Verifikation der Beseitigung bekannter Mängel der Fahrsicherheit.	QM	A	I	A	V	A
UC-02 Umlaufanmeldung/-zuweisung	QM	V	V	A	V	A
■ Konfiguration der Fahrbereitschaft zur Betriebsaufnahme. ► Erweiterte Abfahrkontrolle (Probefahrt) ► Einsetzfahrt Hinweis: Gültig für die Konfiguration, die Fahrten auf dem Betriebshof inklusive der Abfahrkontrolle erfolgen mit UC-44 Fahrt im Depot unter der dortigen Sicherheitsrelevanz.	QM	V	I	A	I	A
■ Überprüfen des konfigurierten Fahrweges des Fahrzeugs / Platoon gemäß den Fahrplandaten, sofern notwendig / sinnvoll, Ergreifen von Maßnahmen um die Routenführung anzupassen um die Pünktlichkeit wiederherzustellen, Informieren der mitreisenden und potentiellen Fahrgäste über Einhaltung / Abweichung der Pünktlichkeit, sowie Unterstützen bei der Sicherstellung des zeitgerechten Erreichens bei Anschlüssen der Fahrt, sofern dieses erforderlich ist. Hinweis: Gültig für regulären Fahrbetrieb außerhalb des BHMS.	QM	I	V	A	I	A
■ Überwachung der autonomen Fahrt sowie Eingreifen im Bedarfsfall.	QM	A	I	A	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-03 Leerfahrt	ASIL C	n/a	V	A	V	A
■ Überwachen des Fahrweges des Fahrzeuges / Platoon gemäß den Fahrplandaten, sofern notwendig / sinnvoll, Ergreifen von Maßnahmen um die Pünktlichkeit wiederherzustellen, Informieren der mitreisenden und potentiellen Fahrgäste über Einhaltung / Abweichung der, sowie Unterstützen bei der Sicherstellung des zeitgerechten Erreichens bei Anschlüssen der Fahrt. ■ Aktualisierung der Linienanzeiger über UC-18 Zielbeschilderung außen und innen ändern.	QM (C)	n/a	V	A	I	A
■ Nachweis (Videoaufzeichnung) der optischen Überprüfung des Fahrgastraumes zur Sicherstellung, daß sich keine Lebensform während der Leerfahrt im Fahrzeug befindet. ■ Überwachung der automatisierten Türschließung über UC-06 Türkontrolle. ▶ Verhinderung der Anfahrt mit geöffneten Türen = ASIL-A, VDV-Schrift-161-2 Kap. 3.4.1 ▶ Türschließwarnung (optisch/akustisch) = QM VDV-Schrift-161-2 Kap. 3.4.3 ▶ Einklemmschutz während des Schließvorgangs = QM VDV-Schrift-161-2 Kap. 3.4.4 ▶ Festhalten der Türen in geschlossener Stellung während der Fahrt = ASIL-B VDV-Schrift-161-2 Kap. 3.4.2 ■ Überwachung der autonomen Fahrt = ASIL-C	ASIL C	n/a	I	I	V	A
UC-04 Fahrgastfahrt	ASIL C	n/a	V	I	V	A
■ Überwachen des Fahrweges des Fahrzeuges / Platoon gemäß den Fahrplandaten, sofern notwendig / sinnvoll, Ergreifen von Maßnahmen um die Pünktlichkeit wiederherzustellen, Informieren der mitreisenden und potentiellen Fahrgäste über Einhaltung / Abweichung der, sowie Unterstützen bei der Sicherstellung des zeitgerechten Erreichens bei Anschlüssen der Fahrt.	QM (C)	n/a	V	A	I	A
■ Überwachung der autonomen Fahrt = ASIL-C ■ Überwachung der automatisierten Türschließung über UC-06 Türkontrolle. ▶ Verhinderung der Anfahrt mit geöffneten Türen = ASIL-A, VDV-Schrift-161-2 Kap. 3.4.1 ▶ Türschließwarnung (optisch/akustisch) = QM VDV-Schrift-161-2 Kap. 3.4.3 ▶ Einklemmschutz während des Schließvorgangs = QM VDV-Schrift-161-2 Kap. 3.4.4 ▶ Festhalten der Türen in geschlossener Stellung während der Fahrt = ASIL-B VDV-Schrift-161-2 Kap. 3.4.2	ASIL C	n/a	I	I	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-05 Regelhalt	QM	n/a	V	A	V	A
■ Überwachen des Fahrweges des Fahrzeuges / Platoon gemäß den Fahrplandaten sowie Informieren der mitreisenden Fahrgäste rechtzeitig per Durchsage über das Erreichen der Haltestelle / Halteposition, damit die Fahrgäste einen Aussteigewunsch abgeben können. ■ (Optional) Ausgabe eines akustischen und optischen Warnsignals in den Fahrgastraum, welches anzeigt, daß die Tür jetzt geöffnet wird, welches ggf. von einer Audio-Durchsage „Vorsicht …“ ergänzt werden kann. *Hinweis:* *Die Ausgabe des akustischen und optischen Warnsignals ist Aufgabe des Türsteuergerätes des Fahrzeugherstellers (OEM), jedoch kann die Signalisierung des Fahrzeugherstellers (OEM) durch den ÖV-Bordrechner ergänzt / ggf. ersetzt werden.* ► Türöffnung ≙Türschließwarnung (optisch/akustisch) = QM VDV-Schrift-161-2 Kap. 3.4.3	QM	n/a	V	A	n/a (rückwirkungsfrei)	A
■ Mit dem Erreichen des Wegpunktes, ab welchem eine sichere Detektion von potentiell wartenden Fahrgästen an Haltestellen / Haltepositionen mit erlaubtem Fahrgastwechsel erreicht wurde, wird die KI gestützte „Erkennung von Fahrgästen an der Haltestelle“ umgesetzt. = QM ■ Sicherstellung des Anhaltens sowie Signalsendung der Türöffnung ► Türöffnung ≙Türschließwarnung (optisch/akustisch) = QM VDV-Schrift-161-2 Kap. 3.4.3 *Hinweis:* *Die Ausgabe des akustischen und optischen Warnsignals ist Aufgabe des Türsteuergerätes des Fahrzeugherstellers (OEM), jedoch kann der ÖV-Bordrechner die Signalisierung des Fahrzeugherstellers (OEM) durch eine eigene Ausgabe ergänzen / ggf. ersetzen.* ► Festhalten der Türen in geschlossener Stellung während der Fahrt = ASIL-B VDV-Schrift-161-2 Kap. 3.4.2 *Hinweis:* *Dieses wird von UC-03 / UC-04 / UC-44 umgesetzt, jedoch nicht von UC-05 (v=0km/h).*	QM	n/a	I	I	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-06 Türkontrolle	ASIL A	n/a	V	A	V	A
■ Fahrgäste rechtzeitig per Durchsage über das Schließen der Türen informieren, damit die Fahrgäste den Türbereich freigeben können. ■ Bei der ÖV-Umlaufplanung genügend Zeit für den Fahrgastwechsel in den jeweiligen Missionen vorsehen.	QM (A)	n/a	V	A	n/a (rückwirkungsfrei)	A
■ Überwachung der automatisierten Türschließung ▶ Verhinderung der Anfahrt mit geöffneten Türen = ASIL-A, VDV-Schrift-161-2 Kap. 3.4.1 ▶ Türschließwarnung (optisch/akustisch) = QM VDV-Schrift-161-2 Kap. 3.4.3 ▶ Einklemmschutz während des Schließvorgangs = QM VDV-Schrift-161-2 Kap. 3.4.4 ▶ Festhalten der Türen in geschlossener Stellung während der Fahrt = ASIL-B VDV-Schrift-161-2 Kap. 3.4.2 *Hinweis: Dieses wird von UC-03 / UC-04 / UC-44 umgesetzt, jedoch nicht von UC-06 (Türschließung vor der Abfahrt, v=0km/h)* ■ Kommunikation mit Fahrgästen im Problemfall sowie Problemlösung initiieren.	ASIL A	n/a	I	I	V	A
UC-07 Fahrzeug abrüsten	QM	V	V	A	V	A
■ Sicherstellung der Aufrechterhaltung der Einsatz- / Betriebsbereitschaft der Fahrzeuge inklusive Umlauf Fahrzeugpflege Service & Wartung) mit Einhaltung der Reparatur- und Wartungsinformationen der Fahrzeugsysteme gemäß den Vorgaben des Herstellers. ■ Sofern ein Instandsetzungsauftrag (Was) von der AD-Leitstelle vorliegen sollte, schreibt der Disponent des BHMS die dafür notwendigen Instandsetzungsaufträge (Wer und Wann) und plant deren Umsetzung und der damit ggf. verbundenen Nicht-Verfügbarkeit des Fahrzeuges. ■ Nachweis der Eignung der maßnahmenumsetzenden Mitarbeiter des BHMS.	QM	V	I	A	I	A
■ Auswertung der Statistikwerte (Fahrplandaten, Ticketing-Daten) zur Optimierung der Geschäftsprozesse.	QM	A	V	A	n/a (rückwirkungsfrei)	n/a (rückwirkungsfrei)
■ Auswertung der Ereignismeldungen und Logfiles, Erstellung der Instandsetzungsanforderungen (inklusive Softwareaktualisierungen und Sicherheitspatches) mit Erstellung der Beauftragung (Was) für das BHMS sowie der aktuellen Nutzungserlaubnis für das Fahrzeug (Autonome Fahrt ist erlaubt / erlaubt mit Auflagen / gesperrt). *Hinweis:* *Probefahrten und Fahrten zwischen den Stationen des BHMS werden über* UC-44 Fahrt im Depot *abgewickelt. Die zugehörige Sicherheitsrelevanz ist dort hinterlegt.*	QM	A	I	A	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-08 Datenaktualisierung	QM	V	V	A	V	A
■ Das BHMS ist verantwortlich für die Umsetzung der Softwareaktualisierung und deren Konfiguration gemäß den Vorgaben der ÖV-Leitstelle. ■ Das BHMS ist verantwortlich für die Umsetzung der Softwareaktualisierung und deren Konfiguration gemäß den Vorgaben der AD-Leitstelle. ■ Das BHMS ist verantwortlich für die Umsetzung der Softwareaktualisierung und deren Konfiguration gemäß den Vorgaben des Fahrzeugherstellers (OEM). ■ Das BHMS ist verantwortlich für das Testen des Fahrzeuges, insbesondere der einwandfreien Funktion der aktualisierten Software.	QM	V	A	I	A	I
■ Die ÖV-Leitstelle ist verantwortlich für die Pflege und die zeitlich angemessene Installation von Sicherheitspatches bei den ÖV-Systemen inklusive Überwachung der Sicherheit und Funktionsfähigkeit, sowie der Absicherung gegen unberechtigte Zugriffe.	QM	A	V	I	I	n/a (rückwirkungsfrei)
■ Die AD-Leitstelle ist verantwortlich für die Pflege und die zeitlich angemessene Installation von Sicherheitspatches bei den AD-Systemen im Fahrzeug plus den Systemen der Technischen Aufsicht (TA), inklusive Überwachung der Sicherheit und der Funktionsfähigkeit, sowie der Absicherung gegen unberechtigte Zugriffe. *Hinweis:* *Die Tätigkeit der Softwarepflege inklusive des Security Vulnerability Monitorings (SVM) ist unabhängig von der Sicherheitsrelevanz der betroffenen Systeme, d.h. die Tätigkeit der Überwachung ist QM, die überwachte Software kann QM oder auch einem ASIL-D unterliegen.*	QM	A	I	n/a (rückwirkungsfrei)	V	I
UC-09 Datenentsorgung	QM	V	V	A	V	A
■ Das BHMS ist verantwortlich für die Umsetzung der Datenentsorgung der Fahrgastdaten auf dem Fahrzeug sowie für die Datenübermittlung an die ÖV-Leitstelle. ■ Das BHMS ist verantwortlich für die Datenentsorgung der AD-Fahrzeugdaten auf dem Fahrzeug sowie für die Datenübermittlung an die AD-Leitstelle bzw. zuständige Behörde.	QM	V	I	A	I	A
■ Die ÖV-Leitstelle ist verantwortlich für die Datenarchivierung der Fahrgastdaten gemäß den Aufbewahrungspflichten.	QM	n/a (rückwirkungsfrei)	V	n/a	n/a	n/a
■ Die AD-Leitstelle ist verantwortlich für die Datenarchivierung der AD-Fahrzeugdaten inklusive der Überwachungsaufzeichnung gemäß den Aufbewahrungspflichten. ■ Die Berichte sind zu dokumentieren und vom Halter oder von der für die Technische Aufsicht verantwortlichen Person sechs Monate lang aufzubewahren und nach Ablauf dieser Frist unverzüglich, bei elektronischer Speicherung automatisiert, zu löschen.	QM	n/a (rückwirkungsfrei)	n/a	n/a	V	n/a

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-10 Fahrgastzählung	QM	A	V	A	n/a (rückwirkungsfrei)	n/a (rückwirkungsfrei)
■ Das BHMS ist zuständig für die Datenentsorgung der Fahrgastdaten unter Beachtung der Betriebsvorschriften (Verfahrensanweisung / Arbeitsvorschrift) zur Datensicherung, Datennutzung und Datenentsorgung inklusive deren Übermittlung an die ÖV-Leitstelle.	QM	A	I	A	n/a (rückwirkungsfrei)	n/a (rückwirkungsfrei)
■ Die ÖV-Leitstelle ist verantwortlich für die Datenauswertung inklusive der Datenarchivierung der Fahrgastdaten gemäß den Aufbewahrungspflichten.	QM	n/a (rückwirkungsfrei)	V	n/a (rückwirkungsfrei)	n/a (rückwirkungsfrei)	n/a (rückwirkungsfrei)
UC-11 Stauerkennung	QM	n/a (rückwirkungsfrei)	V	A	n/a (rückwirkungsfrei)	n/a (rückwirkungsfrei)
■ Der ÖV-Bordrechner ist zuständig für die Stauerkennung. Sobald innerhalb einer bestimmten Zeit nur eine geringe Strecke zurückgelegt wird, sendet der ÖV-Bordrechner eine Warnmeldung an die ÖV-Leitstelle ■ Die ÖV-Leitstelle ist verantwortlich für die Ergreifung notwendiger Maßnahmen zur Wiederherstellung der Fahrplaneinhaltung (Pünktlichkeit)	QM	n/a (rückwirkungsfrei)	V	A	n/a (rückwirkungsfrei)	n/a (rückwirkungsfrei)

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-12 Systemüberwachung und ggf. Störmeldung	ASIL C	V	V	I	V	A
■ Das BHMS ist verantwortlich für die Instandhaltung und Wartung der Systeme inklusive Nachweis der technischen Verwendbarkeit durch das Testen des Fahrzeuges. Randbedingung: Das Fahrzeug befindet sich auf dem Betriebshof (Schnittstelle 3 ist deaktiviert über Schnittstelle 5).	ASIL C	V	n/a (rückwirkungsfrei)	A	I	A
■ Die ÖV-Leitstelle ist verantwortlich für die Ergreifung notwendiger Maßnahmen zur Wiederherstellung der Fahrplaneinhaltung (Pünktlichkeit) im regulären Fahrbetrieb außerhalb des Betriebshofes. Randbedingung: Das Fahrzeug befindet sich außerhalb des Betriebshofes (Regelbetrieb) (Schnittstelle 4 ist deaktiviert über Schnittstelle 5).	QM (C)	n/a (rückwirkungsfrei)	V	A	I	A
Randbedingung: Das Fahrzeug befindet sich auf dem Betriebshof (Schnittstelle 3 ist deaktiviert über Schnittstelle 5). ■ Die AD-Leitstelle ist verantwortlich für die Überwachung der autonomen Fahrt inklusive Umsetzung ▶ der erweiterten Abfahrkontrolle (Probefahrt) = ASIL-C ▶ der Überwachung der automatisierten Türschließung über UC-06 Türkontrolle. ▶ Verhinderung der Anfahrt mit geöffneten Türen = ASIL-A, VDV-Schrift-161-2 Kap. 3.4.1 ▶ Türschließwarnung (optisch/akustisch) = QM VDV-Schrift-161-2 Kap. 3.4.3 ▶ Einklemmschutz während des Schließvorgangs = QM VDV-Schrift-161-2 Kap. 3.4.4 ▶ Festhalten der Türen in geschlossener Stellung während der Fahrt = ASIL-B VDV-Schrift-161-2 Kap. 3.4.2	ASIL C	A	n/a (rückwirkungsfrei) bei Wartung auf dem Betriebshof	I	V	A
Randbedingung: Das Fahrzeug befindet sich außerhalb des Betriebshofes (Regelbetrieb) (Schnittstelle 4 ist deaktiviert über Schnittstelle 5). ■ Die AD-Leitstelle ist verantwortlich für die Überwachung der autonomen Fahrt = ASIL C ▶ Überwachung der automatisierten Türschließung über UC-06 Türkontrolle. ▶ Verhinderung der Anfahrt mit geöffneten Türen = ASIL-A, VDV-Schrift-161-2 Kap. 3.4.1 ▶ Türschließwarnung (optisch/akustisch) = QM VDV-Schrift-161-2 Kap. 3.4.3 ▶ Einklemmschutz während des Schließvorgangs = QM VDV-Schrift-161-2 Kap. 3.4.4 ▶ Festhalten der Türen in geschlossener Stellung während der Fahrt = ASIL-B VDV-Schrift-161-2 Kap. 3.4.2	ASIL C	n/a (rückwirkungsfrei) im regulären Fahrbetrieb	I	I	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-13 Fahrtänderung	ASIL D	V (im Betriebshof)	V (außerhalb Betriebshof)	A	I	A
■ Das BHMS ist verantwortlich für die Instandhaltung und Wartung der Systeme inklusive Nachweis der technischen Verwendbarkeit durch das Testen des Fahrzeuges. Hinweis: Fahrtänderungen treten auf, wenn der Ablauf des Abfahrens der Stationen sich ändert, weil z.B. eine Station leergelaufen ist oder bei einer Station sich ein Stau gebildet hat.	QM (D)	V	n/a (rückwirkungsfrei)	A	I	A
■ Die ÖV-Leitstelle ist verantwortlich für die Ergreifung notwendiger Maßnahmen zur Wiederherstellung der Fahrplaneinhaltung (Pünktlichkeit) im regulären Fahrbetrieb außerhalb des Betriebshofes.	QM (D)	n/a (rückwirkungsfrei)	V	A	I	A
Randbedingung: Das Fahrzeug befindet sich in der Fahrt. ■ Die AD-Leitstelle ist verantwortlich für die Überwachung der autonomen Fahrt = ASIL-C, aber die Änderung der Fahrtrichtung (Routenänderung) während der Fahrt kann unmittelbar (ad hoc) ein Abbiegen einfordern, welches mit der aktuellen Geschwindigkeit der bisherigen Geradeausfahrt nicht vereinbar ist. Die unerwartet auftretende Seitenführungskraft (im Zusammenhang mit der Längsführungskraft) kann das Rad eines Fahrzeuges nicht auf die Straße übertragen (Kammscher Kreis), welches zusätzlich auch noch durch die Wetterabhängigkeit beeinflußt wird. Die Reaktionsfähigkeit des Menschen (Technische Aufsicht) wird hierbei überfordert und das Autonomous Driving System (ADS) des Fahrzeugherstellers kann dieses ebenfalls nicht kompensieren, weil die Eingriffsmöglichkeit der Technischen Aufsicht (TA) über das AD-Bordsystem (ADBS) die Fahrzeugfunktion übersteuern können muß. → ASIL-D. ▶ Überwachung der automatisierten Türschließung über UC-06 Türkontrolle. ▶ Festhalten der Türen in geschlossener Stellung während der Fahrt = ASIL-B VDV-Schrift-161-2 Kap. 3.4.2	ASIL D	I (im Betriebshof)	I (außerhalb Betriebshof)	A	V	A
Randbedingung: Das Fahrzeug befindet sich außerhalb des Betriebshofes (Regelbetrieb) an der Haltestelle / Halteposition oder auf dem Betriebshof an einer Servicestation im Stillstand (v = 0km/h). ■ Die AD-Leitstelle ist verantwortlich für die Überwachung der autonomen Fahrt inklusive Umsetzung der ▶ Überwachung der automatisierten Türschließung über UC-06 Türkontrolle. ▶ Verhinderung der Anfahrt mit geöffneten Türen = ASIL-A, VDV-Schrift-161-2 Kap. 3.4.1 ▶ Türschließwarnung (optisch/akustisch) = QM VDV-Schrift-161-2 Kap. 3.4.3 ▶ Einklemmschutz während des Schließvorgangs = QM VDV-Schrift-161-2 Kap. 3.4.4	ASIL A(D)	I (im Betriebshof)	I (außerhalb Betriebshof)	A	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-14 Umlaufänderung	ASIL D	V (im Betriebshof)	V (außerhalb Betriebshof)	A	I	A
■ Das BHMS ist verantwortlich für die Instandhaltung und Wartung der Systeme inklusive Nachweis der technischen Verwendbarkeit durch das Testen des Fahrzeuges. Hinweis: Umlaufänderungen treten auf, wenn der Ablauf des Abfahrens der Stationen sich ändert, weil z.B. eine Station leergelaufen ist oder bei einer Station sich ein Stau gebildet hat.	QM (D)	V	n/a (rückwirkungsfrei)	A	I	A
■ Die ÖV-Leitstelle ist verantwortlich für die Ergreifung notwendiger Maßnahmen zur Wiederherstellung der Fahrplaneinhaltung (Pünktlichkeit) im regulären Fahrbetrieb außerhalb des Betriebshofes.	QM (D)	n/a (rückwirkungsfrei)	V	A	I	A
Randbedingung: Das Fahrzeug befindet sich in der Fahrt. ■ Die AD-Leitstelle ist verantwortlich für die Überwachung der autonomen Fahrt = ASIL-C, aber die Änderung der Fahrtrichtung (Routenänderung) während der Fahrt kann unmittelbar (ad hoc) ein Abbiegen einfordern, welches mit der aktuellen Geschwindigkeit der bisherigen Geradeausfahrt nicht vereinbar ist. Die unerwartet auftretende Seitenführungskraft (im Zusammenhang mit der Längsführungskraft) kann das Rad eines Fahrzeuges nicht auf die Straße übertragen (Kammscher Kreis), welches zusätzlich auch noch durch die Wetterabhängigkeit beeinflußt wird. Die Reaktionsfähigkeit des Menschen (Technische Aufsicht) wird hierbei überfordert und das Autonomous Driving System (ADS) des Fahrzeugherstellers kann dieses ebenfalls nicht kompensieren, weil die Eingriffsmöglichkeit der Technischen Aufsicht (TA) über das AD-Bordsystem (ADBS) die Fahrzeugfunktion übersteuern können muß. → ASIL-D. ▶ Überwachung der automatisierten Türschließung über UC-06 Türkontrolle. ▶ Festhalten der Türen in geschlossener Stellung während der Fahrt = ASIL-B VDV-Schrift-161-2 Kap. 3.4.2	ASIL D	I (im Betriebshof)	I (außerhalb Betriebshof)	A	V	A
Randbedingung: Das Fahrzeug befindet sich außerhalb des Betriebshofes (Regelbetrieb) an der Haltestelle / Halteposition oder auf dem Betriebshof an einer Servicestation im Stillstand (v = 0km/h). ■ Die AD-Leitstelle ist verantwortlich für die Überwachung der autonomen Fahrt inklusive Umsetzung der ▶ Überwachung der automatisierten Türschließung über UC-06 Türkontrolle. ▶ Verhinderung der Anfahrt mit geöffneten Türen = ASIL-A, VDV-Schrift-161-2 Kap. 3.4.1 ▶ Türschließwarnung (optisch/akustisch) = QM VDV-Schrift-161-2 Kap. 3.4.3 ▶ Einklemmschutz während des Schließvorgangs = QM VDV-Schrift-161-2 Kap. 3.4.4	ASIL A(D)	I (im Betriebshof)	I (außerhalb Betriebshof)	A	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-15 Neuen Umlauf hinzufügen	ASIL C	V (im Betriebshof)	V (außerhalb Betriebshof)	A	I	A
■ Das BHMS ist verantwortlich für die Instandhaltung und Wartung der Systeme inklusive Nachweis der technischen Verwendbarkeit durch das Testen des Fahrzeuges. Hinweis: Fahrtänderungen treten auf, wenn der Ablauf des Abfahrens der Stationen sich ändert, weil z.B. eine Station leergelaufen ist oder bei einer Station sich ein Stau gebildet hat.	QM (C)	V	n/a (rückwirkungsfrei)	A	I	A
■ Die ÖV-Leitstelle ist verantwortlich für das Ergreifen notwendiger Maßnahmen zur Wiederherstellung der Fahrplaneinhaltung (Pünktlichkeit) im regulären Fahrbetrieb außerhalb des Betriebshofes.	QM (C)	n/a (rückwirkungsfrei)	V	A	I	A
Randbedingung: Das Fahrzeug befindet sich in der Fahrt. ■ Die AD-Leitstelle ist verantwortlich für die Überwachung der autonomen Fahrt = ASIL-C Hinweis: Hier wird die bisherige Fahrt (zwischen zwei Haltestellen / Haltepunkten) nicht ad hoc verändert, sondern es werden zusätzlich Fahrten/Mission angehängt. ▶ Überwachung der automatisierten Türschließung über UC-06 Türkontrolle. ▶ Festhalten der Türen in geschlossener Stellung während der Fahrt = ASIL-B VDV-Schrift-161-2 Kap. 3.4.2	ASIL C	I (im Betriebshof)	I (außerhalb Betriebshof)	A	V	A
Randbedingung: Das Fahrzeug befindet sich außerhalb des Betriebshofes (Regelbetrieb) an der Haltestelle / Halteposition oder auf dem Betriebshof an einer Servicestation im Stillstand (v = 0km/h). ■ Die AD-Leitstelle ist verantwortlich für die Überwachung der autonomen Fahrt inklusive Umsetzung der ▶ Überwachung der automatisierten Türschließung über UC-06 Türkontrolle. ▶ Verhinderung der Anfahrt mit geöffneten Türen = ASIL-A, VDV-Schrift-161-2 Kap. 3.4.1 ▶ Türschließwarnung (optisch/akustisch) = QM VDV-Schrift-161-2 Kap. 3.4.3 ▶ Einklemmschutz während des Schließvorgangs = QM VDV-Schrift-161-2 Kap. 3.4.4	ASIL A(C)	I (im Betriebshof)	I (außerhalb Betriebshof)	A	V	A
UC-16 Neue Fahrplandaten aufgrund dispositiver Maßnahmen verteilen	ASIL D	V (im Betriebshof)	V (außerhalb Betriebshof)	A	I	A
■ Das BHMS ist verantwortlich für die Instandhaltung und Wartung der Systeme inklusive Nachweis der technischen Verwendbarkeit durch das Testen des Fahrzeuges. Hinweis: Neue Fahrplandaten treten auf, wenn der Ablauf des Abfahrens der Stationen sich ändert, weil z.B. eine Station leergelaufen ist oder bei einer Station sich ein Stau gebildet hat oder eine Station ausgefallen (defekt) ist.	QM (D)	V	n/a (rückwirkungsfrei)	A	I	A
■ Die ÖV-Leitstelle ist verantwortlich für die Ergreifung notwendiger Maßnahmen zur Wiederherstellung der Fahrplaneinhaltung (Pünktlichkeit) im regulären Fahrbetrieb außerhalb des Betriebshofes.	QM (D)	n/a (rückwirkungsfrei)	V	A	I	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
Randbedingung: Das Fahrzeug befindet sich in der Fahrt. ■ Die AD-Leitstelle ist verantwortlich für die Überwachung der autonomen Fahrt = ASIL-C, aber die Änderung der Fahrtrichtung (Routenänderung) während der Fahrt kann unmittelbar (ad hoc) ein Abbiegen einfordern, welches mit der aktuellen Geschwindigkeit der bisherigen Geradeausfahrt nicht vereinbar ist. Die unerwartet auftretende Seitenführungskraft (im Zusammenhang mit der Längsführungskraft) kann das Rad eines Fahrzeuges nicht auf die Straße übertragen (Kammscher Kreis), welches zusätzlich auch noch durch die Wetterabhängigkeit beeinflußt wird. Die Reaktionsfähigkeit des Menschen (Technische Aufsicht) wird hierbei überfordert und das Autonomous Driving System (ADS) des Fahrzeugherstellers kann dieses ebenfalls nicht kompensieren, weil die Eingriffsmöglichkeit der Technischen Aufsicht (TA) über das AD-Bordsystem (ADBS) die Fahrzeugfunktion übersteuern können muß. → ASIL-D. ▶ Überwachung der automatisierten Türschließung über UC-06 Türkontrolle. ▶ Festhalten der Türen in geschlossener Stellung während der Fahrt = ASIL B VDV-Schrift-161-2 Kap. 3.4.2	ASIL D	I (im Betriebshof)	I (außerhalb Betriebshof)	A	V	A
Randbedingung: Das Fahrzeug befindet sich außerhalb des Betriebshofes (Regelbetrieb) an der Haltestelle / Halteposition oder auf dem Betriebshof an einer Servicestation im Stillstand (v = 0km/h). ■ Die AD-Leitstelle ist verantwortlich für die Überwachung der autonomen Fahrt inklusive Umsetzung der ▶ Überwachung der automatisierten Türschließung über UC-06 Türkontrolle. ▶ Verhinderung der Anfahrt mit geöffneten Türen = ASIL-A, VDV-Schrift-161-2 Kap. 3.4.1 ▶ Türschließwarnung (optisch/akustisch) = QM VDV-Schrift-161-2 Kap. 3.4.3 ▶ Einklemmschutz während des Schließvorgangs = QM VDV-Schrift-161-2 Kap. 3.4.4	ASIL A(D)	I (im Betriebshof)	I (außerhalb Betriebshof)	A	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-17 Anschlußbeziehungen aktualisieren und darstellen	ASIL A	n/a	V	A	V	A
■ Die ÖV-Leitstelle ist verantwortlich für die Fahrplanaktualisierung mit Synchronisation der betroffenen Zu- und Abbringer. ■ Das FGI der ÖV-Leitstelle ist verantwortlich für das Informieren der betroffenen Fahrgäste.	QM (A)	n/a	V	A	I	A
Randbedingung: Das Fahrzeug befindet sich außerhalb des Betriebshofes (Regelbetrieb) an der Haltestelle / Halteposition oder auf dem Betriebshof an einer Servicestation im Stillstand (v = 0km/h). ■ Die AD-Leitstelle ist verantwortlich für die Überwachung der autonomen Fahrt inklusive Umsetzung der ► Überwachung der automatisierten Türschließung über UC-06 Türkontrolle. ► Verhinderung der Anfahrt mit geöffneten Türen = ASIL-A, VDV-Schrift-161-2 Kap. 3.4.1 ► Türschließwarnung (optisch/akustisch) = QM VDV-Schrift-161-2 Kap. 3.4.3 ► Einklemmschutz während des Schließvorgangs = QM VDV-Schrift-161-2 Kap. 3.4.4	ASIL A	n/a	I	A (informative Meldungen)	V	A
UC-18 Zielbeschilderung außen und innen ändern	QM	n/a	V	A	n/a	n/a
■ Die ÖV-Leitstelle ist verantwortlich für die Fahrgastinformation (FGI), dazu zählt auch das korrekte Anzeigen gegenüber dem Fahrgast. *Hinweis:* *Die Verantwortung der Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung) obliegt der ÖV-Leitstelle, jedoch werden diese Daten nicht über diesen Anwendungsfall (UseCase) initiiert, welche das Setzen der Anzeiger über den ÖV-Bordrechner eigenständig und unabhängig umsetzt.*	QM	n/a	V	A	n/a	n/a
UC-19 Liniennummer ändern	QM	n/a	V	A	n/a	n/a
■ Die ÖV-Leitstelle ist verantwortlich für die Fahrgastinformation (FGI), dazu zählt auch das korrekte Anzeigen gegenüber dem Fahrgast. *Hinweis:* *Die Verantwortung der Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung) obliegt der ÖV-Leitstelle, jedoch werden diese Daten nicht über diesen Anwendungsfall (UseCase) initiiert, welcher das Setzen der Anzeiger über den ÖV-Bordrechner eigenständig und unabhängig umsetzt.*	QM	n/a	V	A	n/a	n/a
UC-20 Fahrgäste akustisch informieren	QM	n/a	V	A	n/a	n/a
■ Die ÖV-Leitstelle ist verantwortlich für die Fahrgastinformation (FGI), dazu zählt auch das korrekte Anzeigen gegenüber dem Fahrgast. *Hinweis:* *Die Verantwortung der Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung) obliegt der ÖV-Leitstelle, jedoch werden diese Daten nicht über diesen Anwendungsfall (UseCase) initiiert, welcher das Setzen der Anzeiger über den ÖV-Bordrechner eigenständig und unabhängig umsetzt.*	QM	n/a	V	A	n/a	n/a
UC-21 Fahrgäste textuell informieren (Tickertext)	QM	n/a	V	A	n/a	n/a
■ Die ÖV-Leitstelle ist verantwortlich für die Fahrgastinformation (FGI), dazu zählt auch das korrekte Anzeigen gegenüber dem Fahrgast. *Hinweis:* *Die Verantwortung der Korrektheit und Vollständigkeit, sowie Nutzbarkeit der Fahrplandaten (Datenlieferung) obliegt der ÖV-Leitstelle, jedoch werden diese Daten nicht über diesen Anwendungsfall (UseCase) initiiert, welcher das Setzen der Anzeiger über den ÖV-Bordrechner eigenständig und unabhängig umsetzt.*	QM	n/a	V	A	n/a	n/a

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-22 Problem mit Fahrgast (störendes Verhalten)	**ASIL-C** Abhängig vom Ereignis	n/a	V (anteilig)	A	V (anteilig)	A
■ Die ÖV-Leitstelle ist verantwortlich für die Problemlösung (Einleitung geeigneter Maßnahmen), sofern der beschwerdeführende Fahrgast den Knopf „Kommunikation“ zum Auslösen der Beschwerde verwendet hat. Hinweis: Die ÖV-Leitstelle kann das FG-Notfallmanagement und/oder die Technische Aufsicht der AD-Leitstelle mit einbinden, ggf. die Zuständigkeit / Verantwortung übergeben.	Abhängig vom Ereignis QM (Kommu-nikation) **ASIL-C** Notfall (Fehlbe-dienung)	n/a	V	A	ggf. A	A
■ Die AD-Leitstelle ist verantwortlich für die Problemlösung (Einleitung geeigneter Maßnahmen), sofern der beschwerdeführende Fahrgast den Knopf „Notruf“ / „Nothalt“ zum Auslösen der Beschwerde verwendet hat. Hinweis: Die AD-Leitstelle kann das FG-Notfallmanagement und/oder die ÖV-Leitstelle mit einbinden, ggf. die Zuständigkeit / Verantwortung übergeben.	Abhängig vom Ereignis **ASIL-C** ggf. geringer	n/a	ggf. A	A	V	A
UC-23 Kommunikation mit Fahrgästen bei außergewöhnlichen Ereignissen	**ASIL-C** Abhängig vom Ereignis	n/a	I	A	V	A
■ Die ÖV-Leitstelle ist verantwortlich für die Problemlösung (Einleitung geeigneter Maßnahmen), sofern der ereignismeldende Fahrgast den Knopf „Kommunikation“ zur Meldung des Ereignisses verwendet hat. Hinweis: Die ÖV-Leitstelle kann das FG-Notfallmanagement und/oder die Technische Aufsicht der AD-Leitstelle mit einbinden, ggf. die Zuständigkeit / Verantwortung übergeben.	Abhängig vom Ereignis QM (Kommu-nikation) **ASIL-C** Notfall (Fehlbe-dienung)	n/a	V	A	ggf. A	A
■ Die AD-Leitstelle ist verantwortlich für die Problemlösung (Einleitung geeigneter Maßnahmen), sofern der ereignismeldende Fahrgast den Knopf „Notruf“ / „Nothalt“ zum Auslösen der Beschwerde verwendet hat. Hinweis: Die AD-Leitstelle kann das FG-Notfallmanagement und/oder die ÖV-Leitstelle mit einbinden, ggf. die Zuständigkeit / Verantwortung übergeben.	Abhängig vom Ereignis **ASIL-C** ggf. geringer	n/a	ggf. A	A	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-24 Fundsachen und Sauberkeit im Fahrzeug	QM	n/a (App)	V	A	A (Optional)	A (optional)
■ Die ÖV-Leitstelle ist verantwortlich für die Problemlösung (Einleitung geeigneter Maßnahmen) Hinweis: Im betrachteten Fall erfolgt die Meldung von Fundsachen oder eine Beschwerde wegen Verschmutzung über die spezifische App des ÖPNV-Unternehmens.	QM	n/a (App)	V	A	n/a	n/a
■ Die AD-Leitstelle kann im Bedarfsfall von der ÖV-Leitstelle hinzugezogen werden, um Kamerabilder aus dem Inneren des Fahrzeuges zur Situationsanalyse zu erhalten. *Hinweis:* *Die Behandlung von Fundsachen und Reinigung erfolgt im BHMS mit UC-07 Fahrzeug abrüsten.* *Die Behandlung von Fundsachen und Reinigung über die Kommunikation des Fahrzeuges erfolgt mit UC-23 Kommunikation mit Fahrgästen bei außergewöhnlichen Ereignissen.* *UC-24 beschreibt die Behandlung von Fundsachen und Reinigung via App sowie den Erweiterten Ablauf von UC-23, wenn die ÖV-Leitstelle Kamerabilder zur Verifikation der Situation benötigt.* *Hinweis:* *Die Kamera-Funktion dient in anderen UCs zur Absicherung, Beweissicherung und zum Nachweis, weshalb diese eine ASIL-C Funktion ist, welche für diesen Anwendungsfall nicht benötigt wird → hier QM (jedoch höher abgesichert). Eine höhere Absicherung als gefordert ist zulässig (und technisch auch nicht anders umsetzbar, weil sich die Parameter Hardware Failure (PMHF) ≤ 10 FIT (OP Safe) der Hardware nicht je nach Anwendung ändern können).*	QM	n/a (App)	V	n/a	A (Optional)	A (Optional)
UC-25 Waschvorgang	ASIL C	V	n/a	A	V	A
■ Das BHMS ist verantwortlich für die Einsatzbereitschaft der Fahrzeuge, dazu zählt insbesondere die korrekte und ordnungsgemäße Umsetzung der Fahrzeugpflege (Service & Wartung). ■ Das BHMS ist verantwortlich für die Überwachung der ordnungsgemäßen Reinigung der Sensorik und der Überprüfung auf deren einwandfreie Funktionalität unter Berücksichtigung von AFGBV Anlage 1 Teil 1 Abschnitt 9 Alterung und Abnutzung des Systems. Hinweis: ISO-26262-03:2018 Clause 7.4.3.1 Sicherheitsanforderungen müssen dem Automotive Safety Integrity Level (ASIL) der Funktion und dem zugehörigen Sicherheitsziel entsprechen. Der Waschvorgang reinigt die Sensorik, eine nicht ordnungsgemäße Reinigung der Sensorik kann dazu führen, daß Hüllboxen von Gegenständen oder Personen im Umfeld des Kraftfahrzeugs nicht korrekt erfaßt werden, welches einen Unfall auslösen kann.	ASIL C	V	n/a	A	I	A
■ Die AD-Leitstelle ist verantwortlich für die Überwachung der autonomen Fahrt inklusive Umsetzung der ▶ Überwachung der automatisierten Türschließung über UC-06 Türkontrolle. ▶ Festhalten der Türen in geschlossener Stellung während der Fahrt = ASIL-B VDV-Schrift-161-2 Kap. 3.4.2	ASIL B(C)	I	n/a	A	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-26 Lademanagement	ASIL A	V	V	A	V	A
■ Das BHMS ist verantwortlich für die Fahrzeugpflege (Service & Wartung) inklusive der Einsatzbereitschaft der Fahrzeuge.	ASIL A	V	I	A	I	A
■ Die ÖV-Leitstelle ist verantwortlich für Störfälle (potentielle Liegenbleiber) außerhalb des BHMS zur Aufrechterhaltung des Fahrplanes.	QM (A)	A	V	A	I	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. Hinweis: Die Fahrfunktion ist eine ASIL-C Funktion ist, welches für diesen Anwendungsfall nicht benötigt wird. Eine höhere Absicherung als gefordert ist zulässig (und technisch auch nicht anders umsetzbar, weil sich die Parameter Hardware Failure (PMHF) ≤ 10 FIT (OP Safe) der Hardware nicht je nach Anwendung ändern können).	ASIL C(A)	I	I	A (informative Meldungen)	V	A
UC-27 Ersatzfahrzeug bereitstellen	QM	V	V	A	V	A
■ Das BHMS ist verantwortlich für die Fahrzeugpflege (Service & Wartung) inklusive der Einsatzbereitschaft der (Ersatz-)Fahrzeuge.	QM	V	I	A	I	A
■ Die ÖV-Leitstelle ist verantwortlich für Störfälle (potentielle Liegenbleiber) außerhalb des BHMS zur Aufrechterhaltung des Fahrplanes.	QM	A	V	A	I	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. Hinweis: Die Fahrfunktion ist eine ASIL-C Funktion ist, welches für diesen Anwendungsfall nicht benötigt wird. Eine höhere Absicherung als gefordert ist zulässig (und technisch auch nicht anders umsetzbar, weil sich die Parameter Hardware Failure (PMHF) ≤ 10 FIT (OP Safe) der Hardware nicht je nach Anwendung ändern können). Hinweis: Die Türkontrolle ist eine ASIL-A Funktion.	QM (C)	I	I	A	V	A
UC-28 Eingriffsnotwendigkeit Technische Aufsicht	ASIL C	I	I	I	V	A
■ Sofern bei der (erweiterten) Abfahrkontrolle auf dem Betriebshof eine Störung auftreten sollte, welche zu einem Eingriff der Technischen Aufsicht (TA) führt, dann sind die daraus resultierenden Reparatur- und Instandsetzungsarbeiten vom BHMS zu planen und durchzuführen. *Hinweis:* *Das BHMS ist verantwortlich für die Fahrzeugpflege (Service & Wartung) inklusive der Einsatzbereitschaft der (Ersatz-)Fahrzeuge.*	n/a (Tätigkeit ist nicht Teil des UC)	I	n/a	I	V	A
■ Sofern im Fahrgastbetrieb eine Störung auftritt, welche eine Fortsetzung der Fahrt verhindert, dann sind dispositive Maßnahmen über andere Use Cases einzuleiten. *Hinweis:* *Die ÖV-Leitstelle ist verantwortlich für Störfälle (potentielle Liegenbleiber) außerhalb des BHMS zur Aufrechterhaltung des Fahrplanes.*	n/a (Tätigkeit ist nicht Teil des UC)	n/a	I	I	V	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig.	ASIL C	n/a	n/a	I	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-29 Temporäre Sensorbeeinträchtigung	ASIL C	n/a	n/a	n/a	V	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig.	ASIL C	n/a	n/a	n/a	V	A
UC-30 Fehler in der Selbstpositionierung	ASIL C	n/a	n/a	n/a	V	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig.	ASIL C	n/a	n/a	n/a	V	A
UC-31 Entscheidungshilfe (Fahrtfortsetzung)	ASIL C	I	I	I	V	A
■ Sofern bei der (erweiterten) Abfahrkontrolle auf dem Betriebshof eine Störung auftreten sollte, welche zu einem Eingriff der Technischen Aufsicht (TA) führt, dann sind die daraus resultierenden Reparatur- und Instandsetzungsarbeiten vom BHMS zu planen und durchzuführen. *Hinweis:* *Das BHMS ist verantwortlich für die Fahrzeugpflege (Service & Wartung) inklusive der Einsatzbereitschaft der (Ersatz-)Fahrzeuge.*	n/a (Tätigkeit ist nicht Teil des UC)	I	n/a	I	V	A
■ Sofern im Fahrgastbetrieb eine Störung auftritt, welche eine Fortsetzung der Fahrt verhindert, sind dispositive Maßnahmen über andere Use Cases einzuleiten. *Hinweis:* *Die ÖV-Leitstelle ist verantwortlich für Störfälle (potentielle Liegenbleiber) außerhalb des BHMS zur Aufrechterhaltung des Fahrplanes.*	n/a (Tätigkeit ist nicht Teil des UC)	n/a	I	I	V	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig.	ASIL C	n/a	n/a	I	V	A
UC-32 Detektion von Trajektorien Abweichung	ASIL C	n/a	n/a	n/a	V	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig.	ASIL C	n/a	n/a	n/a	V	A
UC-33 Interpretation des fahrzeuginternen Systemzustandes	ASIL C	n/a	n/a	n/a	V	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig.	ASIL C	n/a	n/a	n/a	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-34 Interpretation des Gesamtsystemzustandes zwischen Infrastruktur/Leitstelle und Fahrzeug	ASIL C	n/a	n/a	n/a	V	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. Randbedingung: Dazu ist es essentiell, daß nur die relevanten Informationen vollständig mittels der Benutzeroberfläche / Graphical User Interface (GUI) ≙ Anwendersoftware ≙ App angezeigt werden. (Vollständigkeit, Übersichtlichkeit, Effizienz)	ASIL C	n/a	n/a	n/a	V	A
UC-35 Detektion von Abweichungen in Sensordaten zwischen Fahrzeug und Infrastruktur	ASIL C	n/a	n/a	n/a	V	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. Randbedingung: Das Betriebshandbuch der AD-Leitstelle des ÖPNV-Unternehmens liefert detaillierte Vorgaben um den sicheren Betrieb des Kraftfahrzeugs zu gewährleisten, welches die Technische Aufsicht (TA) bei ihrer Arbeit unterstützt, die richtigen Reaktionen auf Ereignisse / Störmeldungen durch vordefinierte geeignete (erprobte und etablierte) Maßnahmen einzuleiten.	ASIL C	n/a	n/a	n/a	V	A
UC-36 Detektion und Rückmeldung übertreten der Operativen Design Domain (Kartierung, Wetter, Geschwindigkeit)	ASIL C	n/a	n/a	n/a	V	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. *Hinweis:* *Dieser UseCase beschreibt einen Watchdog, der lediglich die erkannte Abweichung priorisiert meldet.*	ASIL C	n/a	n/a	n/a	V	A
UC-37 Bereitstellen von Verhaltensinformationen an AD-Leitstelle zum späteren System Lernen	ASIL C	n/a	n/a	n/a	V	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. *Hinweis:* *Dieser UseCase beschreibt einen Watchdog, der lediglich die erkannte Abweichung priorisiert meldet.*	ASIL C	n/a	n/a	n/a	V	A
UC-38 Lernen von Verhalten im Störfall aus früheren Fahrsituationen, die von der AD-Leitstelle begleitet wurden	ASIL C	n/a	n/a	n/a	V	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. *Hinweis:* *Dieser UseCase beschreibt einen Watchdog, der lediglich die erkannte Abweichung priorisiert meldet.*	ASIL C	n/a	n/a	n/a	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-39 Ausgestaltung der AD-Leitstelle für die Technische Aufsicht	ASIL C	n/a	n/a	n/a	V	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. *Hinweis:* *Dieser UseCase beschreibt einen Watchdog, der lediglich die erkannte Abweichung priorisiert meldet.*	ASIL C	n/a	n/a	n/a	V	A
UC-40 Nothalt	ASIL A	I/A	I/A	A	V	A
■ Das BHMS hat keine Verantwortung / Zuständigkeit, aber die Möglichkeit der Rückfrage, sofern sich das Fahrzeug auf dem Betriebshof befindet.	QM (A)	I/A	n/a	A	V	A
■ Die ÖV-Leitstelle hat keine Verantwortung / Zuständigkeit, aber die Möglichkeit der Rückfrage, sofern sich das Fahrzeug außerhalb vom Betriebshof befindet. Außerdem kann der ÖV-Bordrechner automatisierte Bandansagen durchführen, sobald ein Knopf (Kommunikation / Notruf / Nothalt) betätigt wurde.	QM (A)	n/a	I/A	A	V	A
■ Die AD-Leitstelle ist verantwortlich für die Notfall-Betreuung, welche den Busfahrer als Ersthelfer im autonomen Betrieb ersetzt. Die Technische Aufsicht (TA) der AD-Leitstelle entscheidet ob eine Einbindung des Fahrgast-Notfall-Management sinnvoll und erforderlich ist, leitet die erforderlichen Maßnahmen (inklusive ggf. Einsatz von Rettungs- und Bergungskräften) zur Beendigung des Notfalls ein und dokumentiert dieses vorschriftsmäßig, gemäß AFGBV. ■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. Die Leichtigkeit des Straßenverkehrs darf zu keiner Zeit unangemessen beeinträchtigt werden, d.h. das Fahrzeug ist gemäß AFGBV § 14 Anforderungen an die Technische Aufsicht (TA) Absatz 3 unverzüglich aus dem Straßenraum zu entfernen. *Hinweis:* *Ein Notfall im Fahrzeug hat keinen Einfluß auf die Anforderungen der Sicherheitsrelevanz auf die UC-04 Fahrgastfahrt (ASIL-C) selbst.* *Hinweis: Es gibt im autonomen Fahrbetrieb keinen Busfahrer, insofern kann dieser auch keinem medizinischen Notfall erliegen.*	ASIL A	I/A	I/A	A	V	A
UC-41 Fahrzeug dauerhaft unerreichbar	ASIL C	V	V	A	V	A
■ Das BHMS ist verantwortlich für die Fahrzeugpflege (Service & Wartung) inklusive der Einsatzbereitschaft inklusive Behebung von Defekten und ggf. Bergung von Liegenbleiber sowie Zuführung zur Instandsetzung.	QM (C)	V	n/a	A	A	A
■ Die ÖV-Leitstelle ist verantwortlich für Störfälle (potentielle Liegenbleiber) außerhalb des BHMS zur Aufrechterhaltung des Fahrplanes.	QM (C)	n/a	V	A	A	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. Die Leichtigkeit des Straßenverkehrs darf zu keiner Zeit unangemessen beeinträchtigt werden, d.h. das Fahrzeug ist gemäß AFGBV 14 Anforderungen an die Technische Aufsicht (TA) Absatz 3 unverzüglich aus dem Straßenraum zu entfernen.	ASIL C	I (BHMS)	I (Fahrgast-betrieb)	A (informative Meldungen)	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-42 Parameter für LSA Beeinflussung setzen	QM (n/a)	n/a	V	A	I	A
■ Die ÖV-Leitstelle ist verantwortlich für die Überwachung des Fahrweges des Fahrzeuges / Platoon gemäß den Fahrplandaten, sofern notwendig / sinnvoll das Ergreifen von Maßnahmen, z.B. Lichtsignalanlagenbeeinflussung (LSA) um die Pünktlichkeit wiederherzustellen, das Informieren der mitreisenden und potentiellen Fahrgäste über Einhaltung / Abweichung der Pünktlichkeit, sowie das Unterstützen bei der Sicherstellung des zeitgerechten Erreichens bei Anschlüssen der Fahrt. *Hinweis:* *Dieser UseCase hat keinen direkten Einfluß auf die Fahrt (UC-03 / UC-04 / UC-44).* *Es wird die Lichtsignalanlage z.B. Ampel beeinflußt, welche indirekt über die Sensorik erfaßt und angewendet wird. Das AD Bordsystem muß plötzlich auftretendes unerwartetes Ereignis, (z.B. veränderte Signale einer Ampelanlage) erkennen und die Anpassung des Fahrpfades und der Parameter (z.B. Geschwindigkeit / Halt) im Rahmen des Betriebsbereiches (z.B. Stadtfahrt, Überlandfahrt) der dynamischen Fahraufgabe anpassen, wobei statistische Handlungsoptionen (aus der Vergangenheit), KI gestützt, in den Auswahlprozeß (Lernen aus der Vergangenheit) der verfügbaren Optionsmöglichkeiten mit berücksichtigt werden können.*	QM (n/a)	n/a	V	A	I	A
UC-43 Parken	QM	V	V	A	n/a	n/a
■ Die ÖV-Leitstelle ist verantwortlich für die Planung und Umsetzung der Fahrpläne. Dazu gehört auch das Ergreifen notwendiger Maßnahmen zur Wiederherstellung der Fahrplaneinhaltung (Pünktlichkeit) im regulären Fahrbetrieb (außerhalb des Betriebshofes) und das Parken, wenn in bekannten Zeiten nur mit einem schwachen Fahrgastaufkommen zu rechnen ist.	QM	V	n/a	A	n/a	n/a
■ Das BHMS ist verantwortlich für die Fahrzeugpflege (Service & Wartung) inklusive der Sicherstellung der Einsatzbereitschaft mittels Instandsetzung. Sofern die Fahrzeugwarteschlange der einzelnen Stationen voll sein sollte, dann wird das Fahrzeug zwischengeparkt, jedoch werden auf dem Betriebshof weder Außen- noch Innenanzeiger gesetzt, auch ist es nicht notwendig zu verifizieren, daß sich keine Person im Fahrzeug aufhält.	QM	n/a	V	n/a	n/a	n/a
UC-44 Fahrt im Depot	ASIL C	V	n/a	A	V	A
■ Das BHMS ist verantwortlich für die Fahrzeugpflege (Service & Wartung) inklusive der Einsatzbereitschaft der Fahrzeuge. Dazu zählt auch die (erweiterte) Abfahrkontrolle.	QM (C)	V	n/a	A	A	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. ■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung der erweiterten Abfahrkontrolle (Probefahrt) mit Verifikation des Fahrzeugzustandes sowie ggf. Abnahme der Instandsetzung.	ASIL C	A	I	A (informative Meldungen)	V	A

UC	Sicherheitsrelevanz	BHMS	ÖV-Leitstelle (Disponent)	ÖV-Bordrechner	AD-Leitstelle (Technische Aufsicht)	AD-Bordsystem
UC-45 MissionCtrl	QM	I (BHMS)	I (Fahrgast-betrieb)	A	V	A
■ Die AD-Leitstelle ist verantwortlich für die Fahrzeugüberwachung inklusive der Steuerung des Fahrzeuges (ADO) über die externe Schnittstelle, sofern notwendig. ■ Das AD-Bordsystem ist für die Umschaltung der Missionen zuständig. (Wechsel zwischen UC-03, UC-04 und UC-44).	QM	I (BHMS)	I (Fahrgast-betrieb)	A	V	A

Legende:
V = Verantwortung
A = Ausführung
I = Informativ eingebunden

3.3.2 Das Autonomous Drivable Object (ADO)

3.3.2.1 Systembild

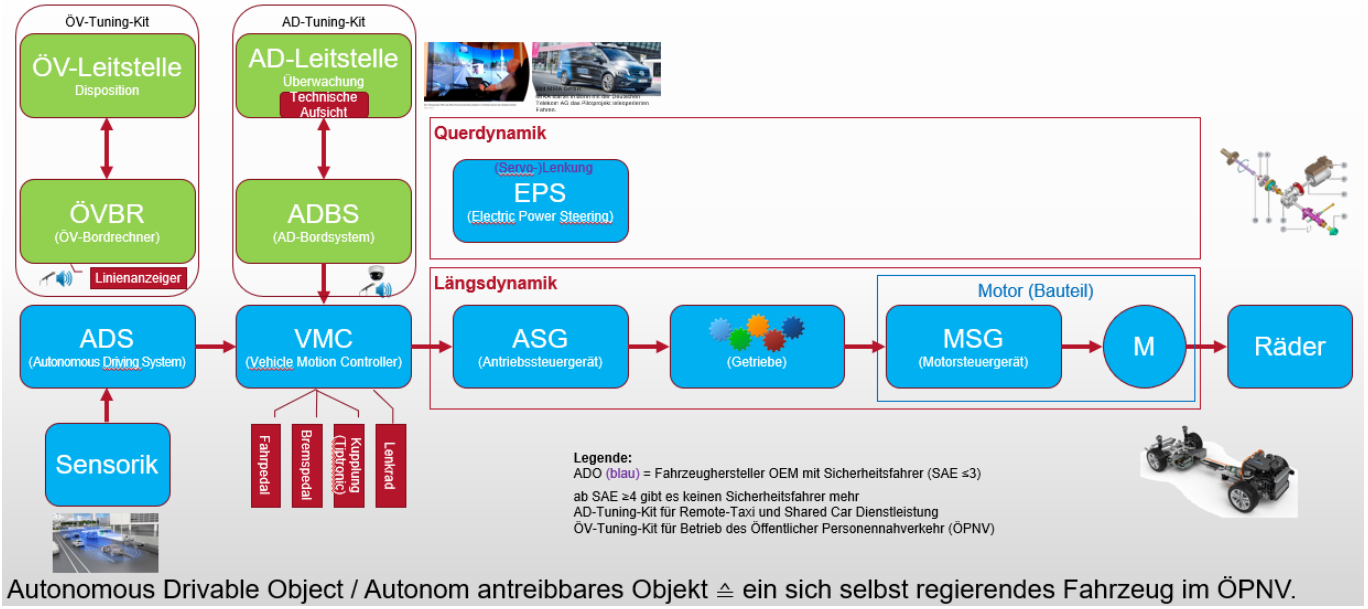


Abbildung 8 Autonomous Drivable Object (ADO) mit optionalen Tuning-Kits

Hinweis (Bildquellenangabe lesbar):
Bild MIRA GmbH (Bild mit Remote-Fahrer):
Der Teleoperator fährt das Mira-Personenshuttle praktisch in Echtzeit durch den Straßenverkehr.
Bild MIRA GmbH (Bild mit Van):
MIRA startet in Bonn mit der Deutschen Telekom AG das Pilotprojekt teleoperierten Fahren.
Quelle:
https://www.automobil-industrie.vogel.de/teleoperator-automatisiertes-fahren-a-c575959fc23164776dc6d21124402e96/?cmp=nl-99&uuid=185eab07a68493792fc68fd5206d6b79

https://mira-mobility.com/mira-und-telekom-testen-ferngesteuerte-shuttles-in-bonn.

Das AD-Kit beinhaltet die fahrzeugspezifische Anpassung der bereitgestellten Interfaces vom Fahrzeughersteller (OEM) zu den vorhandenen Interfaces der Systeme des ÖPNV-Unternehmens, wobei der ÖV-Bordrechner als vorhandenes Interface genutzt werden kann.

3.3.2.2 Regelkreis der Systems Theoretic Process Analysis (STPA)

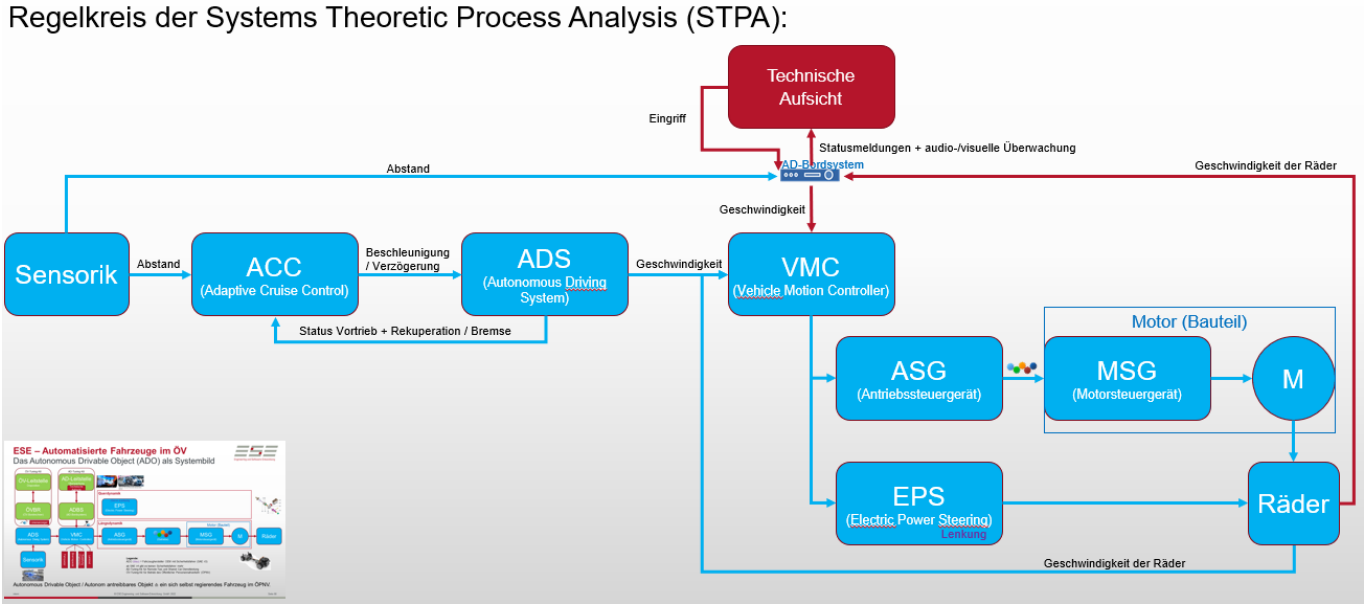


Abbildung 9 Regelkreis von einem autonomen Fahrzeug (ADO) mittels Systems Theoretic Process Analysis (STPA)

3.3.3 Sicherheitsziele / Safety Goals (SG)

Die globale Sicherheitsziele auf der obersten Ebene lauten:

- **SG1 (ASIL-D)**
  - Sicherstellung, daß das Autonomous Drivable Object (ADO) keine negativ auswirkende kinetische Energie auf andere Verkehrsteilnehmer (VRU) ausüben kann.
  - *Verhindern, daß das ADO schädigende kinetische Energie an andere Verkehrsteilnehmer (VRU) transferiert, z.B. durch eine Kollision*.
- **SG2 (ASIL-D)**
  - Sicherstellung, daß auf das ADO keine sich negativ auswirkende kinetische Energie durch andere Verkehrsteilnehmer ausgeübt wird.
  - *Verhindern, daß auf das ADO schädigende kinetische Energie durch andere Verkehrsteilnehmer ausgeübt werden kann, z.B. durch eine Kollision*.
- **SG3 (ASIL-C)**
  - Sicherstellung, daß das ADO die Umgebung wahrnimmt bzw. wahrnehmen kann
  - *Verhindern, daß das ADO nicht die Umgebung wahrnehmen (einsehen) kann*.
- **SG4 (ASIL-A)**
  - Sicherstellung, daß das ADO von der Umgebung wahrgenommen (gesehen) wird.
  - *Verhindern, daß das ADO nicht von der Umgebung wahrgenommen (gesehen) werden kann*.

Hinweis:
Die Sicherheitsziele sind harmonisch und kumulativ zu einander, jedoch hat SG1 Vorrang vor SG2
Selbst auf das vorausfahrende Objekt aufzufahren um den Zusammenstoß mit dem nachfolgenden Objekt zu verhindern macht keinen Sinn.

Hinweis:
Der manuelle (remote) Fahrbetrieb muß den autonomen / automatisierten Fahrbetrieb abschalten und übersteuern können, dabei können jedoch Schutzmaßnahmen z.B. Umrampen oder Fahrerassistenzsysteme (z.B. EPS), welche den (Remote-)Fahrer unterstützen aktiviert bleiben.

Diese Sicherheitsziele sind hierarchisch strukturiert abzuholen.
→ Anforderungen an Sicherheitsanforderungen gemäß ISO-26262:2018.

3.3.4 Sicherheitsmaßnahmen

Das Funktionale Sicherheitskonzept (FSK) des Fahrzeugherstellers (OEM) kann vom Halter Sicherheits-Maßnahmen zum Betrieb einfordern. Dazu zählt insbesondere der (Remote-)Sicherheitsfahrer bei SAE $\leqslant$ 3 bzw. die Überwachung, speziell der Fahrt ($W_{kin} > 0$), durch eine qualifizierte Technische Aufsicht (TA) bei SAE $\geqslant$ 4.

Umgekehrt kann ein ÖPNV-Unternehmen auch Anforderungen an die Vergabe von Bestelllungen knüpfen.

3.3.4.1 Kategorien der Sicherheitsmaßnahmen

SiMF = Sicherheitsmaßnahme Funktional

SiMT = Sicherheitsmaßnahme Technik

SiMQ = Sicherheitsmaßnahme Qualitätssicherung (Prozeßabsicherung, Monitoring / Überwachung)

SiMH = Sicherheitsmaßnahme Herstellung

SiMW = Sicherheitsmaßnahme Wartung und Service

SiMSiF = Sicherheitsmaßnahme Sicherheitsfahrer

3.3.4.1.1 Sicherheitsmaßnahme Funktional (SiMF)

Die Funktionalen Sicherheitsmaßnahmen hängen von der hierarchischen Struktur ab, deshalb hier nur beispielhaft aufgeführt.

- Der Vehicle Motion Controller (VMC) des Fahrzeugherstellers (OEM) muß sicherstellen, daß die (maximale mögliche) Beschleunigung (Längsführung) auf ein vom Remote-Sicherheitsfahrer der Technischen Aufsicht (TA) beherrschbares Maß, sowohl im autonomen als auch im manuellen Fahrbetrieb, begrenzt wird.
- Der Vehicle Motion Controller (VMC) des Fahrzeugherstellers (OEM) muß sicherstellen, daß die (maximale mögliche) Verzögerung (Längsführung) auf ein vom Remote-Sicherheitsfahrer der Technischen Aufsicht (TA) sowie dem nachfolgenden Verkehr, beherrschbares Maß, sowohl im autonomen als auch im manuellen Fahrbetrieb, begrenzt wird.

- Der Vehicle Motion Controller (VMC) des Fahrzeugherstellers (OEM) muß die Betätigung des Fahr- bzw. Bremspedals durch den Remote-Sicherheitsfahrer der Technischen Aufsicht (TA) im autonomen Fahrbetrieb als Eingriff / Eingriffsnotwendigkeit erkennen und daraufhin den autonomen / automatisierten Fahrmodus beenden und in den manuellen (remote) Fahrbetrieb wechseln.

3.3.4.1.2 Sicherheitsmaßnahme Technik (SiMT)

Die Sicherheitsmaßnahmen Technik hängen von der hierarchischen Struktur der (verteilten) Absicherung ab, deshalb hier nur Beispielhaft aufgeführt.

- Die Betätigung des Bremspedals muß vorrangig vor dem Fahrpedal umgesetzt werden und dieses sicher übersteuern. (Die Bremsleistung muß auch bei einem zeitgleichen, maximalen Beschleunigungswert das ADO beherrschbar in kurzer Zeit zum Stillstand bringen).
- Der VMC muß bei der sicheren Betätigung des Bremspedals (ab Schwellwert) das Antriebsmoment abschalten. (Bauteilschutz)
- Der VMC muß bei der sicheren Betätigung des Bremspedals (ab Schwellwert) das autonome Verzögerungsmoment abschalten. (Beherrschbarkeit)
- Der VMC muß bei der sicheren Betätigung des Fahrpedals (ab Schwellwert) das autonome Antriebsmoment abschalten. (Bauteilschutz)
- Der VMC muß bei der sicheren Betätigung des Fahrpedals (ab Schwellwert) das autonome Verzögerungsmoment abschalten. (Bauteilschutz)
- Die Quantitative (der korrekte Wert der Amplitude bzw. Drehwinkels des Durchtretens) muß (von beiden Pedalen) an das Antriebsteuergerät (ASG) bzw. den Triebstrangkoordinator (TSK) = Längsführung (Vortrieb) abgesichert übermittelt werden.
  Abgesichert = E2E, d.h. mit Dämpfung (Cap), Unterstützungsleistung (Botton), Zeitersatzwert, Ersatzwert für sicheren Bereich.
- Der VMC muß beim Fahrtrichtungswechsel von der einen Fahrtrichtung in die andere Umrampen um die Beherrschbarkeit für den Remote-Sicherheitsfahrer / die Technische Aufsicht (TA), die Insassen und den umgebenden Verkehr zu gewährleisten, sowie das Bauteil gegen unnötige Belastung schonen.

Randbedingung:
Um die Potentiale von automatisierten Fahrzeugen im ÖPNV-Einsatz flächendeckend auszuschöpfen, muss ein systemischer Ansatz gefunden werden, der die automatisierten und autonomen Fahrzeuge im ÖV auf allen Ebenen organisatorisch und technisch standardisiert in die betrieblichen Prozesse und dazu in die bestehenden IT-Systemlandschaften integriert. Der ÖV steht einer Reihe von Anbietern gegenüber, die jedoch nur über herstellerspezifische und damit proprietäre Schnittstellen eingebunden werden können. Die geplante Standardisierung ist daher wesentlich für einen diskriminierungsfreien Marktzugang der Hersteller.

Deshalb wurde im Projekt ÖV-LeitmotiF-KI die Steuerungsschnittstelle UM0.19.8 Control (S19.A = CAN) unabhängig von spezifischen Eigenschaften (Fahr- und Bremspedalwinkel bzw. Lenkwinkelwerten) des Fahrzeuges spezifiziert. Stattdessen werden physikalische und mathematische Grundgrößen angewendet,

- Bogenverlauf der Straßenführung statt Lenkwinkel mit
- beschleunigter Geschwindigkeit der Lenkbewegung und
- digitaler Geschwindigkeitswert statt Fahr- und Bremspedalwert.
  Hinweis: Da dieses ein kumulierter Wert ist, können Probleme der gleichzeitigen Fahr- und Bremspedalbetätigung gar nicht auftreten, folglich ist ein Übersteuern auch nicht notwendig.

Systemgrenze = kammscher Kreis.

3.3.4.1.3 Sicherheitsmaßnahme Qualitätssicherung (SiMQ)

Die Sicherheitsmaßnahmen der Qualitätssicherung (Verfahrensanweisungen und Arbeitsvorschriften) hängen neben der hierarchischen Struktur der (verteilten) Absicherung der Systeme zusätzlich auch noch von den unternehmensspezifischen Prozessen und deren Absicherung (Befugnissen)sowie den Mechanismen der Überwachung auf Einhaltung ab. Deshalb hier nur Beispielhaft aufgeführt.

- Arbeitsvorschrift bzgl. Arbeiten an Hochvoltanlagen.
- Reparatur- und Wartungsinformationen für das Kraftfahrzeug vom Fahrzeughersteller (OEM).

3.3.4.1.4 Sicherheitsmaßnahme Herstellung (SiMH)

Existieren nicht im Rahmen des Projektes ÖV-LeitmotiF-KI.

- Die Herstellung des Fahrzeuges obliegt dem Fahrzeughersteller (OEM).
- Die Tuning-Kits (Erweiterung der Fahrzeugausstattung) unterliegen den Hersteller der
  - AD-Systeme → Ferngesteuertes fahren über die Technische Aufsicht (TA) der AD-Leitstelle.
  - ÖV-Bordsysteme mit Außen- und Innenanzeiger → Zusatzausrüstung für den ÖPNV-Betrieb.

- Die Herstellung der Leitstände insbesondere der Software obliegt den Entwicklungsrichtlinien der Hersteller. Diese werden in der Regel an die Bedürfnisse (Anforderungen) des ÖPNV-Unternehmens kundenspezifisch angepaßt.

Im Rahmen des Projektes ÖV-LeitmotiF-KI kann zum Zwecke der Darstellung der Umsetzung und des Feldtests eine entsprechende Simulation zum Einsatz kommen.

3.3.4.1.5 Sicherheitsmaßnahme Wartung (SiMW)

Die funktionalen Sicherheitsmaßnahmen hängen von der hierarchischen Struktur ab, deshalb hier nur beispielhaft aufgeführt.

- Arbeitsvorschrift bzgl. der Fahrzeugpflege (Service & Wartung) des BHMS.
- Schaugläser im Motor, sofern sinnvoll für Service und Wartung ← Fahrzeughersteller (OEM)

3.3.4.1.6 Sicherheitsmaßnahme Sicherheitsfahrer (SiMSiF)

Die funktionalen Sicherheitsmaßnahmen hängen von der hierarchischen Struktur ab, deshalb hier nur beispielhaft aufgeführt.

- Sicherheitstraining für Remote-Fahrer zur ordnungsgemäßen Bewältigung der Anforderungen der Personenbeförderung im öffentlichen Straßenverkehr zur Umsetzung der manuellen Fahraufgabe der Technischen Aufsicht (TA).