Funktionale Sicherheit und Cybersecurity

nach ISO 26262 und ISO/SAE 21434

2 Grundlagen und Schlüsseltechnologien für autonomes Fahren

Sicherheit bedeutet im Allgemeinen nicht, dass kein Schaden entstehen kann, sondern, dass das Risiko akzeptabel ist.

(Dr. Rasmus Adler, Fraunhofer IESE, über die Rolle von KI bei der Fahrsicherheit)

Die zunehmende Automatisierung und Vernetzung moderner Straßenfahrzeuge stellen neue und komplexe Anforderungen an ihre Sicherheit. Um autonome und intelligente Fahrzeuge systematisch abzusichern, ist ein tiefgreifendes Verständnis ihrer technischen Die zu

Die zunehmende Automatisierung und softwarebasierte Steuerung sowie umfassende Vernetzung moderner Straßenfahrzeuge führen zu einem Paradigmenwechsel in der Fahrzeugentwicklung – mit neuen, komplexen Anforderungen an die ganzheitliche Sicherheit. Mit wachsender Systemintelligenz verändern sich sowohl technische Schnittstellen als auch Verantwortlichkeiten innerhalb und außerhalb des Fahrzeugs.

Eine sichere Einführung intelligenter und autonomer Fahrzeuge setzt ein präzises Verständnis ihrer Funktionsgrenzen und Einsatzbedingungen voraus. Taxonomie, Operational Design Domain (ODD) und neue Sicherheitskonzepte bilden dafür die Grundlage.

In diesem Kapitel beleuchten wir gezielt die Herausforderungen, die sich aus adaptiven Fahrzeugarchitekturen, Konnektivität und künstlicher Intelligenz ergeben. Wir analysieren, wie Taxonomiestufen und ODDs als strukturierende Elemente die Sicherheitsanforderungen beeinflussen, und zeigen, wie Technologien wie KI oder Fernsteuerung zusätzliche Komplexität sowie neue Lösungsansätze mit sich bringen.

2.1 Grundpfeiler der Absicherung

Taxonomie, ODD und sichere KI als Fundament

Taxonomiestufen für automatisierte Fahrfunktionen – beispielsweise nach SAE oder UNECE – ermöglichen eine systematische Klassifizierung und Abgrenzung der Funktionsumfänge und bieten damit eine erste strukturelle Einordnung. Die Operational Design Domain (ODD) definiert, unter welchen Umwelt-, Verkehrs- und Systembedingungen eine Funktion sicher betrieben werden darf, und ist damit ein zentrales Element für Risikoabschätzung, Funktionstrennung und Zertifizierung.

Ein weiterer Schlüsselfaktor ist der methodisch abgesicherte Einsatz von KI, da viele zentrale Funktionen – insbesondere in der Wahrnehmung und Entscheidungsfindung – ohne KI nicht mehr realisierbar sind. KI-Technologien müssen daher von Beginn an so gestaltet und geprüft werden, dass ihr Verhalten nachvollziehbar und robust ist und sie gezielt für sicherheitskritische Anwendungen eingesetzt werden können.

Fernsteuerung als Rückfallebene

Ein zunehmend diskutiertes Szenario im Kontext automatisierter Mobilität ist die Fernsteuerung (Remote Driving). Sie kann entweder als temporäre Rückfallebene bei Systemausfällen dienen oder als regulärer Betriebsmodus, etwa im Shuttle-, Logistik- oder Parkbereich. Dabei übernimmt ein Mensch außerhalb des Fahrzeugs über eine Kommunikationsschnittstelle die Kontrolle – teilweise unterstützend (Teleassistenz), teilweise vollständig (Fernlenkung).

Die Fernsteuerung wirft neue sicherheitsrelevante Fragestellungen auf, etwa:

- Wie erkennt das Fahrzeug den Übergabepunkt korrekt und gewährleistet eine sichere Übergabe?
- Wie zuverlässig ist die Kommunikationsverbindung (Latenz, Bandbreite, Ausfallsicherheit)?
- Wer trägt die Verantwortung bei sicherheitskritischen Entscheidungen?
- Welche zusätzlichen Maßnahmen zur funktionalen Sicherheit und Cybersecurity sind erforderlich?

Normativer Rahmen und neue Sicherheitskonzepte

Im normativen Kontext bilden ISO 26262 (funktionale Sicherheit), ISO 21448 (SOTIF) und ISO/SAE 21434 (Cybersecurity) die Grundlage – auch für Szenarien der Fernsteuerung und Fernlenkung. Eine besondere Herausforderung liegt dabei in der Absicherung menschlicher Remote-Operatoren, einschließlich Schulung, Ergonomie und Fehlermanagement.

Mit dem Einzug datengetriebener KI-Technologien stoßen klassische Sicherheitsmethoden an ihre Grenzen: Nichtdeterminismus, adaptives Systemverhalten sowie modell- und datenbedingte Unsicherheiten erfordern ergänzende Konzepte. Hier gewinnen ISO/PAS 8800 (AI Safety) und ISO/IEC TR 5469 (risikobasierte KI-Bewertung [ISO/IEC TR 5469:2024]) an

Bedeutung. Sie adressieren u.a. Datenqualität, erklärbares Verhalten sowie die Absicherung und Überwachung von KI-Komponenten im Betrieb – und ergänzen damit den Rahmen, in dem ODDs definiert, Funktionen abgegrenzt und Zulassungsstrategien entwickelt werden.

2.2 Grundlagen und Funktionsweise automatisierter Fahrzeuge

Ein sogenanntes Level-5-Fahrzeug – auch als selbstfahrendes oder fahrerloses Fahrzeug bezeichnet – ist in der Lage, mithilfe eines komplexen Zusammenspiels aus Sensoren, Kameras, Radar und künstlicher Intelligenz sämtliche Fahraufgaben eigenständig zu übernehmen. Um als vollständig autonom zu gelten, muss ein Fahrzeug ohne menschliches Eingreifen zu einem vorgegebenen Ziel navigieren und dabei sämtliche Verkehrssituationen sicher bewältigen können.

Die technische Basis bilden riesige Datenmengen, die aus Sensoren und Systemen zur Umfeldwahrnehmung stammen – insbesondere Bilddaten, Radarsignale und Lidarmessungen. Mithilfe von maschinellem Lernen (ML) und neuronalen Netzen werden daraus hochkomplexe Modelle erzeugt, die es ermöglichen, Fahrfunktionen ohne menschliche Eingriffe umzusetzen. Neuronale Netze erkennen Muster in den Eingangsdaten und leiten diese an ML-Algorithmen weiter, die das Verhalten des Fahrzeugs trainieren.

Sensoren und Datenquellen

Zu den wichtigsten Sensoren gehören Kameras, die Ampeln, Fahrbahnmarkierungen, Bordsteine, Fußgänger, Verkehrszeichen und andere relevante Objekte identifizieren. Lidarsensoren, häufig rotierend und auf dem Fahrzeugdach montiert, erfassen kontinuierlich die Umgebung und erzeugen eine dynamische dreidimensionale Karte. Inertial Measurement Units (IMU) messen Beschleunigungen und Rotationsbewegungen, sodass die Fahrzeugposition auch bei eingeschränktem GPS präzise bestimmt werden kann. Radarsysteme in den Stoßfängern erkennen Abstände zu Hindernissen und bewegten Objekten in Echtzeit.

Die zentrale KI-Software im Fahrzeug fusioniert diese Sensordaten mit weiteren Quellen, etwa Straßenbilddiensten, hochauflösenden Karten und Cloud-basierter Infrastruktur. Auf diese Weise können Informationen zu Verkehrszeichen, Spurverläufen oder temporären Sperrungen bereits in die Routenplanung einfließen, bevor der relevante Streckenabschnitt erreicht ist.

KI-gestützte Entscheidungsfindung und Fahrzeugsteuerung

Mithilfe von Deep-Learning-Algorithmen simuliert die KI menschliche Wahrnehmungs- und Entscheidungsprozesse und überträgt diese auf die Steuerungssysteme des Fahrzeugs – beispielsweise Lenkung, An-

trieb und Bremsen. Diese Systeme arbeiten vielfach über redundante Steuergeräte, um eine hohe Ausfallsicherheit zu gewährleisten.

Der Fahrer gibt ein Ziel vor, woraufhin mehrere Subsysteme gemeinsam die optimale Route berechnen. Die KI-Software konsultiert dazu auch externe Datenquellen, sodass Orientierungspunkte, Verkehrszeichen oder Ampeln in die Planung einbezogen werden können.

Sicherheitsaspekte und Übersteuerungsfunktionen

Trotz des hohen Automatisierungsgrades ist eine manuelle Übersteuerungsfunktion unverzichtbar. Sie ermöglicht es Insassen, bei Bedarf jederzeit die Kontrolle über das Fahrzeug zu übernehmen – etwa bei Systemfehlern, Unsicherheiten der KI oder unvorhersehbaren Situationen.

Darüber hinaus müssen bei vernetzten Fahrzeugumgebungen zusätzliche Risiken berücksichtigt werden. Cyberangriffe, begrenzte Rechenressourcen und Anforderungen an den Echtzeitbetrieb stellen neue Herausforderungen dar, die durch robuste Sicherheits- und Absicherungskonzepte adressiert werden müssen.

Die nachfolgende Übersicht in Tabelle 2.1 fasst die wichtigsten Sensoren und Datenquellen eines automatisierten Fahrzeugs zusammen und zeigt, welche Aufgaben sie im Zusammenspiel mit der KI übernehmen.

Sensor/Datenquelle	Primäre Aufgabe	Typische Anwendung
Kamera	Erfassung visueller Informationen (Farben, Formen, Symbole)	Erkennung von Verkehrszeichen, Ampeln, Markierungen, Fußgängern, Fahrzeugen
Lidar	Erstellung einer hochauflösenden 3D-Umgebungskarte	Hinderniserkennung, Abstandsberechnung, präzise Lokalisierung
Radar	Distanz- und Geschwindigkeitsmessung bewegter und statischer Objekte	Kollisionswarnung, Abstandsregeltempomat, Toter-Winkel-Überwachung
Inertialmesseinheit (IMU)	Messung von Beschleunigung und Rotationsbewegung	Positionsbestimmung bei GPS-Ausfall, Unterstützung der Spur- und Kurvenlage
GPS/GNSS mit Korrektursignal	Globale Positionsbestimmung	Routenplanung, exakte Fahrzeuglokalisierung
HD-Karten & Straßenbilddienste	Bereitstellung detaillierter, vorab erfasster Umgebungs- und Infrastrukturdaten	Vorausplanung bei Spurwechseln, Erkennung temporärer Sperrungen

→

Sensor/Datenquelle	Primäre Aufgabe	Typische Anwendung
Cloud- und V2X-Kommunikation	Austausch von Echtzeitinformationen mit anderen Fahrzeugen und der Infrastruktur	Warnungen vor Gefahrenstellen, Verkehrsflussoptimierung, Informationen zu Ampelphasen

Tab. 2.1 *Sensoren und ihre Funktionen im automatisierten Fahren*

2.3 Evolution der vernetzten Fahrzeugarchitektur

Moderne Fahrzeuge bestehen aus mehreren verschiedenen elektronischen Steuereinheiten (ECUs), die jeweils spezifische Funktionen übernehmen. In heutigen Fahrzeugen sind bis zu 100 dieser ECUs verbaut (siehe Abbildung 2.1). So gibt es z. B. jeweils ein Steuergerät für das Öffnen und Schließen der Fenster und des Schiebedachs, ein anderes Steuergerät ist für die Überwachung des Lenkradwinkels zuständig, ein weiteres für die Steuerung des ABS-Systems und so weiter.

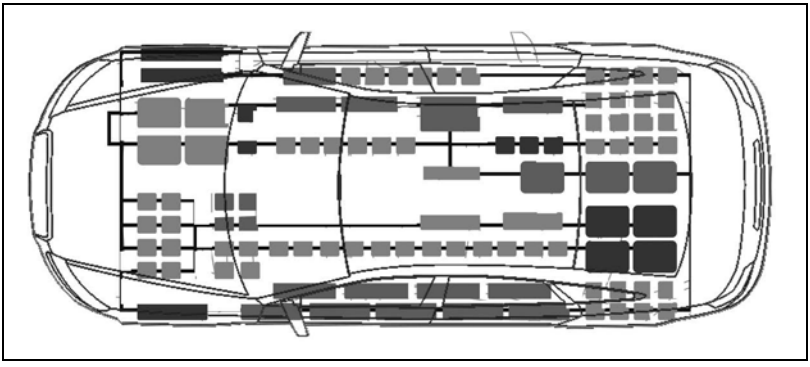

Abb. 2.1 *Vernetzte Fahrzeugarchitektur aus mehreren ECUs*

Diese Steuergeräte müssen sich gegenseitig Daten übermitteln, um Entscheidungen über ihr Verhalten treffen zu können. Diese wachsende Komplexität und Funktionalität moderner Fahrzeuge führte zu einer immer stärker vernetzten Architektur, in der ECUs nicht mehr isoliert arbeiten, sondern über verschiedene Bussysteme (z. B. CAN, LIN, FlexRay, Ethernet) miteinander kommunizieren. Diese Kommunikation ist heute eine zentrale Voraussetzung für Fahrerassistenzsysteme, automatisiertes Fahren und Over-the-Air-Updates.

Ein Steuergerät verhält sich je nach Betriebszustand unterschiedlich, beispielsweise abhängig davon, ob sich das Fahrzeug im Vorwärts- oder Rückwärtsgang befindet oder ob es sich bewegt oder steht. Einige Steuergeräte kommunizieren sowohl mit der Außenwelt als auch mit dem internen Fahrzeugnetzwerk. Die Optionen, die Angreifern zur Verfügung

stehen, werden durch die verschiedenen angebotenen Remote-Endpunkte, die Topologie des Fahrzeugnetzwerks und die in den verschiedenen Steuergeräten programmierten Sicherheitsfunktionen beeinflusst.

Zukünftige zentralisierte Steuergeräte, wie in Abbildung 2.2 dargestellt, werden aus wenigen, hochleistungsfähigen Fahrzeugrechnern bestehen, die in einer fahrzeugzentrierten, zonenorientierten Struktur die Datenströme zentralisieren und mit den eingebetteten Steuergeräten, Sensoren und Aktoren vernetzt sind.

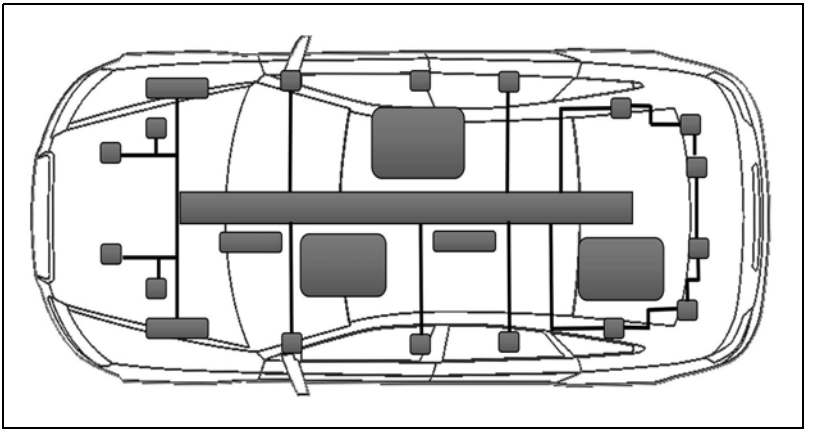

Abb. 2.2 *Zukünftige zentralisierte Steuergerätearchitektur*

Die Zonensteuergeräte senden die Daten über High-Speed-Ethernet (siehe Abbildung 2.3) an die angeschlossenen Fahrzeugsteuergeräte. Diese Art der Verbindung sorgt für eine schnellere, sicherere und leistungsfähigere Datenkommunikation – sowohl innerhalb des Fahrzeugs als auch extern über die Verbindung zur Cloud. Außerdem wird der Kabelbaum im Fahrzeug dadurch kürzer, was wiederum zu Kosten- und Gewichtseinsparungen führt. Mit modernen E/E-Architekturen entwickelt sich das Auto zu einem IoT-Gerät auf Rädern.

In domänen- oder zonenbasierten Architekturen werden verteilte Fahrzeugfunktionen durch zentrale Hochleistungsrechner zusammengeführt, was die Komplexität reduziert und die Effizienz steigert. Diese zentralisierten Architekturen ermöglichen nicht nur effizientere Datenverarbeitung und vereinfachte Diagnosen, sondern sind auch ein wichtiger Baustein für die funktionale Sicherheit und Cybersecurity moderner Fahrzeugplattformen.

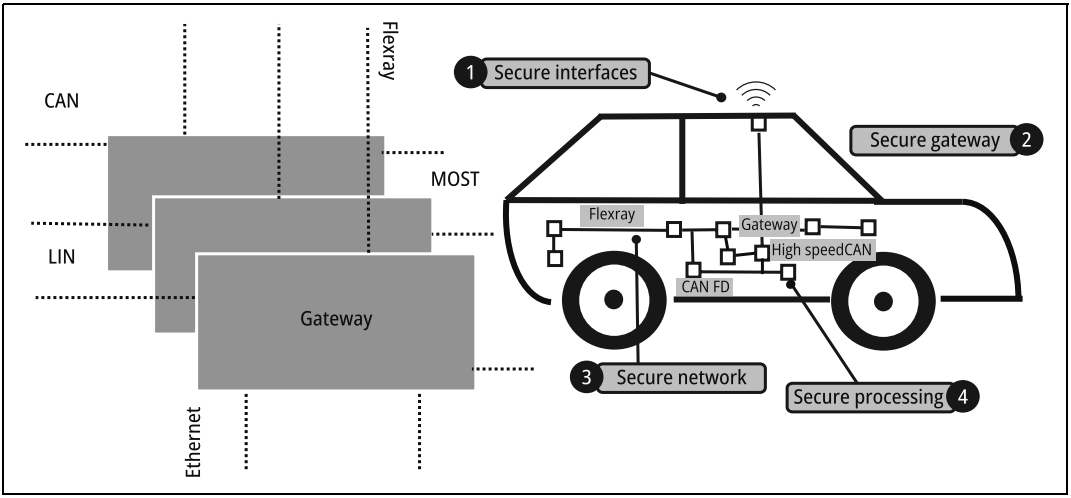

Abb. 2.3 *High-Speed-Ethernet-Controller als Gateway (Bildquelle: Valens Semiconductor)*

2.3.1 Drei Schritte zum erfolgreichen Angriff

Sicherheitskritische Angriffe auf diese Fahrzeuge erfordern in der Regel eine sorgfältige Abfolge von drei Schritten:

2.3.1.1 Schritt 1: Initialer Zugriff auf das Fahrzeugnetzwerk

Im ersten Schritt verschafft sich ein Angreifer aus der Ferne Zugang zu einem internen Fahrzeugnetzwerk, das für Nutzer im Regelbetrieb nicht sichtbar ist. Gelingt der Zugriff, können manipulierte Nachrichten in das System eingeschleust werden. Ziel ist es, ein oder mehrere Steuergeräte (ECUs) zu kompromittieren – entweder direkt oder über verbundene Gateways. Diese Phase erfordert das Ausnutzen von Schwachstellen in extern zugänglichen Schnittstellen wie WLAN, Mobilfunk oder Bluetooth.

Einen solchen Angriff kann man sich folgendermaßen vorstellen: Ein drahtloses Signal wird gesendet, ein fehlfunktionierendes bzw. nicht reagierendes Steuergerät wird infiltriert, und plötzlich fließt manipulierender Code durch die Adern des Fahrzeugs.

2.3.1.2 Schritt 2: Ausweitung des Zugriffs auf sicherheitskritische Funktionen

Im zweiten Schritt erfolgt die Eskalation des Zugriffs innerhalb der Fahrzeugarchitektur. Die Angreifer nutzen die interne Kommunikation – z. B. über das CAN-Bussystem –, um von einem kompromittierten Steuergerät aus auf weitere sicherheitsrelevante ECUs zuzugreifen. Typische

Ziele sind Steuergeräte für Bremssysteme, Lenkung oder Antriebsstrang. Dies setzt die Fähigkeit voraus, Gateway-Steuergeräte zu umgehen oder gezielt zu manipulieren.

Üblicherweise können in der ersten Phase des Angriffs diese kritischen Funktionen nicht direkt beeinflusst werden. Hier kommt die Geschicklichkeit der Angreifer ins Spiel. Sie schaffen es, das Brückensteuergerät im betroffenen Fahrzeug zu überlisten, um z. B. über das CAN-Netzwerk Zugriff auf das Steuergerät für die Bremsen zu erhalten. Mit der drahtlosen Kompromittierung eines Steuergeräts und der Möglichkeit, Nachrichten an ein gewünschtes Zielsteuergerät zu senden, öffnet sich die Tür zur Kommunikation mit den lebenswichtigen Steuergeräten.

2.3.1.3 Schritt 3: Auslösung sicherheitskritischer Funktionen

Im dritten Schritt versuchen die Angreifer, das Zielsteuergerät zu einer sicherheitsrelevanten Aktion zu veranlassen, etwa einem Bremsbefehl oder einem Eingriff in die Lenkung. Dafür müssen sie das Kommunikationsprotokoll des Fahrzeugherstellers verstehen, um gültige Nachrichtenformate generieren zu können. Da diese Datenformate und Signalstrukturen herstellerspezifisch und oft proprietär sind, erfordert dieser Schritt umfassende Reverse-Engineering-Kenntnisse sowie tiefes technisches Verständnis der jeweiligen Fahrzeugarchitektur.

Weitere Inhalte zu Angriffsszenarien und Cybersecurity sind in Kapitel 3, »Zusammenspiel von funktionaler Sicherheit, Cybersecurity und KI«, und Kapitel 6, »Der Standard ISO/SAE 21434 für Cybersecurity«, enthalten.

2.3.2 Projektstory ADAS NextGen: Warum intelligente Fahrzeuge intelligente Sicherheitskonzepte brauchen

Die Drivesmart AG gilt als Vorreiter bei der Entwicklung domänen- und zonenbasierter Fahrzeugplattformen. In der neuesten Generation ihres ADAS NextGen vereinen leistungsstarke Zentralkomponenten die Steuerung komplexer Fahrfunktionen – von Fahrassistenz über Infotainment bis hin zur vorausschauenden Diagnose. Das Ziel: reduzierte Komplexität, höhere Rechenleistung, schnellere Software-Updates – und natürlich mehr Sicherheit.

Robert Flink, Leiter der Produktentwicklung, formulierte früh die Vision einer hochintegrierten Fahrzeugarchitektur mit zentralem Sicherheitskonzept. Gemeinsam mit Anja Bau, Systemarchitektin, und Peter Weiss, Projektleiter und Anforderungsmanager, entstand eine Struktur, in der Sicherheit von Anfang an im Zentrum stand.

Phase 1 – Der erste Puls durch die digitale Ader

Ein Fahrzeug der Drivesmart-Baureihe rollt durch den urbanen Raum – vernetzt, hochautomatisiert, OTA-fähig. Doch aus einem unscheinbaren Café funkt ein Laptop ein Signal – gezielt, drahtlos, unsichtbar. Der Zugriff erfolgt über ein kompromittiertes Bluetooth-Modul, das nicht rechtzeitig gepatcht wurde.

Was folgt, ist keine Explosion, sondern ein Flüstern: Manipulierter Code, eingebettet in ein scheinbar harmloses Datenpaket, bahnt sich seinen Weg in das Gateway-Steuergerät. Noch reagiert das Fahrzeug unauffällig – der Fahrer ahnt nichts.

Isy Kaput, Integrator, erinnert sich später: »Wir hatten alle Security-Mechanismen integriert, aber der Exploit lag genau in einer übersehenen Altkomponente.«

Phase 2 – Die stille Eskalation

Im Inneren des Fahrzeugs beginnt nun ein strategischer Feldzug: Über das interne Kommunikationsnetz – etwa das CAN-Backbone – versucht der Angreifer, die Kommandostrukturen zu kartieren. Die erste Hürde: das zentrale ADAS, das wie ein digitaler Türsteher über Datenflüsse wacht. Doch die Architektur ist komplex – und komplexe Systeme bieten Angriffsmöglichkeiten.

Peter Feinblick, Cybersecurity-Manager, und Dieter Gewiss, funktionaler Sicherheitsmanager, analysieren im Nachgang gemeinsam mit Ulla Wahrlich, Testleiterin, das Verhalten des Systems. Der Angriff nutzt Timing und Datenmuster, um unauffällig privilegierten Zugriff zu erhalten.

Dem Angreifer gelingt es, eine legitime Nachricht so zu verändern, dass sie als systemkonform durchgeht. Mit jedem erfolgreichen Paket wird der Zugriff ausgeweitet: erst das Infotainment-Steuergerät, dann der Bordnetz-Controller, schließlich das Chassis-Modul.

***Das Ziel:** die Bremsen.*

Phase 3 – Die kritische Aktion

Ein Bremsbefehl muss exakt formuliert sein. Die Bitlänge, die Prüfsumme, das Timing – alles muss stimmen. Ein einziger Fehler, und die Nachricht wird verworfen. Doch der Angreifer kennt die Protokolle. Er hat Wochen mit Reverse Engineering verbracht. Jetzt ist der Moment gekommen.

Während der Fahrer auf eine grüne Ampel zufährt, sendet das kompromittierte Steuergerät einen manipulierten Befehl an das Bremsmodul. Ein kurzer Ruck – das Fahrzeug verzögert unerwartet. Der Fahrer denkt an einen Systemfehler. Doch der Angreifer weiß: Die Tür ist offen.

Warum Drivesmart vorausdenkt

Was in diesem Szenario wie Science-Fiction klingt, ist längst Realität in der Automobilindustrie. Moderne Fahrzeugarchitekturen mit zentralisierten Steuergeräten bieten enorme Vorteile – aber auch neue Risiken.

Deshalb setzt Drivesmart auf ein mehrstufiges Sicherheitskonzept, entwickelt von einem Team, das Sicherheit nicht als Zusatz versteht, sondern als Fundament. Lara Vero, technische Projektleiterin, treibt in enger Zusammenarbeit mit Klaus Boden (Konfigurationsmanager) und Dave Rugby (Qualitätsmanager) die kontinuierliche Absicherung aller Softwarestände voran.

Susi Platine, Leiterin des Hardwareteams, und Hans Wolke, Domänenexperte, arbeiten an der Absicherung physischer Schnittstellen und Signalpfade. Tina Mensch, HMI-Designerin, sorgt dafür, dass der Fahrer über plausible Rückmeldungen im Fahrzeugcockpit stets über kritische Zustände informiert ist.

Fernando Haswas, Regulatory Compliance Engineer, koordiniert die Umsetzung regulatorischer Vorgaben – von UNECE bis ISO/SAE – mit der externen Zertifizierungsstelle. Ulrich Richter, unabhängiger externer Assessor, prüft regelmäßig die Integrität der Sicherheitsnachweise und Testdokumente.

Drivesmarts Sicherheitsprinzipien

- *Security by Design in jeder ECU*
- *Hardwaregestützte Vertrauensanker für Gateways und Zonencontroller*
- *Intrusion Detection Systems (IDS) mit CAN-Anomalieerkennung*
- *Segmentierte Netzwerke mit klaren Trust-Zonen*
- *Verifizierte OTA-Update-Mechanismen mit kryptografischer Signaturprüfung*

Zusätzlich werden alle neuen Plattformen der Drivesmart AG gemäß ISO 26262 (funktionale Sicherheit) und ISO/SAE 21434 (Cybersecurity) entwickelt – mit extern zertifizierter Absicherung.

Fazit: Intelligenz braucht Sicherheit

Die Zukunft des Fahrens ist zentralisiert, vernetzt und softwaredefiniert. Doch mit jeder Codezeile wächst auch die Angriffsfläche. Wer – wie das Team der Drivesmart – auf modulare Sicherheitsarchitekturen, proaktive Bedrohungsanalysen und kontinuierliche Systemüberwachung setzt, bleibt nicht nur innovativ, sondern auch vertrauenswürdig. Denn: Ein intelligentes Fahrzeug ist nur dann smart, wenn es auch sicher ist.

2.4 Komplexe Anforderungen für vernetzte E/E-Systeme

Mit dem zunehmenden Softwareanteil und der wachsenden Vernetzung moderner Fahrzeuge wird die Anforderungserstellung für elektrische und elektronische Systeme (E/E-Systeme) immer anspruchsvoller. Diese Systeme müssen nicht nur gegen unbeabsichtigte Fehlfunktionen geschützt werden (funktionale Sicherheit), sondern auch gegen gezielte Angriffe (Cybersecurity). Eine ganzheitliche Analyse beider Aspekte ist unerlässlich – sowohl zur Optimierung von Ressourcen als auch zur Reduzierung von Sicherheitslücken. Die im folgenden Abschnitt aufge-

führten Standards enthalten maßgebliche Anforderungen zur Erreichung des erforderlichen Grades an Sicherheit und Verlässlichkeit. Man erkennt schnell, wie eng verzahnt nicht nur die technischen Systeme, sondern auch die Normen und Standards in der vernetzten Fahrzeugarchitektur sind.

2.4.1 ISO 26262

Die Einhaltung der Anforderungen der ISO 26262 stellt einen essenziellen Rahmen zur Gewährleistung der funktionalen Sicherheit in der Automobilindustrie dar. Diese internationale Norm konzentriert sich speziell auf die sicherheitsrelevanten E/E-Systeme in Fahrzeugen. Ihr Ziel ist es, potenzielle Risiken, die durch Fehler in Software und Hardware entstehen können, systematisch zu identifizieren, zu bewerten und zu minimieren.

Durch einen strukturierten und methodischen Ansatz unterstützt ISO 26262 Entwickler und Hersteller dabei, Sicherheitslücken frühzeitig im Entwicklungsprozess zu erkennen und geeignete Maßnahmen zu ergreifen. Dies umfasst die gesamte Produktlebensdauer – von der Konzeptphase über Design, Implementierung, Integration und Verifikation bis hin zum Betrieb und zur Außerbetriebnahme.

Die Norm definiert dabei klare Anforderungen und Prozesse, um sicherzustellen, dass E/E-Systeme und deren Komponenten so gestaltet sind, dass sie bei möglichen Fehlern keine unakzeptablen Gefahren für Insassen, andere Verkehrsteilnehmer oder die Umwelt verursachen. Insbesondere adressiert ISO 26262 systematisch Fehlermöglichkeiten sowie deren Ursachen und Auswirkungen, um eine angemessene Risikominderung sicherzustellen.

Darüber hinaus bildet ISO 26262 die Grundlage für die Klassifizierung der sicherheitsrelevanten Systeme durch sogenannte Automotive Safety Integrity Levels (ASIL), die die notwendige Strenge der Sicherheitsmaßnahmen bestimmen. Auf diese Weise gewährleistet die Norm einen verbindlichen, nachvollziehbaren und überprüfbaren Rahmen, der die funktionale Sicherheit von E/E-Komponenten und -Systemen über den gesamten Lebenszyklus hinweg sicherstellt.

Tipp

In Kapitel 5, »Das Lebenszyklusmodell der ISO 26262«, werden alle Anforderungen des Standards detailliert aufgeführt und erläutert.

In Kapitel 8, »Unterstützende Prozesse und Querschnittsthemen der ISO 26262«, führen wir spezifische Inhalte vertiefend weiter.

Im integrativen Kapitel 10, »Spezifische Rollen im Sicherheitslebenszyklus«, über alle Domänen liegt der Fokus u. a. auf Rollenbezeichnungen und Rollenbeschreibungen.

2.4.2 ISO 21448 (SOTIF – Safety of the Intended Functionality)

Mit dem Fortschreiten der Automatisierung und Vernetzung in modernen Fahrzeugen steigen die Anforderungen an deren Sicherheit erheblich an. Während ISO 26262 vor allem die funktionale Sicherheit adressiert und sich mit Fehlern in Hardware und Software beschäftigt, erweitert ISO 21448 den Fokus auf die Sicherheit der beabsichtigten Funktionalität – die sogenannte SOTIF. Dies ist besonders relevant für automatisierte und autonome Fahrsysteme, deren Funktionalität nicht nur auf deterministischen Steueralgorithmen beruht, sondern zunehmend auf komplexen KI-basierten Wahrnehmungs- und Entscheidungsprozessen.

SOTIF beschäftigt sich mit den Gefahren, die nicht durch Systemfehler, sondern durch unerwartete oder unbeabsichtigte Verhaltensweisen entstehen können – also Situationen, in denen das System korrekt funktioniert, aber dennoch unsicher agiert. Gerade bei vernetzten E/E-Systemen, die Umgebungsdaten aus einer Vielzahl von Sensoren (Kameras, Lidar, Radar) und externen Quellen (V2X-Kommunikation, Cloud-Dienste) aggregieren und interpretieren, können Unsicherheiten in der Wahrnehmung und Interpretation der Umgebung zu Fehlentscheidungen führen.

Die Anforderungen der ISO 21448 umfassen daher Maßnahmen, um solche Risiken zu minimieren:

- Minimierung von Fehlinterpretationen der Umgebung: SOTIF fordert eine umfassende Analyse möglicher Fehlwahrnehmungen durch Sensoren und Algorithmen, wie z. B. das falsche Erkennen von Objekten oder das Übersehen kritischer Hindernisse. Hierzu gehört auch die Identifikation von Grenzfällen, in denen die Sensorik oder KI-Modelle an ihre Grenzen stoßen, z. B. schlechte Wetterbedingungen oder ungewöhnliche Verkehrssituationen.
- Vermeidung unbeabsichtigter Fahrzeugaktionen: Die Norm legt dar, wie Systeme so gestaltet werden können, dass falsche oder unvorhergesehene Reaktionen vermieden werden, z. B. ein plötzlicher Bremsvorgang oder ein riskantes Ausweichmanöver, das durch falsche Umgebungsdaten ausgelöst wird.
- Validierung potenziell unsicherer Szenarien: Ein zentrales Element ist das systematische Testen und Validieren von Szenarien, die als potenziell gefährlich eingestuft wurden. Diese Tests müssen realistische Umgebungsbedingungen und eine Vielzahl von Fahrsituationen abdecken, um sicherzustellen, dass das Fahrzeug auch unter Grenzbedingungen sicher agiert.
- Berücksichtigung komplexer KI-Auswertungen: Bei automatisierten Fahrsystemen, deren Entscheidungen auf maschinellen Lernverfah-

ren und neuronalen Netzen beruhen, fordert SOTIF zudem Transparenz und Robustheit der Algorithmen. Dies umfasst die Überwachung der Vertrauenswürdigkeit von Entscheidungen, das Handling von Unsicherheiten und den Umgang mit unbekannten oder seltenen Situationen (z. B. durch OOD-Detection – Out-of-Distribution Detection).

Insgesamt ergänzt ISO 21448 somit die funktionale Sicherheit durch einen zusätzlichen Sicherheitsansatz, der speziell auf die Herausforderungen vernetzter, komplexer und KI-basierter E/E-Systeme im automatisierten und autonomen Fahren abgestimmt ist. Die Umsetzung der Norm unterstützt Hersteller dabei, das Vertrauen in automatisierte Fahrsysteme zu erhöhen und deren sichere Integration in den realen Straßenverkehr zu ermöglichen.

Tipp

In Kapitel 7, »SOTIF – Safety of the Intended Funtionality«, behandeln wir ausführlich die ergänzende Sicherheit mit Fokus auf das Systemverhalten.

2.4.3 ISO/SAE 21434

Mit der zunehmenden Vernetzung und Digitalisierung moderner Fahrzeuge gewinnt die Cybersecurity als integraler Bestandteil der Fahrzeugsicherheit immer mehr an Bedeutung. ISO/SAE 21434 definiert einen umfassenden Rahmen für die Identifikation, Bewertung und Minimierung von Cybersecurity-Risiken in allen Phasen des Fahrzeuglebenszyklus, von der Konzeptentwicklung über die Produktion bis hin zur Wartung und Stilllegung.

Diese Norm liefert Anforderungen und ein systematisches Vorgehen, um Bedrohungen und Schwachstellen in vernetzten E/E-Systemen zu identifizieren und zu bewerten. Dabei berücksichtigt ISO/SAE 21434 nicht nur technische Aspekte wie die Absicherung von Steuergeräten, Kommunikationsschnittstellen und Software, sondern auch organisatorische Maßnahmen und das Management von Cybersecurity-Risiken auf Unternehmensebene.

Aufgrund der zunehmenden Komplexität moderner Fahrzeugsysteme und ihrer Vernetzung ist es unerlässlich, verschiedene Analyse- und Bewertungstechniken anzuwenden, um ein umfassendes Bild der Sicherheitslage zu erhalten. Zu den etablierten Methoden gehören:

- FTA (Fault Tree Analysis): Eine systematische Methode zur Identifikation von Ursachen für unerwünschte Ereignisse. FTA unterstützt dabei, kritische Schwachstellen in der Systemarchitektur zu erkennen, die Angriffsvektoren darstellen könnten.

- FMEDA (Failure Modes, Effects and Diagnostic Analysis): Eine detaillierte Analyse von möglichen Fehlerarten sowie deren Ursachen und Auswirkungen auf das System. FMEDA liefert Erkenntnisse über die Fehlerdetektion und -diagnose, was auch für Cybersecurity-relevante Fehlerszenarien wichtig ist.
- TARA (Threat Analysis and Risk Assessment): Ein zentraler Bestandteil der ISO/SAE 21434, der sich auf die Analyse und Bewertung von Bedrohungen und Risiken konzentriert. TARA hilft dabei, potenzielle Angriffsflächen zu identifizieren und deren Auswirkungen auf die Systemsicherheit zu bewerten.

Darüber hinaus kommen auch weitere Methoden wie Zuverlässigkeits-Blockdiagramme oder Markov-Modellierung zum Einsatz, um das Systemverhalten unter Sicherheitsaspekten zu simulieren und vorherzusagen.

Für hochkomplexe und vernetzte Systeme reicht es heute nicht mehr aus, einzelne Komponenten isoliert zu betrachten. Vielmehr erfordert die Cybersecurity-Analyse eine ganzheitliche Perspektive, die Wechselwirkungen zwischen verschiedenen Systemen, den Einfluss menschlichen Verhaltens sowie Umweltfaktoren berücksichtigt. Nur so können ganzheitliche Sicherheitskonzepte entwickelt werden, die auch unbekannte oder neu auftretende Bedrohungen adressieren.

ISO/SAE 21434 schafft somit die Grundlage für ein strukturiertes und nachvollziehbares Cybersecurity-Management im Automobilbereich, das die Integrität, Verfügbarkeit und Vertraulichkeit von Fahrzeugsystemen sichert – und damit einen entscheidenden Beitrag zur Gesamtsicherheit vernetzter und autonomer Fahrzeuge leistet.

Tipp

Kapitel 6, »Der Standard ISO/SAE 21434 für Cybersecurity«, behandelt die definierten Cybersecurity-Anforderungen über den gesamten Fahrzeuglebenszyklus.

2.4.4 Elektromagnetische Verträglichkeit (EMV): Schutz vor Störungen in vernetzten E/E-Systemen

Neben funktionaler Sicherheit und Cybersecurity spielt die elektromagnetische Verträglichkeit (EMV) eine zentrale Rolle für die Zuverlässigkeit und Stabilität moderner elektronischer Systeme in Fahrzeugen. EMV umfasst alle Maßnahmen, die sicherstellen, dass E/E-Systeme innerhalb eines definierten elektromagnetischen Umfelds störungsfrei arbeiten, ohne andere Systeme zu beeinträchtigen oder selbst gestört zu werden.

Vernetzte E/E-Systeme in Fahrzeugen sind zunehmend komplex und umfassen zahlreiche Sensoren, Aktuatoren, Steuergeräte und Kommunikationsschnittstellen, die elektromagnetische Signale aussenden und empfangen. Um Fehlfunktionen und Systemausfälle zu verhindern, müssen diese Systeme umfassend gegen elektromagnetische Störungen geschützt werden.

Die Anforderungen an den EMV-Schutz umfassen sowohl die Emissionen (elektromagnetische Abstrahlungen, die andere Systeme stören können) als auch die Immunität (die Fähigkeit eines Systems, selbst bei Störeinflüssen korrekt zu funktionieren). Dies ist besonders wichtig für sicherheitskritische Funktionen, bei denen elektromagnetische Interferenzen potenziell zu gefährlichen Fehlreaktionen führen können.

Darüber hinaus tragen EMV-Maßnahmen zur elektronischen Stabilität des Fahrzeugs bei. Dies bedeutet, dass trotz elektromagnetischer Einflüsse, wie sie z. B. durch Hochfrequenzquellen oder andere Fahrzeuge verursacht werden, alle E/E-Komponenten zuverlässig und sicher zusammenarbeiten.

Typische EMV-Schutzmaßnahmen umfassen:

- Abschirmungen und Gehäusegestaltung zur Minimierung von elektromagnetischer Strahlung
- Filter und Entstör-Komponenten in Stromversorgungs- und Kommunikationsleitungen
- Robustheitsprüfungen nach entsprechenden Normen (z. B. ISO 11452, CISPR 25)
- Gestaltung der Fahrzeugarchitektur mit Rücksicht auf EMV-Aspekte

Insgesamt ergänzt der EMV-Schutz die Anforderungen an funktionale Sicherheit (ISO 26262), SOTIF (ISO 21448) und Cybersecurity (ISO/SAE 21434) und ist ein unverzichtbarer Bestandteil der Entwicklung zuverlässiger, sicherer und vernetzter Fahrzeugsysteme.

2.4.5 Fail-Operational- und Fail-Safe-Konzepte: Sicherstellung der Zuverlässigkeit autonomer Fahrfunktionen

Mit dem Fortschreiten der Automatisierung und dem Aufkommen autonomer Fahrfunktionen gewinnen Fail-Operational- und Fail-Safe-Konzepte zunehmend an Bedeutung für die Sicherheit und Verlässlichkeit moderner Fahrzeuge. Diese Konzepte beschreiben unterschiedliche Strategien zum Umgang mit Fehlern und Störungen in sicherheitskritischen Systemen.

Fail-Safe bedeutet, dass ein System im Fehlerfall sicher abgeschaltet wird oder in einen sicheren Zustand übergeht, um Gefahren für Insassen

und andere Verkehrsteilnehmer zu vermeiden. Klassische Beispiele sind das kontrollierte Abbremsen oder das Aktivieren von Warnsignalen, wenn ein System ausfällt.

Fail-Operational beschreibt dagegen Systeme, die auch bei Fehlern weiterhin eine eingeschränkte, aber sichere Funktionalität aufrechterhalten. Dies ist besonders bei autonomen Fahrzeugen essenziell, da ein vollständiger Ausfall der Funktion z. B. während einer kritischen Verkehrssituation schwerwiegende Folgen haben kann. Fail-Operational-Systeme müssen daher redundante Hardware, intelligente Fehlermanagementstrategien und robuste Softwarearchitekturen aufweisen, um trotz Fehlern weiterhin korrekt zu funktionieren.

Die Umsetzung dieser Konzepte erfordert eine hohe Systemverfügbarkeit und Echtzeitfähigkeit. Autonome Fahrzeuge müssen sicherheitsrelevante Informationen innerhalb von Millisekunden erfassen, verarbeiten und darauf reagieren können. Dies ist eine Grundvoraussetzung, um in komplexen und dynamischen Verkehrssituationen zuverlässig und sicher agieren zu können.

Zusätzlich steigen mit den Fail-Operational-Anforderungen die Herausforderungen an die Systemarchitektur, insbesondere hinsichtlich Redundanz, Fehlerdiagnose und Wiederherstellungsmechanismen. Es gilt, eine Balance zwischen Kosten, Komplexität und Sicherheitsniveau zu finden, die den speziellen Anforderungen autonomer Fahrsysteme gerecht wird.

Insgesamt sind Fail-Safe- und Fail-Operational-Konzepte zentrale Bausteine, um die Funktionalität, Sicherheit und Zuverlässigkeit intelligenter und autonomer Fahrzeuge sicherzustellen.

2.4.6 V2X-Kommunikation: Vernetzung als Schlüssel zur funktionalen Sicherheit und Cybersecurity

Die zunehmende Konnektivität von Fahrzeugen durch Vehicle-to-Everything-(V2X-)Kommunikation erweitert die Möglichkeiten und Anforderungen an die Sicherheit von E/E-Systemen erheblich. V2X ermöglicht die Kommunikation nicht nur zwischen Fahrzeugen (V2V), sondern auch mit Infrastruktur (V2I), Fußgängern (V2P) und weiteren Verkehrsteilnehmern, was eine umfassende Vernetzung im Verkehrsraum schafft.

Durch den erweiterten Informationsaustausch verbessert V2X die Situationsbewertung und unterstützt damit die Fahrentscheidungen autonomer und assistierter Systeme. Dies trägt maßgeblich zur funktionalen Sicherheit bei, da kritische Verkehrssituationen frühzeitig erkannt und vermieden werden können. Ebenso unterstützt V2X die Erfüllung der

Anforderungen aus der ISO/PAS 21448 (SOTIF), indem unsichere Umgebungszustände durch zusätzliche externe Datenquellen besser erkannt und bewertet werden.

Gleichzeitig führt die Öffnung der Kommunikationsschnittstellen zu neuen und erweiterten Angriffsflächen für Cyberbedrohungen. Daher sind umfassende und robuste Cybersecurity-Maßnahmen unverzichtbar, um die Integrität, Vertraulichkeit und Verfügbarkeit der Daten sicherzustellen. Dies umfasst u. a. die Verschlüsselung der Datenübertragung, Authentifizierungsmechanismen zur Verifizierung der Kommunikationspartner sowie Echtzeitschutz vor Manipulationen und Angriffen.

Die Integration von V2X-Kommunikation erfordert daher ein ganzheitliches Sicherheitskonzept, das sowohl funktionale Sicherheit als auch Cybersecurity in den Entwicklungs- und Betriebsprozessen berücksichtigt. Nur so kann die Technologie ihr volles Potenzial entfalten und gleichzeitig den hohen Sicherheitsanforderungen im vernetzten Straßenverkehr gerecht werden.

2.4.7 Datenintegrität und Datenschutz: Grundlage für Vertrauen und Sicherheit im vernetzten Fahrzeug

Die Gewährleistung der Datenintegrität stellt einen essenziellen Baustein für die Sicherheit und Zuverlässigkeit moderner E/E-Systeme in Fahrzeugen dar. Intelligente Fahrzeuge erfassen und verarbeiten heute eine Vielzahl personenbezogener Daten, darunter Standortinformationen, Fahrverhalten, biometrische Daten und weitere sensible Informationen.

Diese umfangreiche Datenerhebung führt zu hohen Anforderungen an die Integrität, Vertrauenswürdigkeit und Vertraulichkeit der Daten. Datenintegrität bedeutet, dass die erfassten Informationen während der Erfassung, Übertragung, Speicherung und Verarbeitung unverfälscht und vollständig bleiben müssen. Eine Verletzung der Datenintegrität kann zu Fehlentscheidungen autonomer Systeme oder zu Sicherheitslücken führen, die das Fahrverhalten oder die Privatsphäre der Nutzer gefährden.

Parallel dazu ist der Datenschutz ein zentrales Anliegen, das durch gesetzliche Vorgaben wie die Datenschutz-Grundverordnung (DSGVO) in Europa konkret geregelt ist. Diese umfasst Maßnahmen zur Anonymisierung und Pseudonymisierung personenbezogener Daten sowie den Schutz vor unautorisiertem Zugriff, Missbrauch und unerlaubter Weitergabe. Die Einhaltung dieser Anforderungen ist nicht nur rechtlich verbindlich, sondern auch grundlegend, um das Vertrauen der Nutzer in vernetzte Fahrzeugtechnologien zu sichern.

Datenintegrität und Datenschutz sind daher integrale Bestandteile des Sicherheitskonzepts moderner Fahrzeuge und müssen im Entwicklungs-

prozess, bei der Systemarchitektur, bei der Cybersecurity sowie im operativen Betrieb stringent berücksichtigt werden. Nur so kann ein sicherer und vertrauenswürdiger Umgang mit sensiblen Daten gewährleistet werden, der die komplexen Anforderungen des vernetzten Fahrzeugs erfüllt.

2.5 Die Operational Design Domain

Das sichere und zuverlässige Funktionieren automatisierter Fahrfunktionen hängt maßgeblich davon ab, unter welchen Bedingungen sie eingesetzt werden. Genau hier setzt das Konzept der Operational Design Domain (ODD) an: ein zentrales Element für die Entwicklung, Bewertung und Zulassung moderner Fahrerassistenzsysteme.

ODD definiert einfach gesagt den »Einsatzbereich« eines automatisierten Systems bzw. den Bereich, in dem ein autonomes Fahrzeug sicher und zuverlässig funktionieren soll. Dazu gehören beispielsweise Wetterbedingungen, Straßenarten, Verkehrsregeln, Geschwindigkeitsbereiche oder auch spezifische Infrastrukturanforderungen.

Dieser Abschnitt beleuchtet den Zweck und die Bedeutung der ODD im Kontext von ADAS und autonomen Fahrfunktionen. Es wird aufgezeigt, wie ODDs definiert, dokumentiert und in den Entwicklungsprozess integriert werden. Zudem werden verschiedene ODD-Definitionen aus Normen und der Praxis vorgestellt und die Herausforderungen bei der Abgrenzung und Validierung diskutiert. Ziel ist es, ein klares Verständnis dafür zu vermitteln, warum die ODD ein Schlüssel zur sicheren und nachvollziehbaren Automatisierung im Fahrzeug ist.

2.5.1 Zweck und Bedeutung der ODD

Durch die präzise Definition, wo und unter welchen Bedingungen ein Smart Car sicher und zuverlässig betrieben werden kann, erhöht sich die Verkehrssicherheit. Indem die Grenzen der Operational Design Domain klar festgelegt werden, lassen sich Entwicklung, Validierung und der spätere Einsatz autonomer Fahrzeuge gezielt steuern und absichern.

Die ODD beschreibt dabei nicht nur, in welchen geografischen Regionen ein System eingesetzt werden darf, sondern berücksichtigt eine Vielzahl von Einflussfaktoren. Dazu zählen unter anderem:

- Geografische Grenzen: Bestimmt, in welchen Regionen oder auf welchen Straßentypen das System aktiviert werden darf.
- Umgebungsbedingungen: Legt fest, bei welchen Witterungsverhältnissen (z. B. Regen, Schnee, Nebel, starke Sonnenblendung) das System sicher funktioniert. Die geografischen Einschränkungen können

durch die Verfügbarkeit von detaillierten Karten, GPS-Signalstärke oder spezifische Infrastrukturanforderungen bestimmt werden.
- Verkehrsdichte und -teilnehmer: Definiert, welche Verkehrssituationen und Arten von Verkehrsteilnehmern (z. B. Fußgänger, Radfahrer) berücksichtigt werden müssen. Es können auch spezifische Regeln und Vorschriften herangezogen werden, die in verschiedenen Verkehrsumgebungen gelten.
- Infrastruktur: Bezieht sich auf die benötigte Straßenausstattung, Markierungen, Beschilderungen oder digitale Infrastruktur.
- Szenarien verschiedener Situationen: Umfasst typische und außergewöhnliche Verkehrssituationen, die das System erkennen und bewältigen muss.
- Geschwindigkeitsbereiche: ODD legt die zulässige Geschwindigkeit des autonomen Fahrzeugs innerhalb bestimmter Bereiche fest. Dies kann z. B. eine Begrenzung auf Autobahnen oder eine Anpassung der Geschwindigkeit in Wohngebieten umfassen.

Durch die konsequente Berücksichtigung dieser Aspekte ermöglicht die ODD eine realistische Einschätzung der Fähigkeiten und Grenzen automatisierter Fahrfunktionen. Sie schafft Transparenz für Entwickler, Zulassungsbehörden und Anwender und bildet die Grundlage für eine sichere Integration autonomer Systeme in den Straßenverkehr.

Die Definition der ODD ist wichtig, um die Grenzen der Fähigkeiten eines autonomen Fahrzeugs zu klären und sicherzustellen, dass es nur in den Bereichen betrieben wird, in denen es in der Lage ist, sicher zu funktionieren. Die Festlegung der ODD erfolgt in der Regel durch den Fahrzeughersteller oder die Betreiberfirma des autonomen Fahrzeugs und kann je nach technologischer Entwicklung und regulatorischen Vorgaben angepasst werden.

Die ODD wird vom OEM definiert und variiert je nach Fahrzeugtyp und Einsatzzweck. Einige autonome Fahrzeuge können beispielsweise nur auf Autobahnen oder in bestimmten Stadtgebieten fahren, während andere in der Lage sind, in allen Verkehrssituationen zu navigieren. Die ODD wird auch von den Regulierungsbehörden berücksichtigt, um sicherzustellen, dass autonome Fahrzeuge nur in Situationen eingesetzt werden, in denen sie sicher und zuverlässig funktionieren können. Die ODD kann sich im Laufe der Zeit ändern, da neue Technologien entwickelt werden und sich die Verkehrsbedingungen ändern. Die funktionale Sicherheit ist von grundlegender Bedeutung für die Entwicklung von Vertrauen und Akzeptanz von vernetzten und autonomen Fahrzeugen und ihren automatisierten Fahrsystemen, um den Einsatz des autonomen Fahrens zu ermöglichen. Die Sicherheit von autonomen Fahrzeu-

gen hat zwei Aspekte: das sichere Design und die sichere Nutzung des Systems. Um eine sichere Nutzung des Systems zu gewährleisten, ist es wichtig, den Anwendern das Wissen über die wahren Fähigkeiten und Grenzen des automatisierten Fahrsystems zu vermitteln, um einen Missbrauch des Systems zu verhindern.

Zum Beispiel kann die ODD ein automatisches Spurhaltesystem – Automated Lane Keeping System (ALKS) – umfassen. Es können auch Systeme des automatisierten Fahrens mit niedriger Geschwindigkeit (Low-Speed Automated Driving (LSAD) Systems), wie Pods und Shuttles, in städtischen Gebieten mit vordefinierten Routen und Fußgängern bzw. Radfahrern definiert werden. Auf der anderen Seite kann die ODD für ein Autobahn-Chauffeur-System eine vierspurige geteilte Autobahn und nur trockene Witterungsbedingungen umfassen. Die Arten von Szenarien, mit denen ein Fahrzeug konfrontiert werden kann, hängen von seiner definierten ODD ab, was für jede Sicherheitsbewertung und Szenario-Identifikation grundlegend ist.

Eine formale Definition von ODD gemäß SAE J3016 [SAE J3016:2021] lautet: »Betrieblicher Einsatzbereich (ODD) Die Betriebsbedingungen, unter denen ein bestimmtes System zur Fahrautomatisierung oder eine entsprechende Funktion dafür ausgelegt ist zu funktionieren – einschließlich, aber nicht beschränkt auf, Einschränkungen in Bezug auf Umwelt, Geografie, Tageszeit sowie die erforderliche Anwesenheit oder Abwesenheit bestimmter Verkehrs- oder Straßenmerkmale.«

2.5.2 Standards im Kontext von ODD

Um der Automobilindustrie die gemeinsame Nutzung, den Vergleich und die Wiederverwendung von ODD-Definitionen zu ermöglichen, besteht ein deutlicher Bedarf an Standards. Diese sollen Fahrzeugherstellern sowohl eine Anleitung zu den relevanten Attributen für die ODD-Definition als auch ein einheitliches Format zur Beschreibung der ODD bereitstellen.

Der von British Standards Institution (BSI) in Großbritannien entwickelte Standard PAS 1883 [PAS 1883:2020] ist ein richtiger Schritt in diese Richtung, denn er bietet ein Klassifikationsschema für ODD. Ergänzend dazu greift ISO 34503 [ISO 34503:2023] diese Taxonomie auf und stellt ein hochrangiges Definitionsformat für ODD bereit.

Obwohl diese Standardisierungsaktivitäten wichtige Bedürfnisse der Branche ansprechen, besteht in der Automobilbranche noch eine Lücke in Bezug auf ein ODD-Definitionsformat, das speziell für Simulationen geeignet ist. Der britische Leitfaden PAS 1883 richtet sich an die Entwicklung autonomer Fahrzeuge und bietet Empfehlungen für die Entwick-

lung, Prüfung und Zertifizierung solcher Systeme. Er deckt verschiedene Aspekte ab, darunter die Definition von Betriebsbereichen, Risikobewertung, Sicherheitsanforderungen und Prüfmethoden. Dabei ist PAS 1883 nicht verbindlich, sondern als Orientierungshilfe für Hersteller, Regulierungsbehörden und andere Interessengruppen gedacht, um die Entwicklung autonomer Fahrzeuge sicherer und zuverlässiger zu gestalten.

Die Association for Standardisation Automation and Measuring Systems (ASAM) ist eine noch sehr junge Standardisierungsinitiative (ASAM e. V.) in Deutschland, in der Experten von OEMs, Tier-1, Toolanbietern, Ingenieurdienstleister und Forschungsinstituten zusammenarbeiten, um Entwicklungs- und Testsysteme für die Automobilindustrie gemeinsam zu standardisieren. Ziel der Standardisierungsorganisation ASAM e. V. ist es, ein Format bereitzustellen, das in der Lage ist, eine definierte Operational Design Domain für vernetzte automatisierte Fahrzeuge darzustellen.

Das von der Standardisierungsorganisation ASAM e. V. entwickelte »ASAM OpenODD« ist ein maschineninterpretierbares Format einer abstrakten ODD-Spezifikation in einer klar definierten Syntax und Semantik, mit der es möglich ist, erforderliche Analysen zu interpretieren und durchzuführen [ASAM OpenODD:2024]. Mit diesem Format wird eine ODD-Beschreibung austauschbar, vergleichbar und verarbeitbar. Dieses neue Format ermöglicht z. B. den folgenden Anwendungsfall:

Eine Stadt definiert eine ODD für ihre Innenstadt und verwendet dabei das OpenODD-Format von ASAM. Nun können Automobilhersteller die in ASAM OpenODD definierten Fahrzeug-ODDs mit ihrem Fahrzeug vergleichen, um herauszufinden, ob es in dieser bestimmten Innenstadt fahren darf. Für die Zulassungsstellen ist dies ein riesengroßer Vorteil, weil sie ODDs definieren können, anhand derer sie die ODD des Fahrzeugs überprüfen können.

Ein zweiter Anwendungsfall, der die Entwicklung von ADAS- und AD-Systemen unterstützt, ist die Verwendung der ODD zur Definition der Testfälle, die zur Validierung des Fahrzeugs erforderlich sind. Die Anwendung einer ODD trägt dazu bei, die begrenzten Validierungsressourcen auf die wirklich benötigten Szenarien zu konzentrieren.

2.5.3 ODD-Formate, Simulation und Sicherheit im autonomen Fahren

Operational Design Domains müssen so beschrieben werden, dass sie sowohl für die Entwicklung als auch für die virtuelle Validierung automatisierter Fahrfunktionen maschinell interpretierbar sind. Ein zentrales Format dafür ist ASAM OpenODD, das eine standardisierte, strukturierte und semantisch klare Beschreibung von ODDs ermöglicht. Die darin

enthaltenen Informationen leiten sich aus einer abstrakten Fahrzeug-ODD ab und dienen als Grundlage für Simulation, Szenariogenerierung, Testausführung und Sicherheitsbewertung.

Damit eine solche abstrakte ODD-Beschreibung für die Simulation und das Post-Processing nutzbar ist, muss das zugrunde liegende Format folgende Anforderungen erfüllen:

- Durchsuchbarkeit: Strukturierte Inhalte ermöglichen gezielte Abfragen und Filterungen (z. B. für Testfallgenerierung).
- Austauschbarkeit: Standardisierte Datenformate erleichtern den Austausch zwischen verschiedenen Tools und Partnern.
- Erweiterbarkeit: Neue ODD-Merkmale oder Szenarien können flexibel ergänzt werden, ohne bestehende Strukturen zu brechen.
- Maschinenlesbarkeit: Die ODD muss von Software eindeutig interpretierbar sein (z. B. für automatische Testkataloge).
- Messbarkeit und Verifizierbarkeit: Die Inhalte müssen objektiv mess- und überprüfbar sein, um nachweisbare Sicherheitsbewertungen zu ermöglichen.
- Menschliche Lesbarkeit: Eine strukturierte Darstellung in (ggf. eingeschränkter) natürlicher Sprache unterstützt Validierungs- und Reviewprozesse.

2.5.3.1 Sicherheitsmechanismen für den ODD-Betrieb

In einem Szenario mit erweiterter Fahrerassistenz oder autonomem Fahren müssen verschiedene Sicherheitsmechanismen in das Design einbezogen werden, um eine sichere Nutzung zu gewährleisten. Dazu gehören z. B. Rückstellung (Reset), Backup-Kontrolle oder Notfall-Parkmöglichkeiten am Straßenrand. Hier sind einige Beispiele und Referenzen:

- Redundante Systeme und Backup-Systeme: Fahrzeuge mit erweiterter Fahrerassistenz oder autonome Fahrzeuge verfügen häufig über redundante Systeme, um die Funktionsfähigkeit auch im Falle von Fehlern oder Störungen sicherzustellen. Redundante Sensoren, Rechensysteme und Aktuatoren können dazu beitragen, die Auswirkungen eines einzelnen Fehlerpunkts zu minimieren.
- Ausfallsichere Modi und Notfallstopp: Autonome Fahrzeuge sollten über ausfallsichere Modi verfügen, die in Notfallsituationen aktiviert werden können. Diese Modi können sichere Stoppprozesse umfassen, wie z. B. ein kontrolliertes Anhalten und das Aktivieren der Feststellbremse, um potenzielle Gefahren zu minimieren.
- Fernüberwachung und -steuerung: In einigen Fällen können autonome Fahrzeuge von dafür ausgebildetem Personal fernüberwacht und gesteuert werden. Dadurch ist ein Eingreifen in Notfallsituationen

oder bei unvorhergesehenen Umständen möglich, die das Fahrzeug autonom nicht bewältigen kann. Das Bundesgesetzblatt zur Verordnung über Ausnahmen von straßenverkehrsrechtlichen Vorschriften für ferngelenkte Kraftfahrzeuge (Straßenverkehr-Fernlenk-Verordnung, StVFernLV) legt dazu den gesetzlichen Rahmen fest.

Zur Fernüberwachung und -steuerung wurden sechs Fernüberwachungsmodi definiert:

- Notfall-Parkmöglichkeiten am Straßenrand: Autonome Fahrzeuge können so programmiert werden, dass sie sichere Orte zum Notparken erkennen, wenn menschliches Eingreifen notwendig wird oder Systemfehler auftreten. So wird gewährleistet, dass das Fahrzeug sicher abseits der Fahrbahn geparkt wird – Unfälle oder Verkehrsbehinderungen werden vermindert.
- Rückstellung (Reset) und Diagnoseverfahren: Autonome Fahrzeuge können sich bei Software- oder Systemfehlern durch definierte Reset-Methoden selbst stabilisieren. Darüber hinaus können Diagnoseverfahren kontinuierlich den Zustand überwachen und erkennen potenzielle Störungen frühzeitig. Damit unterstützen sie eine (teil-)automatisierte Fehlerbehebung, bevor Sicherheitsrisiken entstehen.
- Fernübernahme für Shuttle- oder Parkfall: In bestimmten Anwendungsfällen – etwa bei Shuttle, Logistik- oder Parkrobotern – übernimmt ein Remote-Operator temporär die Steuerung. Die KI bereitet Übergaben vor und übergibt auf Kommando eines Menschen die Kontrolle, um flexibel auf komplexe Situationen reagieren zu können.
- Sicherheits-Standby (Safe Hold Mode): Bei Ausfall kritischer Teilsysteme oder Verlust der Kommunikation wechselt das Fahrzeug in einen definierten »Safe Standby«- oder »Safe Hold«-Zustand. Es hält an oder verlangsamt sich kontrolliert, wartet auf Anweisungen – und überträgt eine sichere, passiv koordinierte Funktionsüberwachung an den Remote-Operator.
- Virtueller Assistenzeingriff (Teleassistenz) durch Remote- Operator: Der Betreiber kann über sichere Kommunikationsverbindungen unterstützend eingreifen – z. B. um bei schwierigen Manövern wie Spurwechseln, Einparken oder Hindernisumfahrung assistierend zu steuern, während die KI weiterhin die Kontrolle über Fahrweg, Geschwindigkeit und Umgebung übernimmt.
- Fern-Update und Parametermanagement: Während des Betriebs erlaubt dieser Modus die Fernüberwachung von Softwareversionen, Parametern und Kalibrierungen. Remote-Operatoren können sicherheitsrelevante Updates oder Justierungen vornehmen – etwa bei Sen-

sor-Nachkalibrierung oder Anpassung an neue ODD-Rahmenbedingungen –, ohne dass das Fahrzeug physisch angesteuert werden muss.

Es ist wichtig zu beachten, dass diese Sicherheitsmechanismen bei der Gestaltung autonomer Fahrzeuge berücksichtigt werden, aber ihre konkrete Umsetzung je nach Hersteller und autonomem System variieren kann. Darüber hinaus können Fortschritte in der Technologie und Vorschriften zu kontinuierlichen Verbesserungen der Sicherheitsmechanismen führen.

ODD – Status, Herausforderungen und nächste Schritte

Die Operational Design Domain hat sich als zentrales Konzept für die sichere Entwicklung, Validierung und Zulassung automatisierter Fahrfunktionen etabliert. Sie definiert klar, unter welchen Bedingungen ein System sicher betrieben werden kann, und bildet damit die Grundlage für realistische Leistungsversprechen, nachvollziehbare, belastbare Sicherheitsnachweise und eine effektive Kommunikation zwischen Herstellern, Zulassungsbehörden und Anwendern.

Aktuelle Entwicklungen wie die Standardisierung durch ISO 34503 und die maschinenlesbaren Formate von ASAM OpenODD zeigen, dass die Branche zunehmend auf einheitliche, interoperable und automatisiert verarbeitbare ODD-Beschreibungen setzt. Das erleichtert nicht nur die Wiederverwendung und den Austausch von ODD-Definitionen, sondern schafft auch die Voraussetzung für effiziente Simulationen und virtuelle Tests.

Gleichzeitig besteht die Herausforderung darin, ODDs so präzise und flexibel zu gestalten, dass sie sowohl den regulatorischen Anforderungen als auch den dynamischen Realitäten des Straßenverkehrs gerecht werden. Die Weiterentwicklung von Standards, Methoden und Werkzeugen rund um die ODD wird daher auch in Zukunft ein zentrales Thema für die Branche bleiben. Ohne klare ODD keine sichere Automatisierung.

2.6 Taxonomiestufen für intelligente Straßenfahrzeuge

Im Folgenden werden die wichtigsten Taxonomiestufen vorgestellt, die als Grundlage dienen, intelligente Straßenfahrzeuge systematisch zu klassifizieren und einzuordnen. Dabei werden nicht nur die technischen Hintergründe und Definitionen erläutert, sondern auch die vielfältigen Anwendungsfelder, in denen Taxonomien eine entscheidende Rolle spielen.

Taxonomien bieten ein strukturiertes und einheitliches Vokabular, das Entwickler, Hersteller, Prüfer und Regulierungsbehörden gleichermaßen nutzen, um die komplexen Eigenschaften und Fähigkeiten intelli-

genter Fahrzeuge präzise zu beschreiben. Sie ermöglichen es, unterschiedliche Fahrzeugfunktionen, Automatisierungsgrade und operative Einsatzbereiche klar voneinander abzugrenzen und zu standardisieren.

Durch die Nutzung von Taxonomiestufen können Entwicklungsprozesse besser gesteuert, Sicherheitsanforderungen gezielter definiert und Prüfverfahren effizienter gestaltet werden. Ebenso erleichtern sie die Kommunikation zwischen den Beteiligten im Fahrzeugökosystem sowie die Integration neuer Technologien wie künstliche Intelligenz und Cybersecurity-Maßnahmen.

Die folgenden Abschnitte geben einen detaillierten Einblick, wie Taxonomien als strukturierendes Werkzeug dazu beitragen, intelligente Straßenfahrzeuge nicht nur technologisch, sondern auch im Hinblick auf funktionale Sicherheit, Cybersecurity und die Einhaltung von Normen präzise zu bewerten und weiterzuentwickeln.

2.6.1 Die SAE-J3016-Taxonomie

Taxonomiestufen ermöglichen es, Fahrzeuge und ihre Systeme nach Automatisierungsgrad, Einsatzbereich und technologischer Reife zu klassifizieren. Sie schaffen damit einen klaren Ordnungsrahmen, um die vielfältigen Herausforderungen im Bereich funktionale Sicherheit, Cybersecurity und KI-basierte Entwicklungsprozesse zu adressieren.

International etabliert hat sich insbesondere die SAE-J3016-Taxonomie, die seit dem Jahr 2014 insgesamt sechs Stufen der Fahrzeugautomatisierung definiert – von Level 0 (keine Automatisierung) bis Level 5 (volle Automatisierung). Ergänzend dazu werden moderne Taxonomien um die Kriterien ODD und Automation Readiness erweitert, um die Vielfalt automatisierter Fahrfunktionen und deren Einsatzbedingungen noch differenzierter abzubilden.

Die U.S. National Highway Traffic Safety Administration (NHTSA) hat ihre Autonomiestufen an die SAE J3016 angeglichen. Nachfolgend sind die fünf Stufen aufgeführt, die auf die Automatisierungsstufe 0 folgen (siehe Tabelle 2.2).

Level	Name	ISO/SAE PAS 22736: 2021	ODD: Operational Design Domain DDT: Dynamic Driving Task ADS: Automated Driving System	
		Definition	**Einsatzbereich** **Rolle des Fahrers**	**Dynamische Fahraufgabe** **Rolle des automatisierten Fahrsystems**
0	Keine Fahrzeugautomatisierung	Die Leistung des Fahrers bei der gesamten dynamischen Fahraufgabe, auch wenn sie durch aktive Sicherheitssysteme unterstützt oder verbessert wird.	Der Fahrer übernimmt zu jeder Zeit vollständig die Fahraufgabe (Dynamic Driving Task, DDT).	Falls vorhanden, steuert das Automatisierungssystem das Fahrzeug nicht dauerhaft selbst. Andere Systeme können jedoch Warnungen geben oder in Notfällen kurz eingreifen.
1	Fahrerassistenz	Die anhaltende, auf die jeweilige ODD bezogene Ausführung entweder der seitlichen oder der längs gerichteten Fahrzeugbewegungssteuerung als Teilaufgabe der dynamischen Fahraufgabe (DDT) durch ein Fahrzeugautomatisierungssystem – jedoch nicht beides gleichzeitig – mit der Erwartung, dass der Fahrer den verbleibenden Teil der DDT übernimmt.	Der Fahrer übernimmt jederzeit den Teil der dynamischen Fahraufgabe (DDT), den das Fahrzeugautomatisierungssystem nicht ausführt. Er überwacht das System und greift bei Bedarf ein, um den sicheren Betrieb des Fahrzeugs sicherzustellen. Außerdem entscheidet der Fahrer, ob und wann das Fahrzeugautomatisierungssystem ein- oder ausgeschaltet wird, und führt bei Bedarf oder auf Wunsch sofort die gesamte DDT selbst aus.	**Fahrzeugautomatisierungssystem (wenn aktiviert):** Führt einen Teil der dynamischen Fahraufgabe (DDT) aus, indem es entweder die längs gerichtete oder die seitliche Fahrzeugbewegungssteuerung übernimmt. Es deaktiviert sich sofort, sobald der Fahrer dies anfordert. Das System steuert entweder die Richtung oder die Geschwindigkeit. Auf Wunsch des Fahrers schaltet es sich sofort ab.
2	Teilweise Fahrzeugautomatisierung	Die fortgesetzte ODD-spezifische Ausführung sowohl der seitlichen als auch der längs gerichteten Fahrzeugbewegungssteuerung als Teilaufgaben der dynamischen Fahraufgabe (DDT) durch ein Fahrzeugautomatisierungssystem mit der Erwartung, dass der Fahrer die Objekt- und Ereigniserkennung sowie Reaktion (OEDR) übernimmt und das System überwacht.	Der Fahrer übernimmt jederzeit den verbleibenden Teil der dynamischen Fahraufgabe (DDT), den das Fahrzeugautomatisierungssystem nicht ausführt. Er überwacht das Fahrzeugautomatisierungssystem und greift bei Bedarf ein, um den sicheren Betrieb des Fahrzeugs sicherzustellen. Außerdem entscheidet er, ob und wann das Fahrzeugautomatisierungssystem ein- oder ausgeschaltet wird, und führt sofort die gesamte DDT aus, wenn dies erforderlich oder gewünscht ist.	**Fahrzeugautomatisierungssystem (wenn aktiviert):** Führt einen Teil der dynamischen Fahraufgabe (DDT) aus, indem es sowohl die seitliche als auch die längs gerichtete Fahrzeugbewegungssteuerung übernimmt. Es deaktiviert sich sofort, sobald der Fahrer dies verlangt.
3	Bedingte Fahrzeugautomatisierung	Die kontinuierliche ODD-spezifische Ausführung der gesamten DDT (Dynamic Driving Task) durch ein ADS (Automated Driving System) mit der Erwartung, dass der benutzerbereite Fahrer auf Eingaben des ADS zur Intervention reagiert und ebenfalls angemessen auf systemrelevante Ausfälle in anderen Fahrzeugsystemen, die die DDT-Leistung beeinträchtigen, reagiert.	**ADS (wenn nicht aktiviert):** Erlaubt die Aktivierung und den Betrieb nur innerhalb seiner Operational Design Domain (ODD). **ADS (wenn aktiviert):** Führt die gesamte dynamische Fahraufgabe (DDT) innerhalb seiner ODD durch. Erkennt frühzeitig, ob die ODD-Grenzen bald überschritten werden, und fordert bei Bedarf rechtzeitig den DDT-Rückfall-bereiten Benutzer zur Intervention auf. Erkennt systemrelevante Ausfälle, die die DDT-Leistung beeinträchtigen, und fordert bei Bedarf ebenfalls rechtzeitig zur Intervention auf. Deaktiviert sich zu einem angemessenen Zeitpunkt nach einer Aufforderung zur Intervention oder sofort auf Benutzerwunsch.	**ADS (wenn nicht aktiviert):** Erlaubt die Aktivierung / den Betrieb nur innerhalb seiner ODD (Operational Design Domain). **ADS (wenn aktiviert):** Führt die gesamte DDT innerhalb seiner ODD durch. Entscheidet, ob die ODD-Grenzen bald überschritten werden, und gibt ggf. rechtzeitig eine Aufforderung zur Intervention an den DDT-Rückfall-bereiten Benutzer aus. Ermittelt, ob ein systemrelevanter Ausfall des ADS die DDT-Leistung betrifft, und gibt ggf. rechtzeitig eine Aufforderung zur Intervention an den DDT-Rückfall-bereiten Benutzer aus. Deaktiviert sich zu einem angemessenen Zeitpunkt nach Ausgabe einer Aufforderung zur Intervention. Deaktiviert sich sofort auf Benutzeranfrage.

→

Level	Name	ISO/SAE PAS 22736: 2021	ODD: Operational Design Domain DDT: Dynamic Driving Task ADS: Automated Driving System	
		Definition	**Einsatzbereich** **Rolle des Fahrers**	**Dynamische Fahraufgabe** **Rolle des automatisierten Fahrsystems**
4	Hohe Fahrzeugautomatisierung	Die fortlaufende ODD-spezifische Ausführung der gesamten DDT (Dynamic Driving Task) und des DDT-Fallbacks durch ein ADS (Automated Driving System) ohne die Erwartung, dass ein Benutzer auf eine Aufforderung zur Intervention reagieren wird.	**Fahrer/Disponent (wenn das ADS nicht aktiviert ist):** Überprüft den betriebsbereiten Zustand des mit ADS ausgestatteten Fahrzeugs. Entscheidet, ob das ADS aktiviert werden soll, und wird zum Passagier, sobald das ADS aktiviert ist – jedoch nur, wenn er sich physisch im Fahrzeug befindet. **Passagier/Disponent (wenn das ADS aktiviert ist):** Muss die dynamische Fahraufgabe (DDT) oder den DDT-Fallback nicht durchführen. Muss nicht entscheiden, ob und wie ein minimaler Risikozustand erreicht werden kann. Kann die DDT übernehmen, wenn das ADS seine ODD-Grenze erreicht hat. Kann die Deaktivierung des ADS anfordern und wird nach einer angeforderten Deaktivierung wieder zum Fahrer.	**ADS (wenn nicht aktiviert):** Erlaubt die Aktivierung und den Betrieb nur innerhalb seiner ODD. **ADS (wenn aktiviert):** Führt die gesamte dynamische Fahraufgabe (DDT) innerhalb seiner ODD durch. Kann den Passagier auffordern, die Fahrzeugbedienung wieder zu übernehmen, wenn eine ODD-Grenze erreicht wird. Führt den DDT-Fallback durch und wechselt automatisch in einen minimalen Risikozustand, wenn: ■ ein systemrelevanter Ausfall der DDT auftritt, ■ ein Benutzer eine minimale Risikozustandsherstellung verlangt, ■ das Fahrzeug kurz davor steht, seine ODD zu verlassen. Deaktiviert sich ggf. erst, nachdem: ■ ein minimaler Risikozustand erreicht ist oder ■ ein Fahrer die dynamische Fahraufgabe übernimmt. Kann eine vom Benutzer angeforderte Deaktivierung verzögern.
5	Vollständige Fahrzeugautomatisierung	Die fortlaufende und uneingeschränkte Ausführung der gesamten DDT und des DDT-Fallbacks durch ein ADS (Automated Driving System), unabhängig von ODD und ohne die Erwartung, dass ein Benutzer auf eine Aufforderung zur Intervention reagiert.	**Fahrer/Disponent (wenn das ADS nicht aktiviert ist):** Überprüft den betriebsbereiten Zustand des mit ADS ausgestatteten Fahrzeugs. Entscheidet, ob das ADS aktiviert werden soll, und wird zum Passagier, sobald das ADS aktiviert ist – vorausgesetzt, er ist physisch im Fahrzeug anwesend. **Passagier/Disponent (bei aktiviertem ADS):** Muss weder die dynamische Fahraufgabe (DDT) oder den DDT-Fallback durchführen. Trifft keine Entscheidung über das Erreichen eines minimalen Risikozustand. Kann die Deaktivierung des ADS anfordern und danach einen minimalen Risikozustand herstellen. Kann nach der Deaktivierung wieder zum Fahrer werden.	**ADS (wenn nicht aktiviert):** Erlaubt die Aktivierung des ADS unter allen Bedingungen, die von einem Fahrer handhabbar sind. **ADS (wenn aktiviert):** Führt die gesamte dynamische Fahraufgabe (DDT) durch. Führt den DDT-Fallback durch und wechselt automatisch in einen minimalen Risikozustand, wenn: ■ ein systemrelevanter Ausfall des DDT auftritt oder ■ ein Benutzer die Herstellung eines minimalen Risikozustands anfordert. Deaktiviert sich ggf. erst, nachdem: ■ ein minimaler Risikozustand erreicht wurde oder ■ ein Fahrer die DDT übernimmt. Kann eine vom Benutzer angeforderte Deaktivierung verzögern.

Tab. 2.2 *Taxonomie und Definitionen für Begriffe im Zusammenhang mit Fahrerassistenzsystemen*

Die zum Zeitpunkt der Erstellung dieses Buches eingesetzten autonomen Taxis (Robotaxis) in den USA sind reale Beispiele für SAE-Level 4-Systeme. Obwohl diese Fahrzeuge voll autonom innerhalb ihrer ODD agieren, erreichen sie noch nicht SAE-Level 5. Sie dürfen nur in spezifischen geografischen Zonen fahren und sind bei bestimmten Wetterbe-

dingungen nicht einsatzfähig. Bei unklaren Verkehrssituationen (Straßenarbeiten, Unfällen) müssen sie mitunter überwacht oder gestoppt werden. Sie markieren jedoch einen bedeutenden Fortschritt in der praktischen Umsetzung hochautomatisierter Mobilitätskonzepte.

2.6.2 Details zu den Taxonomiestufen

- **Stufe 1 (Assistiertes Fahren)**

  Fahrerassistenzsysteme unterstützen den Fahrer bei Fahraufgaben wie Lenken, Bremsen oder Beschleunigen – beispielsweise durch Warnfunktionen wie ein vibrierendes Lenkrad, das vor Fahrspurverlust warnt, oder durch Rückfahrkameras. Der Fahrer behält stets die vollständige Kontrolle über das Fahrzeug und muss aktiv am Fahrgeschehen teilnehmen.

- **Stufe 2 (Teilautomatisiertes Fahren)**

  Das Fahrerassistenzsystem übernimmt selbstständig bestimmte Aufgaben, wie Lenken oder Beschleunigen, indem es beispielsweise automatisch die Geschwindigkeit des Fahrzeugs anpasst, um Abstand zu halten. Das Fahrzeug kann z. B. innerhalb der Fahrspur bleiben und ggf. selbstständig lenken. Der Fahrer muss jedoch die Hände am Lenkrad behalten und kann das Lenken übernehmen, wenn nötig. Das System unterstützt den Fahrer beim sicheren Wechseln der Fahrspur. Der Fahrer muss dennoch den Spurwechsel aktiv initiieren und überwachen.

- **Stufe 3 (Bedingt automatisiertes Fahren)**

  Unter definierten Bedingungen, wie beispielsweise eine Autobahn oder ein Parkplatz, kann das Fahrzeug Aufgaben übernehmen, wie das Lenken oder Beschleunigen bzw. das Einparken des Fahrzeugs. Das Fahrzeug übernimmt bestimmte Aufgaben, es erfordert jedoch weiterhin die aktive Beteiligung des Fahrers, der jederzeit eingreifen kann.

- **Stufe 4 (Hochautomatisiertes Fahren)**

  Ein bedingt vollautomatisiertes Fahrsystem kann unter bestimmten, klar definierten Bedingungen alle Fahraufgaben übernehmen und die Fahrumgebung überwachen. Unter diesen Umständen ist das bedingt vollautomatisierte Fahrsystem so zuverlässig, dass der Fahrer nicht mehr bereit sein muss, jederzeit eingreifen zu müssen. Das System ist so zuverlässig, dass es bei Einhaltung der definierten Bedingungen ohne menschliche Rückfallebene auskommt. Außerhalb dieser Bedingungen kann das Fahrzeug den Fahrer auffordern, die Kontrolle zu übernehmen, oder das Fahrzeug selbstständig anhalten.

- **Stufe 5 (Vollautomatisiertes Fahren)**
  Aufgrund der hohen Komplexität und facettenreichen Herausforderungen entstehen zukünftige Fahrzeuge auf Level 5 nach SAE J3016 nicht mit einem Paukenschlag, sondern in einer Reihe von Iterationen. Ein Level-5-Fahrzeug ist ein Fahrzeug, das eine Kombination aus Sensoren, Kameras, Radar und KI einsetzt, um sich ohne menschlichen Fahrer fortzubewegen. Um als vollständig autonom zu gelten, muss ein Fahrzeug in der Lage sein, ohne menschliches Eingreifen auf Straßen, die nicht für seine Verwendung geeignet sind, zu einem vorgegebenen Ziel zu navigieren.

Taxonomiestufen als verbindendes Fundament

Die Entwicklung vollautomatisierter Fahrzeuge vereint unterschiedlichste Akteure: Fahrzeughersteller, Software- und Hardwareanbieter, Halbleiterproduzenten und Betreiber der öffentlichen Infrastruktur. Diese Mischung fordert in vielen Bereichen präzise Abstimmungen und reibungslose Zusammenarbeit. Besonders das Zusammenspiel von funktionaler Sicherheit und Cybersecurity – mit überlappenden Normen und Anforderungen – verlangt klare Orientierungspunkte und sehr gute Koordination. Hier leisten Taxonomiestufen einen entscheidenden Beitrag: Sie schaffen ein gemeinsames Verständnis, erleichtern die Identifikation spezifischer Risiken und ermöglichen die gezielte Ableitung von Schutzmaßnahmen. Zudem unterstützen sie die Integration neuer Technologien wie KI in den Entwicklungsprozess. So bilden Taxonomiestufen nicht nur ein gemeinsames technisches Vokabular, sondern auch die Basis, um neue Betriebsformen – etwa die Fernlenkung – in rechtlich verbindliche Rahmen wie die StVFernLV einzubetten.

2.7 Ferngelenkte Fahrzeuge und das neue StVFernLV

Mit der Verabschiedung der neuen Verordnung über den Betrieb ferngelenkter Fahrzeuge (StVFernLV) im Juli 2025 hat der Gesetzgeber in Deutschland einen rechtlichen Rahmen geschaffen, um Teleoperation von Kraftfahrzeugen auf öffentlichen Straßen zu ermöglichen. Die Verordnung erlaubt unter bestimmten Voraussetzungen den Einsatz von Fahrzeugen, die durch eine fernsteuernde Person gelenkt werden – ein Meilenstein für automatisierte Mobilitätskonzepte, insbesondere in urbanen Logistik- und Shuttle-Anwendungen.

Dieser Abschnitt fasst die zentralen Anforderungen der StVFernLV zusammen und zeigt anhand eines Projektbeispiels der Firma Drivesmart, wie die Umsetzung in der industriellen Praxis aussehen kann.

2.7.1 Rechtlicher Rahmen der StVFernLV

Die Verordnung über den Betrieb ferngelenkter Fahrzeuge im öffentlichen Straßenverkehr (StVFernLV), die 2025 in Kraft trat, stellt erstmals einen expliziten gesetzlichen Rahmen für die Zulassung und Nutzung ferngelenkter Fahrzeuge in Deutschland bereit. Ziel der Verordnung ist es, den sicheren Einsatz von Kraftfahrzeugen, die nicht durch eine physisch anwesende Person gesteuert werden, sondern durch eine Fernlenkeinrichtung, rechtssicher zu ermöglichen. Die StVFernLV unterscheidet zwei zentrale Genehmigungsarten:

1. Betriebserlaubnis für das ferngelenkte Kraftfahrzeug
2. Betriebsbereichsgenehmigung

2.7.1.1 Betriebserlaubnis für das ferngelenkte Kraftfahrzeug (§ 4 StVFernLV)

Diese Genehmigung wird vom Kraftfahrt-Bundesamt (KBA) erteilt und betrifft das Fahrzeug selbst sowie dessen technische Ausstattung zur Fernlenkung. Sie stellt sicher, dass das Fahrzeug grundsätzlich technisch geeignet ist, ferngelenkt betrieben zu werden. Die Betriebserlaubnis ist also die formale Voraussetzung dafür, dass ein Fahrzeug überhaupt mit einer Fernsteuerung im Straßenverkehr genutzt werden darf. Dafür sind insbesondere folgende Punkte entscheidend:

- Das Gesamtsystem zum Fernlenken muss den technischen und funktionalen Anforderungen der Anlage 1 zur Verordnung entsprechen. Diese umfassen unter anderem funktionale Sicherheit, technische Redundanz, Kommunikationssicherheit sowie Anforderungen an die Fernsteuerungsarchitektur.
- Das Fahrzeug muss bereits eine gültige Betriebserlaubnis besitzen, etwa eine EU-Typgenehmigung gemäß der Verordnung (EU) 2018/858 oder eine nationale Betriebserlaubnis nach Straßenverkehrs-Zulassungs-Ordnung (StVZO).
- Durch den Einbau der Fernlenkausrüstung darf das Fahrzeug keine Abweichungen von für die Verkehrssicherheit relevanten Bestimmungen europäischer Rechtsakte oder der StVZO aufweisen.
- Der Antragsteller muss ein umfassendes Sicherheitskonzept vorlegen, das sowohl funktionale Sicherheit (Safety) als auch IT-Sicherheit (Cybersecurity) berücksichtigt. Dieses Konzept muss auch Wartungsinformationen und Schutzmaßnahmen gegen unbefugten Zugriff enthalten.

- Zusätzlich ist eine Verpflichtung zur regelmäßigen Berichterstattung über den Betrieb, insbesondere über sicherheitsrelevante Vorfälle, nachzuweisen.

2.7.1.2 Betriebsbereichsgenehmigung (§ 7 StVFernLV)

Diese Genehmigung betrifft den geplanten Einsatzbereich des ferngelenkten Fahrzeugs im öffentlichen Verkehrsraum und wird durch die jeweils zuständige Landesbehörde erteilt. Die Genehmigung bezieht sich auf konkrete räumliche und betriebliche Rahmenbedingungen, innerhalb derer das Fahrzeug ferngelenkt betrieben werden darf.

Im Gegensatz zur allgemeinen Betriebserlaubnis liegt der Fokus hier weniger auf der technischen Reife des Fahrzeugs, sondern auf den sicherheitsrelevanten Aspekten des vorgesehenen Betriebsumfelds. Für eine erfolgreiche Erteilung sind folgende Voraussetzungen im Detail zu erfüllen:

Zunächst ist eine präzise Definition des Betriebsbereichs erforderlich. Dies umfasst die geografische Eingrenzung (z. B. bestimmte Stadtteile, Teststrecken, Industriegebiete), zeitliche Einschränkungen (z. B. nur werktags, nur nachts) sowie betriebliche Rahmenbedingungen (z. B. nur mit Begleitfahrzeug, nur in Schrittgeschwindigkeit). Der Betriebsbereich muss so gewählt sein, dass eine sichere Fernlenkung unter realistischen Bedingungen gewährleistet werden kann.

Darüber hinaus ist eine umfassende Risikobewertung des vorgesehenen Umfelds durchzuführen. Diese Bewertung umfasst unter anderem die Verkehrsdichte, potenzielle Konfliktsituationen mit anderen Verkehrsteilnehmern (Fußgänger, Radfahrer, ÖPNV), Witterungsbedingungen und Sichtverhältnisse. Auf Basis dieser Analyse müssen geeignete Sicherheitsmaßnahmen entwickelt und dokumentiert werden.

Ein zentrales Element ist zudem das Kommunikations- und Notfallmanagementkonzept. Dieses muss sicherstellen, dass während des Betriebs jederzeit eine stabile und manipulationssichere Verbindung zwischen Fahrzeug und Steuerzentrale besteht. Für den Fall eines Verbindungsverlusts oder anderer technischer Störungen sind vordefinierte Sicherheitsreaktionen vorzusehen, etwa ein sicheres Anhalten des Fahrzeugs oder das automatische Verlassen des kritischen Bereichs. Auch Notfallkontakte und Meldeketten sind Bestandteil des Konzepts.

Ergänzend ist der Nachweis zu erbringen, dass alle beteiligten Personen, insbesondere die Fernsteuernden, eine adäquate Schulung absolviert haben. Dies umfasst sowohl den sicheren Umgang mit der Steuerungstechnologie als auch Kenntnisse über rechtliche Rahmenbedingungen, Notfallszenarien und das Verhalten im Mischverkehr.

Die Kombination dieser Maßnahmen stellt sicher, dass ferngelenkte Fahrzeuge nicht nur technisch zuverlässig funktionieren, sondern auch

unter realen Verkehrsbedingungen sicher und verantwortungsvoll eingesetzt werden können. Die Betriebsbereichsgenehmigung stellt somit eine wichtige sicherheitsbezogene Hürde dar, die das Vertrauen in diese neue Technologie stärken soll.

2.7.2 Voraussetzungen für die Betriebsbereichsgenehmigung nach § 7 StVFernLV

Die Betriebsbereichsgenehmigung nach §7 StVFernLV dient der sicherheitlichen Absicherung des geplanten Einsatzgebiets eines ferngelenkten Kraftfahrzeugs im öffentlichen Raum. Während die Betriebserlaubnis (§4) die technische Tauglichkeit des Fahrzeugs und seines Fernlenksystems bestätigt, prüft die zuständige Landesbehörde im Rahmen der Betriebsbereichsgenehmigung, ob das geplante Umfeld und der konkrete Betrieb sicher gestaltet sind. Hierbei müssen mehrere Voraussetzungen umfassend erfüllt sein, die jeweils einer eigenständigen Bewertung und Nachweisführung bedürfen.

2.7.2.1 Definition des Betriebsbereichs

Die genaue Beschreibung des Betriebsbereichs ist die Grundlage jeder Genehmigungsentscheidung. Dabei geht es nicht nur um die geografische Abgrenzung, wie z. B. ein innerstädtisches Quartier, ein Industriepark oder ein Betriebshof, sondern auch um die zeitlichen und betrieblichen Einsatzbedingungen. Zeitliche Einschränkungen können etwa nächtliche Betriebszeiten (z. B. 22:00–6:00 Uhr) oder Einschränkungen auf verkehrsarme Zeiten beinhalten. Betriebliche Aspekte wiederum umfassen Einschränkungen in der Fahrweise (z. B. nur Schritttempo), die Verwendung von Begleitfahrzeugen oder den Einsatz nur unter Aufsicht eines Operators. Die präzise Definition ermöglicht es den Behörden, die Risiken systematisch zu bewerten und die Maßgaben der Genehmigung auf die tatsächliche Nutzung abzustimmen.

2.7.2.2 Risikobewertung des Umfelds

Ein zentrales Element der Genehmigung ist die detaillierte Risikobewertung des vorgesehenen Einsatzgebiets. Diese Bewertung muss aufzeigen, welche potenziellen Gefährdungen durch Verkehrsdichte, Straßenführung, Interaktionen mit anderen Verkehrsteilnehmern (Fußgänger, Radfahrer, Einsatzfahrzeuge), Baustellen oder Witterungsbedingungen entstehen können. Auch infrastrukturelle Besonderheiten – etwa fehlende Abstellflächen, enge Fahrbahnen oder unübersichtliche Kreuzungen – müssen berücksichtigt werden. Die Risikobewertung ist keine rein theoretische Übung, sondern dient als Entscheidungsgrundlage für konkrete Betriebs-

grenzen, Sicherheitsauflagen und technische sowie organisatorische Schutzmaßnahmen. Die Landesbehörde muss nachvollziehen können, dass das Risiko auf ein vertretbares Maß reduziert wurde – nicht nur durch Technik, sondern durch ein ganzheitliches Sicherheitskonzept.

2.7.2.3 Kommunikations- und Notfallmanagementkonzept

Da das Fahrzeug nicht durch eine im Fahrzeug befindliche Person gesteuert wird, ist die Kommunikation zwischen der Fernsteuerstelle (Fernlenkzentrale) und dem Fahrzeug von kritischer Bedeutung. Das Kommunikationskonzept muss daher hohe Anforderungen an Verfügbarkeit, Bandbreite, Latenz und IT-Sicherheit erfüllen. Störungen, Verzögerungen oder gar Unterbrechungen könnten sonst unmittelbar die Verkehrssicherheit gefährden. Das Konzept muss deshalb klare Antworten auf folgende Fragen geben:

- Wie wird eine stabile Verbindung gewährleistet?
- Welche Maßnahmen greifen bei Kommunikationsausfall?
- Wie erkennt das System Störungen frühzeitig?
- Wie wird im Notfall eingegriffen (z. B. automatisches Anhalten, Rückschaltung auf lokalen Betrieb, Alarmierung eines menschlichen Operators)?

Neben der Technik ist auch die organisatorische Einbettung entscheidend: Es muss beschrieben werden, wer in welchen Fällen verantwortlich ist, welche Eskalationswege bestehen und wie diese in Echtzeit funktionieren – idealerweise abgestimmt mit lokalen Behörden, Notdiensten oder Verkehrsbetrieben.

2.7.2.4 Schulung der Fernsteuernden

Schließlich kommt den Menschen hinter den Fernlenkstationen eine zentrale Rolle zu. Sie sind in gewisser Weise das Bindeglied zwischen der Technik und der Verkehrswirklichkeit. Entsprechend hoch sind die Anforderungen an ihre Qualifikation. Neben der technischen Bedienkompetenz müssen sie über umfassende Kenntnisse in den Bereichen Verkehrsrecht, Unfallvermeidung, sicherheitskritisches Verhalten, Einschätzung von Umgebungssituationen und Notfallmaßnahmen verfügen. Die Schulungsprogramme müssen systematisch geplant, dokumentiert und überprüfbar sein. Die Schulung ist dabei nicht als einmalige Maßnahme zu verstehen, sondern als Teil einer kontinuierlichen Kompetenzsicherung, etwa durch regelmäßige Fortbildungen, praktische Übungen und Simulationstrainings. Nur so lässt sich sicherstellen, dass Fernsteuernde im entscheidenden Moment die richtigen Entscheidungen treffen.

2.7.3 Projektstory ADAS NextGen: Die Drivesmart will fernlenkbare Fahrzeuge entwickeln

Die Drivesmart AG ist ein mittelständisches Unternehmen, das sich auf intelligente Fahrerassistenzsysteme (ADAS) spezialisiert hat. Im Sommer 2025 wurde das hauseigene ADAS erfolgreich in eine neue Fahrzeugplattform integriert. Angespornt durch die neue gesetzliche Möglichkeit der Teleoperation, überlegt das Entwicklungsteam unter der Leitung von Robert Flink, das Fahrzeug für den ferngelenkten Betrieb zu ertüchtigen.

Ziel: Erweiterung des Betriebsmodus um »Remote Drive«

Robert Flink stellt ein interdisziplinäres Team zusammen, um die technische und regulatorische Machbarkeit zu prüfen. Folgende Rollen sind beteiligt:

- *Peter Weiss definiert als Projektleiter die Anforderungen an den neuen Betriebsmodus.*
- *Lara Vero leitet das technische Team und koordiniert Änderungsprozesse.*
- *Dieter Gewiss bewertet funktionale Sicherheitsaspekte des Fernlenksystems.*
- *Peter Feinblick analysiert die Risiken bzgl. Cybersecurity.*
- *Fernando Haswas klärt die regulatorischen Anforderungen mit dem KBA.*
- *Anja Bau, Ulla Wahrlich und Isy Kaput prüfen Architektur, Tests und Integration.*

Technische Umsetzung

Das Fahrzeug wird mit einem Remote-Interface ausgestattet, das dem fernsteuernden Operator Zugriff auf Fahrfunktionen, Umgebungsdaten und Systemstatus erlaubt. Sicherheitsmechanismen wie Notfallstopps, Verschlüsselung der Kommunikation, Latenzmonitoring und Umfeldüberwachung werden implementiert. Parallel beginnt Ulla Wahrlich mit der Definition eines Testkonzepts, das auch Fail-Safe-Verhalten und Cyberangriffe abdeckt.

Vorbereitungen für die Betriebserlaubnis

Fernando Haswas erstellt mit Unterstützung von Dieter Gewiss und Peter Feinblick folgende Nachweisdokumente für den Antrag beim KBA:

- *Sicherheitskonzept (gemäß ISO 26262 und StVFernLV Anlage 1)*
- *Cybersecurity-Konzept (in Anlehnung an ISO/SAE 21434)*
- *Systembeschreibung mit Konformitätserklärung zur VO (EU) 2018/858*
- *Beschreibung der Fernsteuerzentrale, inkl. Schulungskonzept für Operatoren*
- *Wartungs- und Diagnosekonzept*

Der externe Assessor Ulrich Richter wird frühzeitig eingebunden, um die Vollständigkeit und Nachvollziehbarkeit der Unterlagen zu prüfen.

Beantragung der Betriebsbereichsgenehmigung

Die Drivesmart AG beantragt zunächst eine Betriebsbereichsgenehmigung für ein eingeschränktes innerstädtisches Testgebiet. Das Konzept beinhaltet:

- *Kartografische Definition der Strecken*
- *Verkehrs- und Risikoanalyse*
- *Kommunikationsinfrastruktur*
- *Eskalations- und Notfallprozeduren*
- *Simulationen und Testberichte als Nachweise*

Nach Abstimmung mit der zuständigen Landesbehörde wird eine befristete Genehmigung für sechs Monate erteilt.

2.7.4 Von der Regelung zur Praxis: Erfolgsfaktoren für die Teleoperation

Die neue StVFernLV schafft erstmals die rechtliche Grundlage für den Betrieb ferngelenkter Fahrzeuge in Deutschland. Das Beispiel der Drivesmart AG verdeutlicht: Nur eine systematische Herangehensweise – mit interdisziplinärem Team, frühzeitiger Einbindung der Zulassungsstellen und stringenter Nachweisführung – führt solche Innovationsprojekte zum Erfolg.

Parallel zu dieser Entwicklung hat das Kraftfahrt-Bundesamt die deutschlandweite Erprobung hochautomatisierter Fahrsysteme der Stufe 4 zugelassen. Testfahrten dürfen damit erstmals unabhängig von zuvor festgelegten Strecken oder Stadtgebieten stattfinden. Diese bundesweite Genehmigung steigert die Effizienz im Testbetrieb, da Einzelgenehmigungen entfallen, und ermöglicht die Weiterentwicklung autonomer Mobilitätslösungen unter realen Bedingungen. Dies beschleunigt die Weiterentwicklung autonomer Mobilitätslösungen enorm. Erste praktische Einsätze fanden im öffentlichen Nahverkehr statt, wo autonome Shuttles während einer Fachveranstaltung im städtischen Raum getestet wurden – begleitet von Sicherheitsfahrern, um die Technologie kontrolliert an die Öffentlichkeit heranzuführen.

Gerade in komplexen urbanen Szenarien oder für spezielle logistische Anwendungen kann die Kombination aus autonomen Funktionen und Teleoperation kurzfristig Sicherheit und Effizienz steigern. So entsteht ein flexibles Gesamtsystem, das Schritt für Schritt den Übergang von der Erprobung hin zum regulären Betrieb im öffentlichen Verkehr ermöglicht.

Die technische Basis automatisierter Fahrzeuge ist nur ein Teil des Gesamtbilds. Ebenso entscheidend ist, wie Sicherheit, Cybersecurity und künstliche Intelligenz zusammenspielen. Das nun folgende Kapitel 3, »Zusammenspiel von funktionaler Sicherheit, Cybersecurity und KI«, beleuchtet diese Wechselwirkungen und zeigt, warum erst ihr Zusammenspiel den Weg zu vertrauenswürdigen Fahrzeugarchitekturen ebnet.