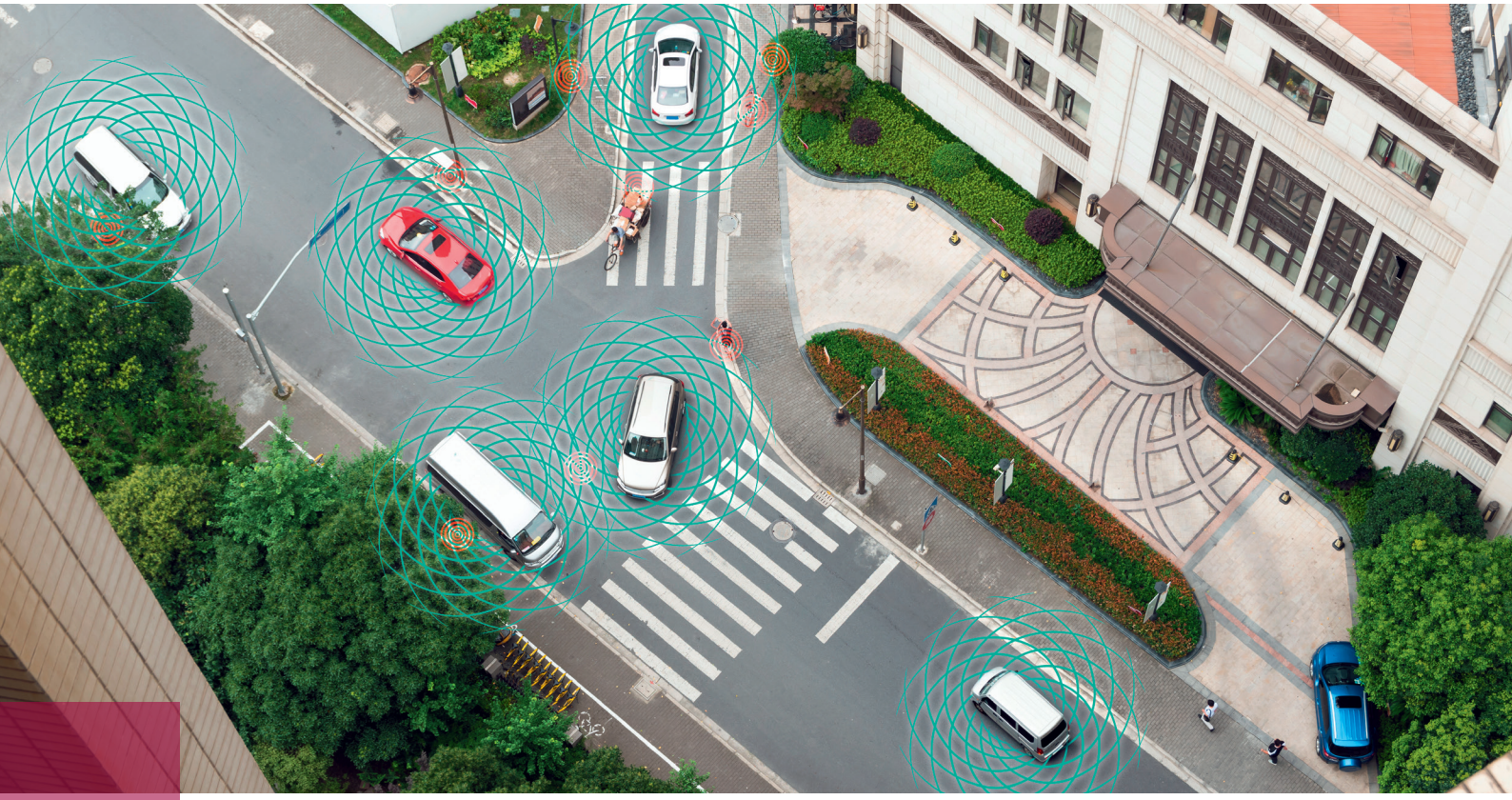
Lernende Systeme

DIE PLATTFORM FÜR KÜNSTLICHE INTELLIGENZ



Potenziale für industrieübergreifendes Flottenlernen

KI-Mobilitätsdatenplattform zur Risikominimierung des automatisierten Fahrens

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

WHITEPAPER

Tobias Hesse, Christoph Peylo et al.
AG Mobilität und intelligente Verkehrssysteme

Inhalt

Zusammenfassung

Ob in Transport, Logistik, im Individualverkehr oder im öffentlichen Nahverkehr – Verkehrsträger erreichen dank Künstlicher Intelligenz immer höhere Automatisierungsgrade. Automatisiertes Fahren kann helfen, die Verkehrssicherheit zu erhöhen, Verkehrsflüsse zu optimieren und Schadstoffemissionen zu reduzieren. Durch immer leistungsfähigere Verfahren der KI und des Maschinellen Lernens wird die Technologie des automatisierten Fahrens zunehmend verbessert, sodass sie in mehr als 99 Prozent der Situationen in Real-Tests funktioniert. Ein Restrisiko für mögliches Fehlverhalten tritt im Zusammenhang mit sogenannten Edge und Corner Cases (Grenz- und Übergangsfälle) auf. Für diese selten auftretenden Sonderfälle sind KI-Systeme unter Umständen nicht ausreichend trainiert und getestet. Das zentrale Ziel des Papiers ist es, die Bedeutung von Corner Cases für die Risikominimierung des autonomen Fahrens zu beschreiben und die Relevanz einer industrieübergreifenden Plattform zum Austausch von Mobilitätsdaten aufzuzeigen.

Um die Potenziale des industrieübergreifenden Flottenlernens zu erschließen, schlagen die Expertinnen und Experten der Arbeitsgruppe Mobilität und intelligente Verkehrssysteme der Plattform Lernende Systeme daher im vorliegenden Whitepaper die Gründung einer gemeinschaftlichen KI-Mobilitätsdatenplattform vor. Diese Plattform soll zur Risikominimierung beim automatisierten Fahren beitragen. Durch das sogenannte Flottenlernen können Fahrzeughersteller ihre Fahrzeuge optimieren, indem sie mit den Nutzungsdaten zu Corner Cases auf einer industrieübergreifenden Plattform trainieren. Die Plattform soll durch das Sammeln von Daten zu identifizierten Corner Cases als Basis für das Trainieren von KI-Systemen im gesamten Mobilitätssektor dienen, um damit die Voraussetzungen für ein industrieübergreifendes Flottenlernen schaffen zu können.

Das Konzept der industrieübergreifenden Plattform zum Austausch von Mobilitätsdaten sieht folgenden Ablauf vor: Die Plattform sammelt Beispiele, versucht, sie zu reproduzieren und mit anderen Modellen bezüglich ihrer Robustheit zu vergleichen, um auf bereits bekannte Corner Cases und Modelle bezüglich ihrer Robustheit auf diese entsprechend reagieren zu können. Dazu ist eine umfangreiche Sammlung von Rohdaten verschiedener Fahrzeugsensoren erforderlich, die als Test- und Validierungsdaten dienen (z. B. Lidar- und Radardaten von Kameras und Lasersensoren).

Im Papier werden dazu zentrale Hintergründe, etwa zu technologischen Herausforderungen oder zum Beitrag von KI-Methoden zum automatisierten Fahren, vorgestellt (Kapitel 1). Dazu zählen etwa Lösungen zur systematischen Beschreibung und Minderung des Restrisikos bei automatisierten Fahrzeugen. Anschließend werden zentrale Begriffe und bisherige Konzepte im Bereich des automatisierten Fahrens vorgestellt, die mit dem Konzept einer gemeinschaftlichen Plattform zum Austausch von Mobilitätsdaten verknüpft sind (Kapitel 2). Für die Realisierung einer Plattform für ein industrieübergreifendes Flottenlernen benötigen teilnehmende Unternehmen zur Datenverarbeitung und -weitergabe leistungsstarke Netzwerke oder Datenträger, damit die Daten in den jeweiligen Fahrzeugen gesammelt und später ausgelesen werden können. Für die Umsetzung eines effektiven

Flottenlernens ist es zudem wichtig, dass die Qualität der neu gelernten Modelle inklusive einer geeigneten Auswahl von Validierungsszenarien sichergestellt wird. Um bei Sonderfällen im Straßenverkehr (Corner Cases) sowohl Wahrnehmungsdefizite der Sensorik (Kamera, Radar, Ultraschall- und Laser-/Lidarsensoren) als auch Planungs- und Regelfehler der Systeme im Betrieb identifizieren zu können, sollen in Zukunft KI-Verfahren eingesetzt werden.

Im Papier werden darüber hinaus auch bestehende Projekte und domänenübergreifende Initiativen und Aktivitäten vorgestellt (Kapitel 3). Dazu zählen etwa Initiativen im nationalen sowie internationalen Bereich, die es ermöglichen sollen, Daten in einem weltweit wettbewerbsfähigen digitalen Ökosystem (z. B. GAIA-X) effizient und sicher auszutauschen. Im Gegensatz zu jenen Ansätzen liegt der Fokus der KI-Mobilitätsdatenplattform, die im vorliegenden Papier vorgestellt wird, gezielt auf Corner Cases. Das Konzept der gemeinschaftlichen KI-Plattform zum Austausch von Mobilitätsdaten wird in Kapitel 4 detaillierter skizziert. Als technische Vermittlungs-Plattform (Web-Service) soll diese Beispiele für Corner Cases sammeln, zudem eine Referenzlinie zur Risikoeinschätzung bilden sowie die Validierung von ML-Modellen ermöglichen. Die Plattform soll dabei von einer neutralen Institution betrieben werden, das Betreibermodell der Plattform sieht einen transaktionsbasierten Service vor, sodass die Plattform sich finanziell selbst trägt.

Mit dem Konzept zur Gründung einer gemeinschaftlichen KI-Mobilitätsdatenplattform möchten die Expertinnen und Experten einen Beitrag zur Risikoeinschätzung leisten und die Förderung von Standardisierung und Regulierung von KI-Systemen in der Mobilität anregen. Zur Umsetzung schlagen die Autorinnen und Autoren abschließend Gestaltungsoptionen und die Anpassung bestimmter Rahmenbedingungen vor, die Akteure aus Unternehmen und Politik adressieren (Kapitel 5). Als zentrale Gelingensbedingung für die KI-Mobilitätsdatenplattform gelten etwa Standards für die Modellierung und Austauschformate von Daten (z. B. standardisierte Datenformate, Schnittstellen und Protokolle), die den Zugang zu gemeinsamen Tools und Technologien ermöglichen. Zu den weiteren Gestaltungsoptionen zählen die Unterstützung der Gründung einer finanziell selbsttragenden Plattform, der Aufbau einer Community für die KI-Mobilitätsdatenplattform sowie die Förderung weiterer Forschungsvorhaben unter anderem zur Beschreibung, Identifikation und Bewertung von Corner Cases.

1. Hintergrund und Zielsetzung

Ein wesentlicher Innovationstreiber und Wettbewerbsfaktor der Mobilitätsbranche (Automobil, Schienenverkehr und andere Industrien) liegt im **automatisierten Fahren**, ermöglicht unter anderem durch **Methoden der Künstlichen Intelligenz (KI)**. In Deutschland investieren vor allem die großen Automobilkonzerne und Zulieferer große Summen, um mit dem Engagement der Wettbewerber aus den USA und Asien mitzuhalten (Plattform Lernende Systeme 2019; Sopra Steria Consulting/F.A.Z. Institut 2019).

Trotz kostenintensiver und umfassender Forschungs- und Entwicklungsaktivitäten von mehreren Milliarden Euro in den letzten 20 Jahren zu Lernenden Systemen im Straßenverkehr gibt es bislang keine breite Markteinführung von hochautomatisierten Fahrzeugen.[1] Die Technologie des automatisierten Fahrens ist zwar bereits sehr weit entwickelt und wird durch **immer leistungsfähigere Verfahren der KI und des Maschinellen Lernens weiter verbessert**, sodass sie in mehr als 99 Prozent der Situationen in Real-Tests funktioniert. Trotzdem verbleibt ein **Restrisiko** für mögliches Fehlverhalten. Dieses tritt häufig im Zusammenhang mit sogenannten **Edge und Corner Cases**[2] (Grenz- und Übergangsfälle) auf. Diese beschreiben Sonderfälle, die so selten auftreten, dass die Lernenden Systeme dafür gegebenenfalls nicht ausreichend konzipiert, trainiert und getestet wurden. Zur Lösung dieses Problems schlägt die Arbeitsgruppe vor, eine KI-Mobilitätsdatenplattform für industrieübergreifendes Flottenlernen zu realisieren. Die Plattform dient dem Sammeln von Daten zu identifizierten Corner Cases, um aus diesen zu lernen und um die Erkenntnisse für Lernende Systeme im Mobilitätssektor zu nutzen.

Das vorliegende Papier zeigt zentrale Aspekte auf, wie das Vertrauen in die Sicherheit der Technologie verbessert und zukünftige Zulassungsvoraussetzungen mitgedacht werden können, um die Risiken beim Einsatz automatisierter Fahrzeuge im Mischverkehr zu minimieren. Dies geht mit den Überlegungen zur Umsetzung von Normen und Standards einher, welche die KI-Normungsroadmap des Deutschen Instituts für Normung e. V. (DIN) und die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (DKE) im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) beschreibt (DIN/DKE 2020). Nur wenn KI-Systeme in der Mobilität erklär- und validierbar sind, ist nachvollziehbar, wie sie Entscheidungen im Straßenverkehr treffen. Hierbei unterstützen Normen und Standards. So verweisen auch die Autorinnen und Autoren des Whitepapers Zertifizierung von KI-Systemen der Plattform Lernende Systeme darauf, dass Zertifizierungsverfahren bestimmte Standards von KI-Systemen garantieren müssen, gleichzeitig aber Überregulierung vermeiden und Innovation ermöglichen sollten (Heesen et al. 2020).

1 Die Einteilung der verschiedenen Klassen zu automatisiertem Fahren wurde 2014 in der Norm SAE J3016 festgelegt. Automatisierung fängt mit der Ebene 3 (bedingte Automatisierung) an. Hier muss ein Fahrer in der Lage sein, auf Anforderung eingreifen zu können. In Stufe 4 ist dies nicht mehr notwendig, allerdings werden nicht alle Fahrsituationen unterstützt. Erst in Ebene 5 werden alle Fahrmodi unterstützt. (SAE 2018)

2 Für eine verbesserte Lesbarkeit bezeichnen die Autorinnen und Autoren im vorliegenden Whitepaper die sogenannten Edge und Corner Cases nur noch als Corner Cases, beziehen sich dabei jedoch auch immer auf Edge Cases.

Beitrag von KI-Methoden zum automatisierten Fahren

Die vielversprechendsten Ansätze für die Weiterentwicklung des automatisierten Fahrens basieren in wesentlichen Teilen auf KI-Methoden, insbesondere **Maschinellem Lernen (ML)**. ML hat die Eigenschaft, dass das Systemverhalten nicht wie klassische Software über deskriptive Regeln programmiert ist, sondern auf Basis einer repräsentativen Menge von Trainingsdaten, quasi einer großen „Datenstichprobe", aus der Anwendungsdomäne gelernt wird, zum Beispiel mit neuronalen Netzen. Voraussetzung für die Effektivität von ML-Ansätzen ist, dass das Erheben der Datenstichprobe aus dem Eingaberaum der jeweiligen „Operationalen Design Domäne" (ODD) umfassend erfolgt, das bedeutet, dass die Daten möglichst alle repräsentativen und typischen Fälle abdecken.

Operationale Design Domäne (ODD) eines autonomen Systems beschreibt die Betriebsbedingungen, für welche es funktional ausgelegt ist. Dazu gehören zum Beispiel Verkehrsarten (Straßen-, Schienenfahrzeug), die Umgebungen, in denen es operiert (Autobahn, Landstraße, innerstädtisch, innerhalb eines geschlossenen Campus oder Bahndepots), lokale Einschränkungen (zum Beispiel auf bestimmte Städte, Vorstädte), Wetterbedingungen und viele mehr.

Abbildung 1: Operationale Design Domäne (ODD) eines autonomen Systems

Anmerkung: Die **Operationale Design Domäne** (ODD) beschreibt die Grenze innerhalb der Gesamtheit von möglichen Betriebsbedingungen. Mögliche Corner Cases (rote Symbole) treten oftmals in Randbereichen der Parameter auf.

In der Praxis ist es vergleichsweise einfach, typische und häufig auftretende Daten in diesem Eingaberaum zu sammeln: so wie Sensordaten, die beispielsweise weiße Autos oder Fußgänger mit blauen Jeans und weißen T-Shirts identifizieren. Schwieriger ist es jedoch, selten beobachtbare Daten zu gewinnen, wie zum Beispiel Fußgänger in untypischen Outfits oder nicht in Deutschland heimische Tiere wie Kängurus. Im Hinblick auf Sicherheit

ergeben die selten auftretenden Daten jedoch einen in der Summe nicht zu vernachlässigenden Anteil.[3] Dieses Restrisiko besteht unter anderem, weil (1) nicht nachgewiesen werden kann, dass die Stichprobe für das Training der ML-Ansätze eine ausreichende Anzahl an Fällen abdeckt, oder (2) nicht verifiziert werden kann, dass die Stichprobe für das Testen die „harte Realität"[4] hinreichend genau abdeckt. Für eine erfolgreiche Markteinführung von automatisierten Fahrzeugen gilt es daher, eine Lösung zur systematischen Beschreibung und Minderung des Restrisikos zu finden. Die Lösungsansätze hierfür liegen im regulatorischen und technologischen Bereich.

Technologische Herausforderungen

Zur Absicherung von ML-Methoden für das automatisierte Fahren existieren vielschichtige Lösungsansätze: Dies umfasst zum Beispiel die Verbesserung der Erklärbarkeit der sogenannten „Black Box" KI oder auch ein genaueres Verständnis der Robustheit und Evidenzbeschreibung der ML-Methoden. Eine wesentliche Rolle nimmt an dieser Stelle auch die **intelligente Stichprobenerhebung** der Eingabedaten im Kontext von Corner Cases ein. Es geht um die Sammlung, Analyse und Modellierung insbesondere der Rand- und Eckbereiche der ODD.

Plattformkonzept als Lösungsansatz

Das vorliegende Papier schlägt ein Plattformkonzept vor, in dem Corner Cases als Anwendungsfall im Fokus stehen. Die Herausforderungen und Chancen zur Sicherheit bzw. Absicherung von ML-Ansätzen betreffen eine Vielzahl an Herstellern (zum Beispiel Automobil- und Schienenverkehr) und -zulieferern von automatisierten Fahrzeugen. Die systematische Betrachtung von Corner Cases spielt hier eine wesentliche Rolle. Es bedarf deshalb einer **gemeinschaftlichen Plattform zum Austausch von Mobilitätsdaten**, mit der Datenstichproben industrieübergreifend identifiziert, gesammelt und modelliert werden können, um damit Voraussetzungen für ein industrieübergreifendes Flottenlernen (siehe Kapitel 2.1) zu schaffen (Plattform Lernende Systeme, 2019). Die gewonnenen Corner Cases sollen den einzelnen Akteuren über die KI-Mobilitätsdatenplattform zur Verfügung gestellt werden. Zudem soll die gemeinschaftliche Plattform wertvolle Grundlage für Regulierungen und Zulassungsprozesse für die verschiedenen Anwendungsszenarien, ähnlich einer „Führerscheinprüfung für automatisierte Fahrzeugflotten", sein. Damit unterstützt sie die Etablierung von Normen und Standards, die auf technischer Ebene helfen, die Sicherheit von automatisierten Fahrzeugen im Laufe ihrer Inbetriebnahme zu wahren (DIN/DKE 2020). Inwieweit und in welchem Umfang die auf der Plattform vorhandenen Daten für staatliche Zulassungsprozesse genutzt werden können, müsste im Rahmen von Betreibermodellen geklärt und festgelegt werden.

3 Dies wird auch als „long-tail distribution" bezeichnet, weil die Datenverteilung bis in die Randbereiche der Achsen reicht.
4 „Harte Realität" meint in diesem Kontext das sichere, autonome Betreiben von Millionen von Fahrzeugen über mehrere Jahre hinweg.

2. Grundlagen: Zentrale Begriffe und bestehende Konzepte

Um das Konzept einer gemeinschaftlichen Plattform zum Austausch von Mobilitätsdaten eindeutig zu skizzieren, definieren die Autorinnen und Autoren zunächst die Grundlagen aus dem Forschungsfeld Künstlicher Intelligenz im Bereich des automatisierten Fahrens. Es werden sowohl zentrale Begriffe wie Flottenlernen und das Lernen von Corner Cases definiert als auch die Nutzung von Daten abhängig von Art (Rohdaten, simulierte Daten, Realdaten), Vorkommen (Granularität) sowie Umgang (Standardisierung) beschrieben. Zudem werden der Unterschied zwischen Verifizierung und Validierung dargelegt und das sogenannte Sampling von großen Parameterräumen sowie der Begriff Optimierung erläutert.

2.1 Flottenlernen: Lernen von Corner Cases

Heutzutage gibt es bereits Automobilhersteller, die durch das sogenannte Flottenlernen ihre Fahrzeuge ständig optimieren: Sie sammeln Nutzungsdaten ihrer gesamten Fahrzeugflotte und laden neue Updates auf jedes einzelne Fahrzeug der entsprechenden Flotte. Der Begriff der Flotte bezieht sich in der Regel auf die Fahrzeuge eines einzigen Herstellers, wobei auch herstellerübergreifende Konfigurationen denkbar sind.[5] Vorreiter auf diesem Gebiet sind US-amerikanische Unternehmen[6], die bereits Testfahrzeuge auf den Straßen fahren lassen und diese effektiv mit Flottenlernen trainieren. Auch in Deutschland weiten die Automobilhersteller ihre Fähigkeiten im Flottenlernen aus.

Der Prozess des Flottenlernens umfasst folgende Schritte: Nachdem die Daten aus Fahrzeugen gesammelt wurden, werden sie zur Analyse und Verarbeitung auf ein Backend (ein serverseitiges System beispielsweise des Herstellers) übertragen. Während der Analyse werden diese Daten mit den bereits vorhandenen Szenarien verglichen, um sicherzustellen, dass relevante Sequenzen in vergleichbaren Größenordnungen vorhanden sind. Ein „Oversampling" von unkritischen Fahrsituationen kann durch diesen Vergleich vermieden werden. Anschließend wird ein Training mit den aus den neuen Daten entstandenen Modellen initiiert, welches mit einer Validierung durch das Abspielen unterschiedlicher Szenarien und einer Freigabe zur Verbreitung abschließt. Im Anschluss werden die aktualisierten Modelle an die entsprechende Fahrzeugflotte gesendet, die damit wieder auf dem neuesten Stand ist. Das Flottenlernen kann so insbesondere der Gefahr durch die im Autoverkehr auftretenden Corner Cases vorbeugen.

5 Der Begriff Konfiguration ist im vorliegenden Whitepaper gleichbedeutend mit dem Begriff „Setup".

6 Zum Beispiel Tesla und Waymo (Tochterfirma von Alphabet). Das Unternehmen Agnik betreibt bspw. seit 2010 mit MineFleet eine Data-Mining-Software, die Mobililtätsdaten fürs Flottenlernen sammelt und verarbeitet (Kargupta, Sarkar & Gilligan 2010).

Für die Realisierung einer Plattform für ein industrieübergreifendes Flottenlernen benötigen die Hersteller zur Datenverarbeitung und -weitergabe entweder leistungsstarke Netzwerke mit einer breitbandigen Internetverbindung oder Datenträger, die den Fahrzeugen entnommen und gegebenenfalls in ein bereitstehendes mobiles Backend eingelesen werden können, also im internen Bereich des technischen Systems. Darüber hinaus ist es für die Umsetzung eines effektiven Flottenlernens wichtig, dass die Qualität der neu gelernten Modelle inklusive einer geeigneten Auswahl von Validierungsszenarien sichergestellt wird. Zudem muss auch die Übertragung dieser Modelle in die Fahrzeuge über den Update- und Initialisierungsprozess sicher ablaufen. Zur Optimierung des Flottenlernprozesses müssen jeweils die Daten gefunden werden, welche die höchste Relevanz für das aktuell auftretende Problem in der derzeitigen Konfiguration haben.

2.2 Corner Cases

Corner Cases sind für Lernende Systeme Sonderfälle – auch als Grenz- und Übergangsfälle bezeichnet – die so selten auftreten, dass die Systeme dafür nicht entsprechend konzipiert wurden. Lernende Systeme können den Umgang mit Corner Cases auch nicht durch einfaches Hinzufügen von Trainingsdaten lernen. Es gibt unterschiedliche Arten von Corner Cases: solche, bei denen Daten zur Identifizierung fehlen, gerade weil sie so selten eintreten, und solche, die auch durch mehr verfügbare Daten nicht einfacher zu erkennen sind. Im zukünftig vernetzten Straßenverkehr trifft das zum Beispiel zu, wenn ein automatisiertes Auto eine Ampel bei schlechtem Wetter aus einem ganz bestimmten Winkel trotz Kamera-, Laser-, Radar- und Ultraschallsensoren nicht erkennt. Dann reagiert das Fahrzeug als Lernendes System – bestehend aus den genannten Wahrnehmungskomponenten – entweder (1) *nicht*, weil es die Ampel nicht wahrnimmt, oder (2) es verhält sich *unbeabsichtigt richtig oder falsch*, indem es beispielsweise abbremst oder beschleunigt und dadurch möglicherweise die Verkehrssicherheit gefährdet.

In der Regel kann ein solch *unbeabsichtigtes Verhalten* oder *Nicht-Verhalten* der Lernenden Systeme nachträglich analysiert und auf einen Corner Case zurückgeführt werden. Im laufenden Betrieb können Corner Cases nicht grundsätzlich, und dann eher durch manuelle Analysen der aufgenommenen Daten, von Programmiererinnen und Programmierern erkannt werden. Etwa, wenn das Lernende System einen Menschen am Straßenrand erkennt und darauf reagiert, obwohl es sich um ein Werbeplakat am Straßenrand handelt, auf dem Menschen abgebildet sind.

Um sowohl Wahrnehmungsdefizite der Sensorik (Kamera, Radar, Ultraschall- und Laser-/Lidarsensoren) als auch Planungs- und Regelfehler des Systems im Betrieb identifizieren zu können, sollen in Zukunft KI-Verfahren eingesetzt werden. Wahrnehmungsdefizite einer Kamera können beispielsweise durch Verschmutzung der Kameralinse auftreten. Planungs- und Regelfehler können unterlaufen, wenn für bestimmte Verkehrssituationen noch kein richtiges Verhalten erlernt ist, wie zum Beispiel eine zuvor erkannte Ampel, die nun durch andere Verkehrsteilnehmer (Busse, LKW) oder Gegenstände verdeckt ist.

Weitere Beispiele sind eine von Hochwasser oder Bauschutt bedeckte Straße, die nicht als bedeckt oder verschmutzt erkannt wird. Solche Situationen sind so selten, dass sie nicht oder kaum in Trainingsdaten vorkommen und somit auch nicht erlernt werden.

Für die Reduzierung von Corner Cases sollten bereits in der Entwicklung automatisierter Fahrzeuge entsprechende Maßnahmen durchgeführt werden. Um die Robustheit von KI-Modellen bezüglich Wahrnehmungsfehlern zu erhöhen, können beispielsweise „Adversarial Examples" verwendet werden. Dies sind eigens konzipierte Trainingsdaten, die ein KI-System absichtlich zu einer Fehlklassifikation verleiten sollen. Diese Technik wird im Rahmen von Adversarial Attacks bewusst eingesetzt. So könnten beispielsweise optische Manipulationen von Verkehrsschildern simuliert werden, die Lernende Systeme vor einem Nicht- oder Fehlverhalten bewahren.

Planen: Planungssprache und Situationskalkül

Planen ist eine der wesentlichen Kompetenzen, die KI-Systemen zugeschrieben werden. Konkret umfasst es die Realisierung von Strategien oder Handlungssequenzen, die typischerweise von intelligenten Agenten, autonomen Robotern und automatisierten Fahrzeugen ausgeführt werden. In der Regel handelt es sich dabei um komplexe Lösungen, die im multidimensionalen Raum gefunden und optimiert werden. Im Straßenverkehr, der als dynamische unbekannte Umgebung charakterisiert wird, muss die Strategie oft online überarbeitet werden.

Beim autonomen Fahren existiert ein Planungsproblem aus zwei Gründen:

(1) Ein automatisiertes Fahrzeug kann nicht als ein reaktiver Controller konzipiert werden, weil die Geschwindigkeit des Fahrzeugs zu hoch ist, um ausschließlich auf Ereignisse im unmittelbaren Fahrzeugumfeld zu reagieren.

(2) Es kann zudem auch keine Vorausberechnung der KI erfolgen, da sich das Verkehrsumfeld hochdynamisch verändert.

Im Kontext des automatisierten Fahrens wird häufig der Begriff der Trajektorienplanung verwendet. Er beschreibt die Festlegung (und dynamische Revision) einer Bahn auf der Fahrbahnoberfläche und deren zeitlichen Verlauf, sodass auch dynamische Größen wie Geschwindigkeit, Beschleunigung etc. geplant oder daraus abgeleitet werden. Die kollisionsfreie Navigation – im Sinne der Festlegung einer Trajektorie – kann auch auf die Lösung des Problems der Optimierung mit Beschränkungen (constraints) zurückgeführt werden. Dabei werden bestimmte Zielgrößen wie Zeit, Komfort oder Energieverbrauch unter Berücksichtigung der Kollisionsvermeidungsbedingungen für das Fahren auf der berechneten Bahn minimiert. Konkret bedeutet dies, dass das Auto nicht gegen eine Fußgängerin oder einen Fußgänger fährt oder gegen ein anderes Hindernis, etwa ein parkendes Auto auf der Fahrbahn, prallt.

2.3 Datensammlung und Datenstruktur

Rohdaten

Um auf bereits bekannte Corner Cases und Modelle bezüglich ihrer Robustheit auf diese entsprechend reagieren zu können, sammelt die Plattform Beispiele und versucht, sie zu reproduzieren und mit anderen Modellen bezüglich ihrer Robustheit zu vergleichen. Hierfür wird eine umfangreiche Sammlung von Rohdaten verschiedener Fahrzeugsensoren benötigt. Sie dienen als Test- und Validierungsdaten für ML-Modelle, die zum Testen hochgeladen werden können. Dazu gehören Bild-, Lidar- und Radardaten von Kameras und Lasersensoren, die Automobilen ermöglichen, ihre Umgebung wahrzunehmen. Zusätzlich unterstützen verfügbare V2X-Daten (Vehicle-to-everything) das Lernen von Corner Cases. Sie enthalten viele Informationen über mögliche Unsicherheiten, die die Verarbeitung von Situationen und die Ableitung von Aktionen im Straßenverkehr mitbestimmen und somit die Verkehrssicherheit erhöhen können. Zu diesen V2X-Daten zählen zum Beispiel Infrastruktur-Daten, Daten zu Mobilitätsereignissen wie Staus und Baustellen, aber unter anderem auch geografische Kartendaten oder Wetterdaten.

Zur bestmöglichen Verarbeitung auf der Plattform sollten die Daten idealerweise als Rohdaten vorliegen. Das bedeutet, dass beispielsweise Kameradaten unmittelbar für KI-Verfahren genutzt werden können, ohne dass sie vorher weiterverarbeitet (zum Beispiel in ein anderes Dateiformat umgewandelt) wurden. Dadurch wird gewährleistet, dass die Daten möglichst im Originalzustand ohne Transformationsfehler in die Lernverfahren einfließen.

Realdaten und simulierte Daten

Das Sammeln von Daten aus Millionen Straßenkilometern führt im Realtestbetrieb nicht zu einer ausreichenden Abdeckung kritischer Szenarien. Es stellt sich zudem das Problem der Annotation, das heißt der genauen Zuordnung von Bildobjekten auf semantische Klassen. Um eine möglichst breite Verwendbarkeit der Realdaten für Training und Validierung gewährleisten zu können, müssen zum Beispiel Kameradaten pixelgenau annotiert werden. Dabei wird jedes Pixel einer semantischen Klasse (z. B. „Straße“, „Verkehrsschild“, „Fahrradfaher“, …) zugeordnet. Dies erfordert trotz Fortschritten im Bereich der Annotationswerkzeuge und Angeboten aus Ländern mit vergleichsweise geringen Lohnkosten erhebliche zeitliche und monetäre Ressourcen. Für multisensorielle Daten, die auch Lidar- und Radarinformationen enthalten, ist das Problem noch gravierender. Zudem wirft das Sammeln von Realdaten auch die Privatheits- und Datenschutzproblematik auf. Denn jede Verarbeitung von Daten, die personenbezogen zuordenbar ist, selbst ihre Anonymisierung, bedarf einer Rechtsgrundlage.[7]

7 Das Sammeln, Austauschen, Anonymisieren und Verarbeiten von Daten wirft weitere Problematiken hinsichtlich Datenschutz, Privatheit und Haftung auf, die im Rahmen dieses Whitepapers jedoch nicht umfassend betrachtet werden können.

Ein Lösungsansatz ist die Verwendung simulierter Daten, die künstlich erzeugt wurden und nicht aus realen Ereignissen stammen. Die Verfahren der synthetischen Datenerzeugung durch Simulation bieten eine Reihe von Vorteilen: die Nutzungsrechte sind nicht grundsätzlich eingeschränkt und vor allem können Parameter wie zum Beispiel Fahrzeuggeschwindigkeiten oder Komplexität der Szene beliebig variiert werden. Ferner können im realen Raum riskante Aktionen beliebig oft ohne Einschränkung nachgestellt werden. Darüber hinaus können die synthetischen Verfahren auch sehr einfach die für Training und Validierung benötigten „Ground-truth-Daten" liefern, da diese direkt aus dem Modell stammen.

Die synthetische Datenerzeugung eignet sich insbesondere, um systematische Trainings- und Validierungsdaten zu erzeugen. So können Fahrsituationen in der Simulation beliebig variiert werden. Nur mit Daten einer relevanten Abdeckung kann die Absicherung der KI-Module gewährleistet werden. Für synthetische Daten muss allerdings sichergestellt sein, dass sie Realdaten hinreichend gut ersetzen können.

Granularität der Daten

Abhängig von der expliziten Problemstellung im Bereich des automatisierten Fahrens oder vom Reifegrad des Fahrzeugs sind Daten unterschiedlicher Granularität notwendig, also unterschiedliche Verdichtungsgrade von Datensätzen. Wenn zum Beispiel die Umgebungswahrnehmung (Perzeption) verbessert werden soll, müssen zunächst Rohdaten (Sensorausgaben) gesammelt, ausgewertet und als Grundlage für die Entwicklung neuer Modelle herangezogen werden.

Daraus ergeben sich folgende Problemstellungen:

1. Die Datenmengen sind sehr groß, sodass in der Regel ein aufwändig organisierter Flottenversuch vonnöten ist, im Rahmen dessen Datenträger in die Fahrzeuge verbaut und regelmäßig ausgetauscht werden. Es gibt Ansätze, bei denen in der Nähe der Teststrecke ein mobiles Backend aufgebaut wird, welches den Austausch der Daten erleichtert. Dies ist jedoch noch nicht die Regel. Des Weiteren wird darauf hingearbeitet, relevante Situationen im Feld zu erkennen, sodass nur diese Daten hochgeladen werden müssen. Hilfreich ist hier, sich auf die Sammlung von Corner Cases anstelle einer umfassenden Datensammlung zu konzentrieren. Dies erlaubt einerseits die Fokussierung auf die Qualität der Daten und stellt andererseits einen Hebel dar, um Anforderungen oder Speicher- und Übertragungsbedarf zu begrenzen. Ein wesentlicher Schlüssel für eine zielführende Auswahl der Corner Cases liegt im Design eines geeigneten, intelligenten Trigger- oder Selektionsmechanismus.

2. Es ist fraglich, inwieweit die Rohdaten verallgemeinerbar sind, das heißt, wie gut sie sich für Konfigurationen (Sensorarten und -positionen, Datenübermittlungsprotokolle, Umgebungsparameter etc.) wiederverwenden lassen, die nicht der ursprünglichen Konfiguration entsprechen.

Die genannten Problemstellungen zeigen Vorteile für das Sammeln von abstrakteren Daten auf. Wenn jedoch lediglich Ereignisse auf hohem Abstraktionsniveau beschrieben werden, stellt sich die Frage nach der Nützlichkeit dieser Daten für die Verbesserung (oder auch die Validierung) der Zielsysteme.

Der Detaillierungsgrad kann grundsätzlich dann reduziert werden, wenn ausgehend von einem spezifischen Problem hin zu einem allgemeinen Problem gedacht wird. Er kann auch erhöht werden, wenn der Weg von den in der Regel neuronal gelösten Perzeptionsaufgaben hin zur Planung (oft symbolisch oder zumindest hybrid) führt. Da es sich bei Corner Cases um Grenz- und Übergangsfälle handelt, ist es darüber hinaus wichtig, geeignete Verfahren zur Verbesserung der Labeling-Qualität solcher Corner-Case-Daten verfügbar zu machen. Diese Verfahren sollten in der Lage sein, das aufgezeigte Spannungsfeld zwischen Rohdaten und abstrakteren Daten sowie komplett abstrakten Daten zu ergänzen.

2.4 Standardisierung von Datenaustauschformaten

Eine Mobilitätsplattform für den Austausch von Daten hat nur Erfolg, wenn sie auf standardisierte Lösungen zugreifen und aktiv als Partner für Standardisierungsgremien und verwandte Initiativen fungieren kann. Dazu zählt, dass sie sowohl etablierte, industrieübergreifende Standards und Normen nutzt als auch neue Standardisierungsaktivitäten im eigenen Umfeld initiiert.

Nur durch die Verwendung von Standards wie einer gemeinsamen Sprache und Methodologie für die Zusammenarbeit kann die Plattform als erfolgreicher Enabler für den Datenaustausch zwischen den vielen verschiedenen Marktakteuren (Anwender und Data Provider) auftreten. Darüber hinaus tragen Standards dazu bei, Synergieeffekte zu erzielen und die Kosten für den Aufbau und die Instandhaltung der Plattform zu minimieren. Je niedriger die Kosten für die Sammlung, Speicherung und Bereitstellung der Daten ausfallen, desto attraktiver wird die Plattform für die teilnehmenden Akteure.

Der Bedarf an standardisierten Lösungen für die Plattform ist vielfältig. So benötigt die Plattform für die Beschreibung verschiedener Datenarten und -modelle standardisierte Formate wie zum Beispiel Ontologien (siehe Infobox, S. 14). Dies gilt auch für Metadaten, Labels, Rückverfolgbarkeit, Datenqualität, Metriken und Weiteres. Darüber hinaus bedarf die Kontextualisierung von Daten und Modellen weiterer Beschreibungsformate für Anwendungsfälle und Anforderungen. Das beinhaltet Referenzen zu Systemen, Komponenten und Funktionen, in welchen Daten von Corner Cases produziert oder verwendet werden.

Ontologien
Im Bereich der Informatik sind Ontologien die Grundlage für ein gemeinsames Verständnis sprachlich gefasster und formal geordneter Darstellungen einer Menge von Begrifflichkeiten und der zwischen ihnen bestehenden Beziehungen. Das Ziel ist, eine einfache, eindeutige und sichere Beschreibung der Funktionalitäten und deren systemischen Wechselwirkungen zu erreichen. Um ein fokussiertes System mit eindeutigen informatorischen Schnittstellen, Integritäts- und Inferenzregeln zu erhalten, muss zunächst eine Ontologie definiert werden.

Zur Ableitung einer eindeutigen Ontologie ist ein gemeinsames Modellverständnis des Gesamtsystems (Fahrzeug in Interaktion mit Passagier und Umgebung) notwendig. Die dafür notwendigen Systemmodelle und die zu betrachtenden Wechselwirkungen können mit Methoden des Model Based Systems Engineering (MBSE) abgebildet werden. Hierzu dient beispielsweise die Modellierungssprache SysML. Für die weitere und detailliertere Darstellung der Funktionen des automatisierten Fahrens eignen sich Beschreibungssprachen bzw. -formate, wie zum Beispiel openSCENARIO, openDRIVE, openLABELING.

2.5 Methodische Ansätze und Konzeptualisierung zentraler Begriffe

Bei der Entwicklung von (automatisierten) Fahrzeugen ist es notwendig, stets alle Funktionen auf deren Korrektheit zu überprüfen. Hierfür gibt es zwei methodische Ansätze, die Verifizierung und die Validierung. Obwohl diese in der gesprochenen Sprache häufig als Synonyme verwendet werden, gibt es im Entwicklungseinsatz wichtige Unterschiede.

Die Aufgabe der Verifizierung ist es zu überprüfen, ob ein Produkt gemäß den Spezifikationen, Richtlinien, Gesetzen und Anforderungen korrekt entwickelt wurde und funktioniert. Im Gegensatz dazu überprüft die Validierung, ob die Nutzeransprüche, also die beabsichtigte Funktion, erfüllt werden. Damit versucht die Validierung eine Antwort auf die Frage zu finden, ob das richtige Produkt entwickelt wurde.

Eine besondere Herausforderung für die Verifizierung und Validierung stellen moderne Ansätze auf Basis von Lernenden Systemen und Künstlicher Intelligenz dar. Die Güte dieser Methoden ist direkt an die Auswahl der Daten gekoppelt, die für das Training dieser Verfahren verwendet werden. Oftmals befinden sich diese Daten jedoch in einem hochdimensionalen Parameterraum, sodass die Auswahl von vielfältigen und zugleich repräsentativen Daten sowie eine suffiziente Abdeckung des Raumes an relevanten Parameterkombinationen anspruchsvolle Aufgaben sind. Ein solcher Parameterraum kann zum Beispiel unterschiedliche Wetter- oder Lichtbedingungen, Tageszeiten, Objektkonstellationen, Oberflächeneigenschaften und szenendynamische Eigenschaften beinhalten. Diese Suche nach Parametern wird häufig auch als Sampling von Parameterräumen bezeichnet.

Ebenfalls von großer Bedeutung ist die Stichprobenziehung von Parameterräumen für die notwendigen Tests während unterschiedlicher Entwicklungszyklen. Selbst bei Verwendung von Tests in simulierten Umgebungen auf großen Serverfarmen ist es nicht möglich, jede erdenkliche Parameterkombination zu testen. Daher ist eine intelligente Auswahl notwendig, um möglichst alle relevanten Szenarien abzudecken. Hierfür ist es notwendig, Optimierungsverfahren und automatisierte Labeling-Verfahren einzusetzen, die eine repräsentative und zugleich effiziente, aber dennoch handhabbare Auswahl an Testszenarien (Parameterkombinationen) erstellen, sodass eine vertrauenswürdige Verifikation bzw. Validierung durchgeführt werden kann.

3. Bestehende Projekte und domänenübergreifende Initiativen

Damit KI-Systeme in der Mobilität sicher und verlässlich funktionieren, bedarf es – wie in Kapitel 2.4 dargelegt – der Einführung und Nutzung von Normen und Standards (siehe KI-Normungsroadmap, (DIN/ DKE 2020)). Auch die Autorinnen und Autoren des Whitepapers *Zertifizierung von KI-Systemen* der Plattform Lernende Systeme diskutieren die Ausgestaltung gelungener Zertifizierungsverfahren: Je nachdem, wie hoch das Risiko der KI-Anwendung eingestuft wird, sollte eine Zulassung – freiwillig oder verpflichtend – eingeführt werden (Heesen et al. 2020).

Bis es zu einem flächendeckenden Einsatz automatisierter Fahrzeuge kommt, bedarf es noch weiterer Risikominimierung. Zu dieser kann die skizzierte Plattform einen Beitrag leisten, indem die ML-Modelle nach der Prüfung eine entsprechende Kennzeichnung erhalten. Die somit stattgefundene Validierung der Modelle ermöglicht es der Plattform, eine Referenzlinie zur Risikoeinschätzung zu bilden. In diese Risikoeinschätzung könnten Datenschutz, IT-Sicherheit und Privatheitsaspekte einfließen. Das in Kapitel 4 skizzierte Konzept der gemeinschaftlichen Plattform zum Austausch von Mobilitätsdaten ist über die Normungs- und Standardisierungsaktivitäten hinaus im Kontext bereits laufender Aktivitäten und Vorhaben zu verstehen.

Das Bundesministerium für Bildung und Forschung (BMBF) förderte bereits im Jahr 2018 das vom Verband der Automobilindustrie (VDA) unterstützte Projekt KI-Plattform[8], im Rahmen dessen ein Konzept für den Aufbau einer akteursübergreifenden Plattform für Lern- und Testdaten erarbeitet wurde, die Industrieübernahmen, Forschungsinstituten und Prüforganisationen gleichermaßen zur Verfügung stehen sollte. Diese sollte dem Entwickeln und Testen von autonomen Fahrzeugen dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) hat im Jahr 2019 mit hoher Industriebeteiligung eine Serie von KI-relevanten Förderprojekten gestartet. Um zukünftig automatisiertes Fahren unter Einbeziehung von KI-Methoden zu unterstützen, sollen im Rahmen der „VDA-Leitinitiative autonomes und vernetztes Fahren“ Datenstrukturen, Methoden und konkrete Algorithmen entwickelt werden. Die komplementär aufgesetzten Projekte verfügen über folgende Schwerpunkte:

- Methoden (KI Data Tooling) (VDA 2020a)
- Lernende Systeme (KI Delta Learning) (VDA 2020b)
- KI-Sicherheitsnachweise (KI-Absicherung VDA 2020c)
- Wissenskompetenz (KI-Wissen)

Auf Bundesebene gibt es Bestrebungen, Verkehrsdaten und -dienste zunehmend auf sogenannten Datenmarktplätzen der Allgemeinheit zur Verfügung zu stellen. Dies ermöglicht auch Analysen oder den Aufbau verknüpfender Dienste für weitere Akteure. Diese

8 Siehe https://www.elektronikforschung.de/projekte/ki-plattform

Dienstplattformen, wie beispielsweise die mCLOUD des Bundesministeriums für Verkehr und Infrastruktur (BMVI) oder der Mobilitätsdatenmarktplatz (MDM) des Bundesamts für Straßenwesen, bieten aber noch nicht die hochaufgelösten Datenqualitäten, die für KI-Anwendungen erforderlich sind (BMVI 2020; BASt 2020).

Hinzu kommen weitere Initiativen im nationalen sowie internationalen Bereich, die es ermöglichen sollen, Daten effizient und sicher auszutauschen. Zudem soll es auch möglich sein, die Dienste in die einzelnen Ökosysteme barrierefrei einzubinden oder verschiedene Ökosysteme miteinander zu verbinden und damit Mehrwerte zu generieren. Zu diesen Initiativen zählen unter anderem der Datenraum Mobilität (DRM) mit einem verkehrsübergreifenden und intermodalen Ansatz sowie GAIA-X (acatech 2020; BMWi 2020).

Mit GAIA-X, der gemeinsamen Initiative des BMWi und des BMBF, soll ein weltweit wettbewerbsfähiges offenes digitales Ökosystem entstehen, welches es ermöglicht, Unternehmen und Geschäftsmodelle aus Deutschland und Europa heraus zu vermarkten und anzuwenden. Dabei stehen sowohl die digitale Souveränität als auch die Skalierungsfähigkeit für Dienste- und Plattform-Anbieter im Vordergrund. Sie stellen die Basis für eine Vielzahl von Anwendungsgebieten dar. Ziel ist eine sichere und vernetzte Dateninfrastruktur, die den höchsten Ansprüchen an digitale Souveränität genügt und Innovationen fördert. In einem offenen und transparenten digitalen Ökosystem sollen Daten und Dienste verfügbar gemacht, zusammengeführt und vertrauensvoll geteilt werden können.

Mit dem Transfer-Projekt TPX hat das BMWi eine neue Aktivität für die Harmonisierung und den Wissensaustausch geschaffen, die projektübergreifend für die Projekte der VDA-Leitinitiative ein gemeinsames, praxisbezogenes Verständnis über Methoden, Werkzeuge und Standards zur Absicherung automatischer Fahrmanöver schaffen wird (DLR 2020). Neben den Projekten der PEGASUS-Familie SET Level 4to5 und VV-Methoden sind auch die vorstehend genannten BMWi KI-Projekte Bestandteil der Plattform TPX. Der Schwerpunkt liegt auf der Unterstützung der Vereinheitlichung von Datenstrukturen, Architekturen, Nutzung von Werkzeugen und gemeinsamen Spezifikationen sowie der Wissensverbreitung in diesem Kontext.

Das BMBF fördert im Projekt VIVID[9] die Entwicklung einer virtuellen Testumgebung für die Validierung von Sensorsystemen von autonomen Fahrzeugen. Als Bestandteil der deutsch-japanischen Forschungskooperation soll dort die Standardisierung und internationale Verbreitung der virtuellen Testmethode vorangetrieben werden. Bei der Entwicklung von Methoden zur Absicherung der Sensorsysteme autonomer Fahrzeuge anhand virtueller Daten steht VIVID im Austausch mit der PEGASUS-Projektfamilie.

9 Siehe https://www.elektronikforschung.de/projekte/vivid

TÜV Süd startete im Jahr 2019 die OpenGenesis-Initiative, um eine Validierungsplattform zu schaffen, deren Schlüsselmerkmale dem Konzept im vorliegenden Whitepaper sehr ähnlich sind. OpenGenesis fehlten allerdings von Beginn an potente Unterstützer aus dem Kreis der OEM oder Zulieferer, sodass kein geeignetes Momentum entstehen konnte.

Im Vergleich zu dieser Initiative unterscheidet sich der Konzeptvorschlag der Autorinnen und Autoren des vorliegenden Whitepapers in einer wesentlich fokussierteren Zielstellung in Bezug auf Corner Cases und einem spezifischeren Leistungsversprechen. Wie diese konkret aussehen, wird im nachfolgenden Kapitel ausgeführt.

4. Konzeption: KI-Plattform zum Datenaustausch in der Mobilität

Die gemeinschaftlich genutzte Plattform zum Austausch von Mobilitätsdaten leistet einen wichtigen Beitrag zur Risikominimierung im Bereich des automatisierten Fahrens. Als technische Vermittlungs-Plattform (Web-Service) sammelt sie Beispiele für Corner Cases. In einem weiteren Schritt kann sie auch eine Referenzlinie zur Risikoeinschätzung bilden und eine Möglichkeit zur Validierung von ML-Modellen bieten. Damit dient die Plattform sowohl dem Gemeinwohl erhöhter Sicherheit der Gesellschaft als auch den wirtschaftlichen Interessen auf nationaler und europäischer Ebene. Denn automatisierte Fahrzeuge werden im laufenden Betrieb trotz einer hohen Anzahl und qualitativ hochwertiger Trainingsdaten weiterhin auf Corner Cases reagieren müssen. Es ist deshalb wichtig, diese Fälle einordnen zu können und mit der gesamten Fahrzeugflotte zu teilen.

Ziel der Mobilitätsplattform ist es, aus den gesammelten Daten von bereits identifizierten Corner Cases zu lernen, um diese Erkenntnisse auf andere KI-Systeme übertragen zu können. Die Plattform soll deshalb

1. Daten aggregieren können, mit denen unterschiedliche KI-Modelle getestet werden können. Die Abhängigkeit von bestimmten Sensor-Modalitäten und -Konfigurationen ist dabei explizit darzustellen.
2. die Entwicklung eines Annotationsformats und Standards vorantreiben, um die Vergleichbarkeit der unterschiedlichen Modelle zu ermöglichen.
3. Trainings- und Testdaten für die Forschung und Entwicklung zugänglich machen und so zu weiteren Erkenntnissen bezüglich des Agierens bei Unbekanntem führen.

Es wird auch zukünftig die Herausforderung bestehen, weitere Corner Cases zu identifizieren und in die Plattform aufzunehmen. Denn es ist niemals vollständig feststellbar, welche Fehler (sogenannte „unknown unknowns“) in der Zukunft noch zu erwarten sind. Daraus ist ein dauerhafter Bedarf für eine solche Plattform ableitbar.

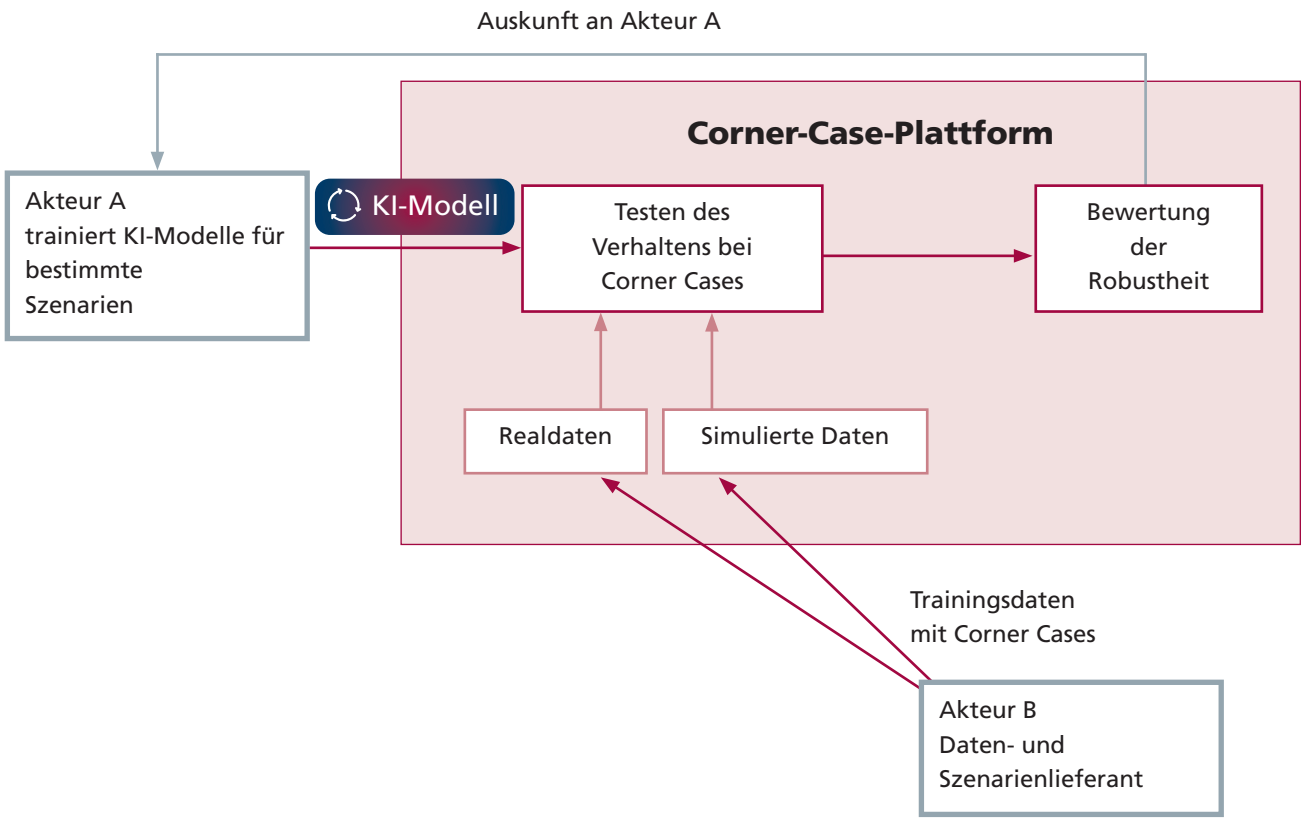
Funktionsweise

Die Plattform ermöglicht es allen Akteuren der gesamten Wertschöpfungskette[10], dieselbe Infrastruktur zu nutzen, um die Robustheit eigener KI-Modelle auf Corner Cases hin testen und bewerten lassen zu können. Dies setzt natürlich voraus, dass es sich um Software-Artefakte mit ähnlichen architekturellen Grundvoraussetzungen handelt und diese auf einer Plattform ausgeführt werden können. Dies schließt Modelle aus, die nur auf spezifischen

10 In der Industrie sind das unter anderem sogenannte Original Equipment Manufacturer (OEM), Zulieferer von Komponenten, Hersteller von Kameras, Sensoren etc.

Hardware-Plattformen betrieben werden können. Dazu müssen auf der Plattform Szenarien mit Corner Cases verfügbar sein. KI-Modelle können hochgeladen werden, und das Verhalten der KI-Systeme hinsichtlich dieser Szenarien kann überprüft und ausgewertet werden. Im Anschluss wird die Bewertung als Feedback beispielsweise an die Flottenbetreiber kommuniziert, sodass diese ihre entsprechenden Modelle aktualisieren und wiederum in ihren Flotten verteilen können. In einer weiteren Ausbaustufe ist es denkbar, dass ein Nachtraining der KI-Systeme direkt auf der Plattform erfolgen kann und zertifizierte Updates direkt über die Plattform verteilt werden können. Die Plattform ermöglicht damit den Austausch sowohl zwischen Akteuren, etwa Flottenbetreibern, die ihre Modelle testen und in ihrer Robustheit verbessern möchten, als auch zwischen Akteuren, die über Corner-Case-Szenarien verfügen oder über Trainingsdaten, mit denen Wahrnehmungsfehler nachtrainiert und Modelle somit robuster gestaltet werden können (siehe Abbildung 2). Die dabei entstehenden Informationen über Unterschiede zwischen dem ursprünglichen Training und dem Nachtraining können als Anpassung zugrunde liegender Labeling-Modelle (Konnotationsmodelle) aufgefasst werden und zur Verbesserung des Wissens über die Corner Cases beitragen.

Abbildung 2: Vereinfachte Darstellung der Funktionsweise der Corner-Case-Plattform



Technisch funktioniert das Testen auf der Plattform über einen Test der Datenquellen der ML-Modelle. Das Ergebnis gibt den Akteuren Auskunft über die Robustheit ihrer hochgeladenen Modelle und kann Hinweise auf Planungs- oder Wahrnehmungsfehler geben. Auf Basis dieser Einschätzung kann das Modell dann weiter verbessert werden. So könnte beispielsweise die Bilddatenerkennung von Kamerasensoren geprüft werden. Der Hersteller der Kamera kann das eigene KI-Modell auf die Plattform laden und dort die Bilddatenerkennung bewerten lassen. Hierfür muss eine standardisierte Schnittstelle geschaffen werden (Sensorschnittstelle, Computer-HW-Schnittstelle, Speicherschnittstelle für die Modellausgaben). Es bieten sich dafür bestehende Standards (Containerisierung, ONNX, ASAM Open Label etc.) an. Das eigentliche Testen kann abhängig vom Testobjekt sowohl mit Realdaten als auch mit simulierten Daten erfolgen. Danach wird die Bewertung des KI-Modells wieder an den Hersteller zurückgespielt. Um datenschutzrelevante Vorbehalte abzubauen, kann auf diese Weise der Zugriff auf potenziell personenbezogene Testdaten auf die Betreiber der Plattform minimiert werden. Die Kunden erhalten lediglich eine anonymisierte Bewertung der Robustheit und Performanz der getesteten Modelle. Die Plattform bildet damit eine Grundlage sowohl für die Validierung als auch für die Verifizierung über die gesamte Entwicklungsprozesskette und auf den verschiedenen Teilsystemstufen.

Für das automatisierte Fahren ist die Validierung auf sorgfältig erzeugten und kuratierten Referenzdatensätzen wichtiger Bestandteil von Sicherheitsnachweisen und Zulassungsprozessen. Schlüssel dieser Qualitätskontrolle ist insbesondere eine intelligente Stichprobenerhebung des Eingabeparameter-Raumes, welches die Berücksichtigung von Corner Cases und deren Analyse erfordert. Das seltene Auftreten von Corner Cases in der Realität macht wiederum diese Untersuchung in der Praxis mühsam und schwierig. Die Skalierungseffekte einer Mobilitätsplattform werden die Erstellung eines solchen Referenzdatensatzes entscheidend begünstigen. Denn die Vorgehensweisen zur Identifizierung neuer Corner Cases sind Basis für die Forschung und Entwicklung von Methoden zur (automatisierten) Identifizierung weiterer Corner Cases und der zugehörigen Konnotationen (Labels) von Corner-Case-bezogenen Daten.

Konzeption des Betreibermodells der KI-Mobilitätsdatenplattform

Das Betreibermodell der Plattform sieht einen transaktionsbasierten Service vor, sodass die Plattform sich finanziell selbst trägt. Um Modelle auf die Plattform hochladen zu können und validieren zu lassen, sollen die am Service interessierten Akteure einen geringfügigen finanziellen Betrag leisten. Dieser kommt wiederum den Akteuren zugute, die die Modelle in ihrer Robustheit verbessern.

Eine neutrale Institution könnte die Plattform betreiben, etwa das Straßenbauamt, der TÜV oder weitere Prüf- und Zulassungsstellen. Sie sollen dadurch auch Zulassungen für ML-Modelle anbieten können, die selten auftretende Corner Cases berücksichtigen. Um den Mehrwert der Plattformnutzung für die Akteure zu vergrößern, bedarf es der Einführung eines vertrauenswürdigen Siegels. Der Plattform-Betreiber soll dieses vergeben und damit die getesteten, robusten ML-Modelle nach aktuellem Forschungsstand auszeichnen.

Dies ist für die nutzenden Akteure von Vorteil, weil sie keine eigenen aufwändigen Verfahren für die Prüfung der Modelle aufsetzen müssen und zudem eine Bescheinigung für ihr vertrauenswürdiges ML-Modell von dem unabhängigen Plattform-Betreiber erhalten. Voraussetzung hierfür sind hohe Sicherheitsanforderungen und Vertrauenswürdigkeit, die seitens des Betreibers gegeben sein müssen. Der steigende Wettbewerbsdruck auf die Akteure verstärkt dies zusätzlich. Dies zeigt sich beispielsweise, wenn das Modell von Akteur A besser bewertet wird als das Modell von Akteur B und Letzterer hiermit einen Wettbewerbsnachteil spüren könnte. Auch wenn Akteur A das nach aktuellem Stand beste Modell auf dem Markt hätte, könnte dieser sich nach Austausch auf der Plattform um ein mögliches Ausspionieren oder Kopieren sorgen. Um diesen Fällen vorzubeugen, muss der vertrauenswürdige, neutrale Plattform-Betreiber seine Sicherheits- und Datenschutzanforderungen transparent machen.

Wie die Realisierung des skizzierten Plattformkonzepts zur Verbesserung des automatisierten Fahrens gelingen kann und welche Faktoren dabei eine wesentliche Rolle spielen, zeigen die Autorinnen und Autoren im nachfolgenden Kapitel auf.

5. Gestaltungsoptionen und Perspektiven

Um die Potenziale des industrieübergreifenden Flottenlernens zu erschließen und eine Risikominimierung des automatisierten Fahrens zu erreichen, schlagen die Autorinnen und Autoren des vorliegenden Whitepapers die Gründung einer gemeinschaftlichen KI-Mobilitätsdatenplattform vor. Sie möchten mit diesem Impuls einen Beitrag zur Risikoeinschätzung leisten, der eine Grundlage für das Vorantreiben von Standardisierung und Regulierung von KI-Systemen in der Mobilität schafft. Der Nutzen für Hersteller und Technologieentwickler einer solchen Plattform, die ein „Benchmarking" erlaubt, ist evident. Dafür sind Gestaltungsoptionen und Rahmenbedingungen für die Umsetzung des Vorhabens nötig, die sich insbesondere an Akteure aus Politik und Wirtschaft richten. Sie schließen an die Empfehlungen der KI-Normungsroadmap und des Whitepapers *Zertifizierung von KI-Systemen* der Plattform Lernende Systeme an (vgl. Heesen et al. 2020).

Darüber hinaus weisen die Autorinnen und Autoren darauf hin, wie die Plattform in die Realität umgesetzt werden kann, und legen dar, welcher Forschungsbedarf weiterhin notwendig ist, um in diesem Feld eine Spitzenposition zu erreichen oder zu behaupten, und welche offenen Fragen noch zu lösen sind.

Internationale Standardisierung von Datenformaten vorantreiben

Wesentliche Gelingensbedingung für die KI-Mobilitätsdatenplattform sind Standards für die Modellierung und Austauschformate von Daten, die den Zugang zu gemeinsamen Tools und Technologien ermöglichen, etwa der Verwendung einer gemeinsamen Sprache und Methoden für die Plattform-Anwender. Dies ist auch eine wesentliche Voraussetzung, um ein „Benchmarking" und eine Vergleichbarkeit herzustellen. Nur mithilfe standardisierter Datenformate, Schnittstellen und Protokolle können Corner Cases unabhängig von der Sensor-Konfiguration oder dem Fahrzeugtyp auf der Plattform kategorisiert werden. Hierfür müssen eindeutige Referenzdatensätze sogenannter open-Formate (siehe ASAM e. V.) festgelegt werden. Darüber hinaus bedarf es für die Übertragbarkeit von Modellen standardisierter Simulationsumgebungen einschließlich standardisierter Modelle für diese Umgebungen.

Zu Standards gehören auch Wegweiser für Prozesse und Methodologien. Der Plattform-Betreiber muss eindeutige Richtlinien für den Zugang und die Handhabung der Daten definieren. Selbstverständlich müssen diese nach rechtlichen und ethischen Aspekten gestaltet werden und somit frühzeitig Fragen der Haftung sowie rechtliche Rahmenbedingungen geklärt sein. Die Zusammenarbeit der verschiedenen Akteure bedarf einer

Methodenbeschreibung aller Kernanwendungsfälle der Plattform. Dies beinhaltet die Beschreibung von Prozessschritten, Akteuren und deren Rollen, Werkzeugen, Konnotationsverfahren, Artefakten und Schnittstellen.

Gründung einer finanziell selbsttragenden Plattform unterstützen

Die Autorinnen und Autoren schlagen vor, dass die Plattform über ein privatwirtschaftliches Konsortium getragen wird. Sie empfehlen die Gründung der finanziell selbsttragenden Plattform über ein öffentlich gefördertes Projekt. Voraussetzung für eine gelingende Realisierung der Plattform ist die Anerkennung der angebotenen Dienstleistungen seitens der Politik, aber auch der Industrie. Eine stärkere Einbindung der Industrie und Wirtschaft bereits in der Gründungsphase wird insbesondere dann möglich sein, wenn die Leistung der Plattform nicht nur anerkannt, sondern gefordert ist. Nur wenn eine Risikoeinordnung über ein Benchmarking, wie das über die Plattform, möglich ist – zum Beispiel als Basis für Zulassungsprozesse – und zudem eine belohnende Regelung zu Risikomanagement von KI-Systemen eingeführt wird, ist die Plattform tragfähig und kann ihren Nutzen für Hersteller und Technologielieferanten insbesondere aus Mittelstand und Forschung entfalten.

Die Expertinnen und Experten schlagen darüber hinaus einen Förderaufruf für ein Vorbereitungsprojekt vor, das laufende, thematisch verwandte Aktivitäten verschiedener Akteure[11] konsolidiert. Der Förderaufruf richtet sich sowohl an die Industrie als auch an die öffentliche Hand. Zudem bedarf es eines Betreiberkonzepts, das alle notwendigen organisatorisch-rechtlichen Aspekte abbildet und vom Konsortium umgesetzt werden kann. Es bedarf zusätzlich weiterer Anwendungsprojekte, um den Transfer des Flottenlernens in die Vorentwicklung zu befördern.

Community für die KI-Mobilitätsdatenplattform aufbauen

Die Plattform soll als aktiver Anwender dieser Standards einen Austausch mit Standardisierungsgremien und verwandten Initiativen etablieren, zum Beispiel mit dem Projekt KI Data Tooling der VDA-Leitinitiative.

Die Bedeutung der Standardisierung von Datenaustauschformaten zahlt auch auf die zukünftige Relevanz der Plattform als gemeinschaftliche Plattform ein. Eine rein technische Handhabung des Datenaustauschs kann dieses Ziel nicht allein unterstützen. Das Konzept einer solchen gemeinschaftlichen Plattform bedarf moderner Gestaltungsansätze, um verschiedene Partner und Akteure in Wirtschaft und Wissenschaft zu aktiven Beiträgen zu motivieren und den Nutzen und die Ergebnisse der durch die Plattform erfolgten Analysen zu motivieren. Die Ergebnisse einer Robustheitsbewertung sind zunächst

11 Dazu gehören Projekte wie GAIA-X, VDA-Leitinitiative für Künstliche Intelligenz oder auch Akteure wie die Pegasus-Familie und relevante Institutionen, z. B. TÜV.

einmal sehr abstrakt und müssen zielgruppenorientiert erklärt und visualisiert werden. Hier ist auch in der grundsätzlichen Mensch-Maschine-Interaktion und der Gestaltung von Schnittstellen noch echter Forschungsbedarf gegeben. Hier können kollaborations- und kundenzentrierte Entwicklungsmodelle unterstützend wirken, wie zum Beispiel agile Methoden und Design Thinking.

Investition in Forschung erhöhen und Forschungsfragen adressieren

Eine Risikominimierung des industrieübergreifenden Flottenlernens im Bereich des automatisierten Fahrens kann aus der Sicht der Autorinnen und Autoren nur erreicht werden, wenn die folgenden offenen Forschungsfragen adressiert werden. Sie zielen ab auf die Beschreibung, Identifikation und Bewertung von Corner Cases:

- **Beschreiben:** Wie erreicht man Beschreibungen von Corner Cases, die eine Übertragbarkeit tatsächlich ermöglichen? Gibt es eine Klasse von Corner Cases (oder kritischen Szenarien), die einerseits spezifisch genug sind, um als sinnvolle Ausgangsbasis für Assessment-Methoden von KI-basierten Fahrautomatisierungsfunktionen herangezogen werden zu können, aber andererseits auch eine gewisse Allgemeingültigkeit besitzen (also sich nicht auf ein individuelles System beziehen)?
- **Identifizieren:** Welche Methoden sind geeignet, um diese Art von Corner Cases zu identifizieren und sicherzustellen, dass eine ausreichend hohe Abdeckung dieser erreicht wurde?
- **Bewerten:** Wie können Eigenschaften von Modellen systematisch anhand von Simulations- und Realdaten bewertet werden?

Nur wenn die Gestaltungsoptionen und Rahmenbedingungen seitens der Politik und der Wirtschaft entsprechend zeitnah umgesetzt werden, kann ein wichtiger Beitrag zu einer vertrauenswürdigen KI geleistet werden. Die Risikominimierung im Bereich des automatisierten Fahrens kann ihre Einführung wesentlich beschleunigen.

Literatur

acatech (2020): Datenraum Mobilität, München. https://www.acatech.de/projekt/datenraum-mobilitaet/ (abgerufen am: 02.12.2020).

Bundesanstalt für Straßenwesen (BASt) (2020): MDM-Plattform – der Nationale Zugangspunkt für Mobilitätsdaten, Bergisch Gladbach. https://www.mdm-portal.de (abgerufen am: 02.12.2020).

Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) (2020): mCloud. Das offene Datenportal des BMVI, Bonn. https://www.mcloud.de/web/guest (abgerufen am: 02.12.2020).

Bundesministerium für Wirtschaft und Energie (BMWi) (2020): GAIA-X. Eine vernetzte Datenstruktur für ein europäisches digitales Ökosystem, Berlin. https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.html (abgerufen am: 02.12.2020).

Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR) (2020): TPX – Transfer Project Exchange, Braunschweig. https://transfer-project-exchange.com (abgerufen am: 02.12.2020).

DIN/DKE (2020): Deutsche Normungsroadmap Künstliche Intelligenz, Berlin/Frankfurt am Main. https://www.din.de/resource/blob/772438/ecb20518d982843c3f8b0cd106f13881/normungsroadmap-ki-data.pdf (abgerufen am: 02.12.2020).

Heesen, J. et al. (Hrsg.) (2020): Zertifizierung von KI-Systemen – Kompass für die Entwicklung und Anwendung vertrauenswürdiger KI-Systeme. Whitepaper aus der Plattform Lernende Systeme, München. https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG3_Whitepaper_EB_200831.pdf (abgerufen am: 16.02.2021).

Kargupta, H., Sarkar, K., Gilligan, M. (2010): MineFleet: an overview of a widely adopted distributed vehicle performance data mining system. Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining, 37–46, 2010.

Plattform Lernende Systeme (2019): Auf dem Weg zu einem intelligenten Mobilitätsraum. Bericht der Arbeitsgruppe Mobilität und intelligente Verkehrssysteme, München. https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG5_Bericht_280619.pdf (abgerufen am: 02.12.2020).

Projekt „KI-Familie" der VDA-Leitinitiative (2020a): KI Data Tooling, Berlin (Projektkoordination: BMW AG). https://ki-datatooling.vdali.de (abgerufen am: 02.12.2020).

Projekt „KI-Familie“ der VDA-Leitinitiative (2020b): KI-Delta-Learning, Berlin (Projektkoordination: Mercedes-Benz AG). https://www.ki-deltalearning.de/footer-menu (abgerufen am: 02.12.2020).

Projekt „KI-Familie“ der VDA-Leitinitiative (2020c): KI-Absicherung, Berlin (Projektkoordination: Volkswagen AG). https://www.ki-absicherung-projekt.de (abgerufen am: 02.12.2020).

SAE 2018 SAE International (2018): Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (J3016), 2018. https://www.sae.org/standards/content/j3016_201806/ (abgerufen am 12.02.2021).

Sopra Steria Consulting / F.A.Z. Institut (2019): Branchenkompass Automotive 2019 – Mehr Standbeine für neues Wachstum, Hamburg. https://www.soprasteria.de/newsroom/publikationen/branchenkompass-automotive-2019 (abgerufen am: 02.12.2020).

Über dieses Whitepaper

Dieses Whitepaper wurde von der Arbeitsgruppe Mobilität, intelligente Verkehrssysteme der Plattform Lernende Systeme erstellt. Als eine von insgesamt sieben Arbeitsgruppen untersucht sie, wie Lernende Systeme unsere Mobilitätsstrukturen verändern und welche Eigenschaften sie haben müssen, um den größten Nutzen für Individuum und Gesellschaft zu erzielen. Die Arbeitsgruppe hinterfragt, wie Infrastrukturen und Systemarchitekturen im Mobilitätssektor weiterentwickelt werden müssen, um Lernende Systeme sinnvoll zu integrieren.

Autorinnen und Autoren
Dr. Tobias Hesse, Deutsches Zentrum für Luft- und Raumfahrt (DLR)
Dr. Christoph Peylo, Bosch Center for Artificial Intelligence (BCAI)
Dr. Claus Bahlmann, Siemens Mobility GmbH
Dr. Astrid Elbe, Intel Corporation
Igor Neiva Camargo, Continental Automotive GmbH
Prof. Dr. Philipp Slusallek, DFKI GmbH

Autorinnen und Autoren mit Gaststatus
Dr. Christian Müller, DFKI GmbH
Dipl.-Ing. Sascha Ott, Karlsruher Institut für Technologie (KIT)
Dr. Fabian Oboril, Intel Corporation
Dr. Kay-Ulrich Scholl, Intel Corporation

Die Arbeitsgruppe wird geleitet von
Dr. Tobias Hesse, Deutsches Zentrum für Luft- und Raumfahrt (DLR)
Dr. Christoph Peylo, Bosch Center for Artificial Intelligence (BCAI)

Mitglieder der AG sind
Prof. Dr. Dr. Albert Albers, Karlsruher Institut für Technologie (KIT)
Dr. Claus Bahlmann, Siemens Mobility GmbH
Prof. Dr. Fabian Behrendt, Fraunhofer-Institut für Fabrikbetrieb und -automatisierung IFF
Dr. Astrid Elbe, Intel Corporation
Prof. Dr. Stefanos Fasoulas, Universität Stuttgart
Dr. Rudolf Felix, PSI FLS Fuzzy Logik & Neuro Systeme GmbH für PSI Software AG
Prof. Dr. Axel Hahn, OFFIS/Universität Oldenburg
Dr. Sören Kerner, Fraunhofer-Institut für Materialfluss und Logistik IML
Hans Kolß, Flixbus GmbH
Igor Neiva Camargo, Continental Automotive GmbH
Prof. Dr. Ilja Radusch, Fraunhofer FOKUS, TU Berlin/DCAITI
Dr. Peter Schlicht, Volkswagen AG
Prof. Dr. Philipp Slusallek, DFKI GmbH
Dr. Anatoly Sherman, SICK AG
Prof. Dr. J. Marius Zöllner, FZI Forschungszentrum Informatik

Die Arbeitsgruppe wird unterstützt von
Dr. Corina Apachite, Continental Automotive GmbH
Richard Goebelt, VdTÜV
Dr. Tim Gutheit, Infineon
Dr. Christian Müller, DFKI GmbH
Dipl.-Ing. Sascha Ott, Karlsruher Institut für Technologie (KIT)

Redaktion
Rebecca Ebner, Geschäftsstelle der Plattform Lernende Systeme
Dr. Erduana Wald, Geschäftsstelle der Plattform Lernende Systeme
Dr. Ursula Ohliger, Geschäftsstelle der Plattform Lernende Systeme

Über die Plattform Lernende Systeme

Lernende Systeme im Sinne der Gesellschaft zu gestalten – mit diesem Anspruch wurde die Plattform Lernende Systeme im Jahr 2017 vom Bundesministerium für Bildung und Forschung (BMBF) auf Anregung des Fachforums Autonome Systeme des Hightech-Forums und acatech – Deutsche Akademie der Technikwissenschaften initiiert. Die Plattform bündelt die vorhandene Expertise im Bereich Künstliche Intelligenz und unterstützt den weiteren Weg Deutschlands zu einem international führenden Technologieanbieter. Die rund 200 Mitglieder der Plattform sind in Arbeitsgruppen und einem Lenkungskreis organisiert. Sie zeigen den persönlichen, gesellschaftlichen und wirtschaftlichen Nutzen von Lernenden Systemen auf und benennen Herausforderungen und Gestaltungsoptionen.

Impressum

Herausgeber
Lernende Systeme –
Die Plattform für Künstliche Intelligenz
Geschäftsstelle | c/o acatech
Karolinenplatz 4 | 80333 München
www.plattform-lernende-systeme.de

Gestaltung und Produktion
PRpetuum GmbH, München

Stand
Februar 2021

Bildnachweis
zapp2photo/AdobeStock/Titel

Bei Fragen oder Anmerkungen zu dieser Publikation kontaktieren Sie bitte Johannes Winter (Leiter der Geschäftsstelle):
kontakt@plattform-lernende-systeme.de

Folgen Sie uns auf Twitter: @LernendeSysteme

Empfohlene Zitierweise
Tobias Hesse, Christoph Peylo et al. (Hrsg.):
Potenziale für industrieübergreifendes Flottenlernen – KI-Mobilitätsdatenplattform zur Risikominimierung des automatisierten Fahrens. Whitepaper aus der Plattform Lernende Systeme, München 2021