Zur Veröffentlichung

Neues Forschungsprojekt *Safe AI Engineering* gestartet – für mehr Sicherheit beim automatisierten Fahren

Berlin, 19.03.2025 – Für die Akzeptanz der Nutzenden spielt das Thema Sicherheit eine zentrale Rolle bei der Entwicklung autonomer Fahrzeuge. Mit dem Einsatz von Künstlicher Intelligenz (KI) verschärfen sich die Anforderungen an die Absicherung autonomer Fahrfunktionen noch weiter. Genau an dieser Stelle setzt das am 1. März gestartete Forschungsprojekt *Safe AI Engineering* an: Mehr Sicherheit und eine bessere Integration von KI stehen im Mittelpunkt des Vorhabens, an dem 24 Partner aus Industrie und Wissenschaft beteiligt sind. Während der dreijährigen Laufzeit werden praxistaugliche Methoden entwickelt, welche die Sicherheit einer KI-Funktion über ihren gesamten Lebenszyklus hinweg gewährleisten.

Ziel des Projekts ist es, eine Methodik zur ganzheitlichen Absicherung von KI-Funktionen im automatisierten Fahren zu entwickeln – von der Planung über Entwicklung, Tests, Anwendung und Monitoring bis hin zur kontinuierlichen Verbesserung. Einem begleitenden Sicherheitsnachweis kommt deshalb eine besondere Bedeutung zu. Hierzu wird ein praxistauglicher Ansatz erarbeitet, um die internationale Führungsrolle der deutschen Automobilindustrie im sicheren autonomen Fahren weiter zu stärken.

Was sind die Kerninnovationen von Safe AI Engineering?
Das Projekt verknüpft Sicherheitsanforderungen direkt mit dem AI (Artificial Intelligence)-Engineering, welches die systematische Entwicklung, Implementierung und Wartung von KI-Systemen über ihren gesamten Lebenszyklus umfasst. Dabei werden hochwertige Trainings- und Validierungsdaten, einschließlich synthetischer Daten, vereinheitlicht, so dass diese unabhängig vom initialen System verwendet werden können. Dies ermöglicht langfristig eine bessere und nachhaltigere Datennutzung und reduziert dadurch Kosten. Zudem werden erklärbare, robuste Absicherungsmethoden entwickelt, um die Nachvollziehbarkeit bei der Bewertung der Leistungsfähigkeit einer KI weiter zu verbessern. Die Einführung einer evidenzbasierten Überwachung von KI-Modellen sichert die kontinuierliche Verbesserung dieser Modelle auch zur Laufzeit eines automatisierten Fahrzeugs. Zum Abschluss des Projekts werden die Methoden in praxisrelevanten Umgebungen erprobt und bewertet.

Wo setzt das Projekt an?
Safe AI Engineering soll die Lücke zwischen Verifikation & Validierung (V&V) und Sicherheitsnachweisen für KI schließen. Dazu werden bestehende Normen wie ISO 26262, SOTIF (ISO/PAS 21448) und ISO/PAS 8800 integriert, die internationale Standards für KI-Funktionen setzen. Das Vorhaben fügt sich nahtlos in die Projektlandschaft der VDA Leitinitiative autonomes und vernetztes Fahren ein und ist Teil der zweiten Generation der KI Familie zusammen mit den Projekten jbDATA und nxtAIM. Die Methodik wird anhand einer KI-Perzeptionsfunktion zur Fußgängererkennung erarbeitet und in drei Anwendungsfällen mit steigender Komplexität getestet: Von einer statischen Szene mit einem Fußgänger bis hin zu dynamischen, realitätsnahen Verkehrssituationen.

Wie wirkt das Projekt in die Zukunft?
Das Projekt Safe AI Engineering trägt maßgeblich zur sicheren Integration von KI in Fahrzeugen bei und soll langfristig einen Standard für die Absicherung KI-basierter Funktionen im automatisierten Fahren ermöglichen. Die entwickelte Methodik kann bei einer behördlichen Zulassung von automatisierten Fahrzeugen unterstützen und insbesondere eine einheitliche

Bewertung ermöglichen. Fahrzeughersteller und Zulieferer profitieren deshalb unmittelbar von einer solchen Methodik, die den gesamten KI-Lebenszyklus umfasst. Behörden können in Bezug auf die Methodik insbesondere auf Transparenz und Nachvollziehbarkeit setzen. Dies ermöglicht langfristig eine schnellere Einführung entsprechender automatisierter Fahrfunktionen. Nutzende erhalten ein automatisiertes Fahrzeug, in dem KI-Funktionen sicher und zuverlässig arbeiten.

Gefördert vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) ist das Projekt Safe AI Engineering ein konsequenter nächster Schritt in Richtung autonomer Mobilität – vorangetrieben von starken Partnern aus Industrie und Forschung in Deutschland. Die Projektpartner stellen bestehende Fahrzeuge, Daten und Hardware zur Verfügung, die in vorherigen Forschungsprojekten erarbeitet wurden. Safe AI Engineering leistet damit einen entscheidenden Beitrag für eine sichere, skalierbare und zukunftsfähige Integration von KI in automatisierte Mobilitätssysteme.

Projekt: Safe AI Engineering – Sicherheitsargumentation-befähigendes AI Engineering über den gesamten Lebenszyklus einer KI-Funktion

Website: www.safe-ai-engineering.de
LinkedIn: linkedin.com/company/ki-familie

Dauer: 36 Monate | März 2025 – Februar 2028

Projektbudget: 34,5 Mio. €

Fördervolumen: 17,2 Mio. €

Koordinatoren: Dr. Ulrich Wurstbauer, DXC Luxoft; Prof. Dr. Frank Köster, DLR-Institut für KI-Sicherheit

Anzahl der Partner: 24

Partner: DXC Luxoft GmbH, Deutsches Zentrum für Luft- und Raumfahrt e.V., Akkodis Germany GmbH, AVL Deutschland GmbH, Bundesanstalt für Straßen- und Verkehrswesen, Bertrandt Ing.-Büro GmbH, Robert Bosch GmbH, Capgemini Engineering Deutschland S.A.S. & Co KG, Cariad SE, Continental Automotive Technologies GmbH, Fraunhofer-Gesellschaft e.V., FZI Forschungszentrum Informatik, Intel Deutschland GmbH, Karlsruhe Institute of Technology (KIT), Mercedes-Benz AG, Opel Automobile GmbH, Porsche AG, Spleenlab GmbH, Technische Universität Berlin, Technische Universität Braunschweig, TÜV AI.Lab GmbH, Valeo Schalter und Sensoren GmbH, ZF Friedrichshafen AG

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages