Als wir im Jahr 2016 zum ersten Mal auf den einschlägigen Konferenzen unser Konzept der digitalen Realität vorgestellt haben, begegnete man uns einerseits mit großem Interesse, weil ganz offensichtlich die Lösung für ein Problem skizziert wurde, das insbesondere im Zusammenhang Weiterentwicklung von hochautomatisierten Fahrzeugen bestand, andererseits jedoch auch mit einem hohen Maß an Skepsis, denn die simulationsbasierte KI befand sich damals noch in den Kinderschuhen.

Heute sind synthetische Daten ein fester Bestandteil der Entwicklung, der Validierung und letzten Endes auch bei der Zertifizierung von Lernenden Systemen und somit kann das Konzept der digitalen Realität als richtungsweisend bezeichnet werden. In Zeiten, in denen sich der Begriff des digitalen Zwillings für bestimmte Aspekte dieser Idee durchgesetzt hat und in denen große Projektfamilien wie die VDA Leitinitiative es als selbstverständlich erachten mit synthetischen Daten zu arbeiten, möchten wir darauf hinweisen, dass die Simulation an sich nur das Ergebnis eines Prozesses ist, bei dem KI eine große Rolle spielen kann. Das Konzept der digitalen Realität beschreibt nämlich ein Verfahren, bei dem die Inhalte der Simulation durch KI erzeugt werden. Dadurch erreichen wir ein höheres Maß von Flexibilität, Validität im Sinne von Vergleichbarkeit mit realen Daten, und letzten Endes auch Skalierbarkeit, da kein menschlicher Designer erforderlich ist, um die Simulation auszugestalten. Funktionale Sicherheit für kritische Systeme insbesondere. Der Transport von Menschen und Gütern ist zu einer Frage der Qualität von Daten geworden.

Prof. Dr.-Ing. Philipp Slusallek |
Deutsches Forschungszentrum für Künstliche Intelligenz GmbH

SafeTRANS
SAFETY IN TRANSPORTATION SYSTEMS

NEWS

SafeTRANS News 1/2021

Digitale Realitäten - Sicherheit durch künstliche Intelligenz

IMPRESSUM

Herausgeber:
SafeTRANS e.V.
Escherweg 2, 26121 Oldenburg
Tel.: 0441 / 9722 540
Fax: 0441 / 9722 502
E-Mail: info@safetrans-de.org
Web: www.safetrans-de.org

Vorstand:
Prof. Dr. Werner Damm, Carl von Ossietzky Universität Oldenburg
Prof. Dr. Karsten Lemmer, DLR
Martin Rothfelder, Siemens AG

Sitz des Vereins: Oldenburg (Oldb)
Vereinsregister: VR 200314
Steuernummer: 64/220/15287

Redaktion und Layout:
Franziska Griebel
Escherweg 2, 26121 Oldenburg
Tel.: 0441 / 9722 540
Fax: 0441 / 9722 502
E-Mail: redaktion@safetrans-de.org

Bildmaterial:
Bonnie Bartusch, BTC Embedded Systems, Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, DLR Systems Engineering für zukünftige Mobilität, ICS GmbH, INGenX Technologies GmbH, OFFIS, Parasoft, SafeTRANS, Shutterstock, TU Kaiserslautern,
Titelseite: © eyetronic/Adobe Stock, Seite 12/13: © Ico Maker/Adobe Stock

Druck:
officina DRUCK Behrens Druck- und Verlags-GmbH, Oldenburg

Ausgabe:
SafeTRANS News 1/2021 werden im Juni 2021 veröffentlicht und kostenlos abgegeben.

SafeTRANS News 1/2021

Aktuelle Meldungen

Neues aus dem Forschungs- und Wirtschaftsumfeld

Neues Mitglied bei SafeTRANS: Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI)

Seit 2021 ist das Deutsche Forschungszentrum für Künstliche Intelligenz GmbH Mitglied in SafeTRANS.
Das DFKI ist auf dem Gebiet innovativer Softwaretechnologien auf der Basis von Methoden der Künstlichen Intelligenz eine führende wirtschaftsnahe Forschungseinrichtung Deutschlands. In der internationalen Wissenschaftswelt zählt das DFKI zu den wichtigsten „Centers of Excellence“. Es unterhält Standorte in Kaiserslautern, Saarbrücken, Bremen, ein Projektbüro in Berlin, ein Labor in Niedersachsen (Oldenburg und Osnabrück) und Außenstellen in St. Wendel und Trier.
Aktuell forschen ca. 1.080 Mitarbeiter aus über 65 Nationen an innovativen Software-Lösungen mit u. a. diesen inhaltlichen Schwerpunkten: Smarte Daten & Wissensdienste, Cyber-Physical Systems, Robotik, Eingebettete Intelligenz, Smart Service Engineering, Intelligente Netze, Agenten und Simulierte Realität, Kognitive Assistenzsysteme, Innovative Fabriksysteme, Marine Perception und Interaktives Maschinelles Lernen.
www.dfki.de

Start des Projektes „AORTA – die automatisierte Rettungsgasse für Einsatzfahrzeuge“

Das Forschungsprojekt AORTA nutzt künstliche Intelligenz und die Automatisierung von Fahrzeugen, um das Bilden einer Rettungsgasse zu unterstützen und so Leben zu retten.
In Notsituationen wie Verkehrsunfällen und Unglücken zählt jede Sekunde, und eine schnell und korrekt gebildete Rettungsgasse kann lebensrettende Auswirkung haben. Rettungsdienstverbände schätzen, dass ein um vier Minuten früheres Eintreffen der Einsatzkräfte die Überlebenschancen um bis zu 40% steigert. Eine korrekt und rechtzeitig gebildete Rettungsgasse ist jedoch selten vorzufinden und ohne das vorausschauende und umsichtige Handeln aller Verkehrsteilnehmer schwierig umzusetzen. Vielen Autofahrern fehlt der Überblick über die Situation des gesamten Verkehrs um sie herum, weshalb sie oft nicht richtig reagieren. So bleiben die Einsatzfahrzeuge im Stau stecken und verlieren wertvolle Zeit.
Im Januar startete das Forschungs- und Entwicklungsprojekt AORTA (Automatisierte Bildung von Rettungsgassen in komplexen Szenarien durch intelligente Vernetzung). Ein Konsortium aus elf Forschungseinrichtungen, öffentlichen Institutionen und Industriepartnern unter der Leitung der Technischen Universität Kaiserslautern erforscht und erprobt in AORTA die automatisierte Bildung einer Rettungsgasse.

AORTA Kreuzungssituation

Erreicht wird dies durch die Integration von Infrastruktur, Sensorik, Kommunikation, Fahrzeugtechnik und Darstellungsfunktionen, welche koordinierte Entscheidungsebenen verschiedener Abstraktionsgrade von der Einsatzleitstelle bis hin zum automatisierten Fahrmanöver auf klein- bzw. großflächigem Raum ermöglicht. Entwickelt wird eine dezentrale Datenplattform, auf welcher eine künstliche Intelligenz die Entscheidungen für kooperative Fahraufgaben trifft und den Fahrzeugen mitteilt. Dafür sind statische und dynamische Informationen von vernetzten Fahrzeugen, digitaler Straßeninfrastruktur und Sensoren entlang der Route von Einsatzfahrzeugen nötig. Die Lösung wird als kompatible Erweiterung zu existierenden und zukünftigen Automationslösungen der Fahrzeughersteller konzipiert und basiert auf aktuellen Standards, sodass keine Modifikation auf Fahrzeugseite notwendig ist, um beteiligte Fahrzeuge einzubinden.
Das SafeTRANS-Mitglied embeteco verantwortet im Projekt AORTA die Konzeption und Realisierung von HMI-Anwendungen (HMI = Human Machine Interface, Mensch-Maschine-Schnittstelle) und modernen Realisierungen von HMI-Schnittstellen. Um nicht-autonome Fahrzeuge, deren Anteil aktuell noch der größte unter den Verkehrsteilnehmern ist, ebenfalls in das AORTA-Szenario einzubinden, werden mobile Komponenten genutzt, die über entsprechende Mensch-Maschine-Schnittstellen die Fahrzeugführer mit wichtigen Informationen versorgen und Informationen des Fahrers in das Gesamtsystem zurückspiegeln.
Die Kommunikation muss dabei ablenkungsarm erfolgen. Im Projekt werden Interaktionsvarianten wie Gesten, Berührung und Sprache geprüft, um den entsprechenden Risikoaspekten und Rahmenbedingungen in ausreichendem Maße Rechnung zu tragen (z. B. ist das Halten eines Smartphones in der Hand laut StVO während der Führen eines PKW nicht nur verboten, sondern stellt auch eine weitere erhebliche Ablenkung und somit ein Risiko dar). Ziel des Teilvorhaben AORTA-HMI ist die Konzeption, Entwicklung und Evaluierung geeigneter HMI-Schnittstellen für die unterschiedlichen Anwendungsfälle (manuelles Fahren, autonomes Fahren, Fahren eines Einsatzfahrzeugs). Dazu werden spezifische Anforderungen erhoben und analysiert. Insbesondere muss untersucht werden, inwieweit neben unidirektionalen Anzeigen auch bidirektionale Interaktionskomponenten der HMI eine ablenkungsfreie bzw. mindestens ablenkungsarme Nutzung ermöglichen und in welchen Kontexten eine Überforderung der Fahrzeugführer zu erwarten ist. Es gilt zu eruieren, inwiefern visuelle Handlungsempfehlungen, auf den zur Verfügung stehenden Anzeigegeräten, ablenkungsfrei eingesetzt werden können. Das Projekt wird gefördert durch das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) mit rund 4,3 Mio. Euro auf Grundlage der Förderrichtlinie „Ein zukunftsfähiges, nachhaltiges Mobilitätssystem durch automatisiertes Fahren und Vernetzung“.

Projektpartner:
Technische Universität Kaiserslautern – Lehrstuhl Mechatronik in Maschinenbau und Fahrzeugtechnik (MEC)
3D Mapping Solutions GmbH, Holzkirchen
AKKA DSO GmbH, München
Altran Deutschland S.A.S. & Co KG, München
ASB Kaiserslautern
Bundesanstalt für Straßenwesen, Bergisch Gladbach
DC Vision Systems GmbH, Nürnberg
Dresden Elektronik Ingenieurtechnik GmbH, Dresden
embeteco GmbH & Co. KG, Oldenburg
Stadt Kaiserslautern
SysGen GmbH, Bremen

Gefördert durch:
Bundesministerium für Verkehr und digitale Infrastruktur
aufgrund eines Beschlusses des Deutschen Bundestages

Leuchtturmprojekt: IT-Campus in Oldenburg

Im Nordwesten von Deutschland wird die Kompetenz im Bereich IT-Grundlagen- und Anwendungsforschung weiter ausgebaut: Ein IT-Campus, den das Oldenburger Forschungsinstitut für Informatik OFFIS plant, wird mit 35 Mio. Euro vom Bund gefördert.
Der IT-Campus soll zum Innovationsquartier Oldenburg ausgebaut werden. Ziel ist es, ein Umfeld zu schaffen, in dem sich Unternehmen und Start-Ups ansiedeln sowie bestehende Unternehmen mit Innovationsabteilungen und Spin-Offs einbringen.
Prof. Sebastian Lehnhoff, Vorstandsvorsitzender des OFFIS betont: „Mit der Ansiedlung der Institute des DLR und des DFKI wurde der Wissenschaftsstandort Oldenburg in den letzten zwei Jahren mit Unterstützung des Landes weiter aufgewertet. Mit den zusätzlichen Bundesmitteln wird es uns nun möglich sein, den IT-Standort Oldenburg zu einem international sichtbaren Leuchtturm der Digitalisierung auszubauen.“


Prof. Dr. Sebastian Lehnhoff


Prof. Dr.-Ing. Wolfgang Nebel

Professor Wolfgang Nebel, OFFIS-Vorstandsmitglied und Initiator des IT-Campus ergänzt: „Mit der nun möglichen Erweiterung des IT-Campus zum Innovationsquartier bietet sich die einzigartige Chance das Konzept einer durchgängigen Innovationskette von der Forschung bis zur Umsetzung in Wirtschaft und Gesellschaft zu realisieren.“
Auf dem Campus werden unter anderem OFFIS sowie die Carl von Ossietzky Universität Oldenburg in enger Zusammenarbeit forschen, gemeinsam mit dem DFKI-Labor und dem neuen DLR-Institut Systems Engineering für zukünftige Mobilität. Forschungsschwerpunkte sind die Herausforderungen und Chancen für Digitalisierung und Gesellschaft in den Bereichen Produktion, Energiewirtschaft, Gesundheit und Pflege, Mobilität der Zukunft sowie Umwelt und Nachhaltigkeit.
www.offis.de

INGenX Technologies beruft Achim Rettberg in ingenieurswissenschaftlichen Beirat

Das Technologieberatungsunternehmen INGenX Technologies GmbH vertieft seinen ingenieurwissenschaftlichen Ansatz und beruft Prof. Dr. Achim Rettberg in den Beirat zur Unterstützung der Geschäftsführung. Jörg Krüger, Gründer und Geschäftsführer der INGenX Technologies GmbH, meint dazu: „Mit Herrn Prof. Dr. Achim Rettberg haben wir einen international anerkannten und sehr erfahrenen Experten auf dem Fachgebiete cyber-physikalische Systeme und Embedded Software gewinnen können. Ich freue mich sehr, einen so etablierten und kommunikativen Partner in unserem Beirat begrüßen zu können."
Mit seinem erworbenen Wissen in mehr als 30 Jahren in Wissenschaft und Praxis in der Forschung und Entwicklung von eingebetteten, sicherheitskritischen Systemen bringt Achim Rettberg vielfältige Erfahrungen zur Unterstützung von INGenX Technologies ein. Achim Rettberg hat u. a. als globaler Experte und Coach für modellbasierte Entwicklung die neuesten Entwurfs- und Entwicklungsmethoden beim Fahrzeugelektronikhersteller HELLA eingeführt und ist heute im Rahmen einer von Behr-Hella Thermocontrol GmbH initiierten Stiftungsprofessur Inhaber des Lehrstuhls für „Human-Machine-Interface Technologien Eingebetteter Systeme" an der Hochschule Hamm-Lippstadt. Seine Forschungs- und Tätigkeitsschwerpunkte zum zeitgemäßen, modellbasierten Systementwurf mit Schwerpunkt auf funktionaler Sicherheit sowie die damit verbundenen nationalen und internationalen Kontakte zu Experten auf diesem Gebiet werden INGenX Technologies und deren Kunden aus der Automobil- und Luftfahrzeugindustrie sowie der Medizintechnik unterstützen. Achim Rettberg ergänzt den Beirat neben Stefan Henke, dessen Fachwissen Internationales Management umfasst.

Beirat der INGenX Technologies GmbH (v.l.n.r.): Jörg Krüger, Geschäftsführer, Stefan Henke und Prof. Dr. Achim Rettberg, Beiräte

INGenX Technologies deckt ein umfangreiches Vertikalportfolio ab: von der technologisch-strategischen Beratung des Managements bis hin zur realen Implementierungsunterstützung, um zu einer sicheren Produktentwicklung beizutragen. Das tiefe Verständnis eingebetteter Systeme und deren Funktions- und Nutzungsumgebungen wurde bereits vor mehr als 15 Jahren durch erste modellbasierte Entwicklungsansätze während der AIRBUS A380 Entwicklung aufgebaut, die damals ihrer Zeit weit voraus waren.
https://ingenx.tech/

Nothalt ade – Intelligente Infrastruktur leitet automatisierte Fahrzeuge durch kritische Situationen

Wenn hochautomatisierte und vernetzte Autos mit einer Situation nicht umgehen können, geben sie die Kontrolle wieder an den Fahrenden zurück. Reagiert der Insasse nicht, hält es sicherheitshalber an. Das kann zum Beispiel in komplizierten Baustellen vorkommen, bei denen die Spurmarkierungen fehlen oder bei Nebel. Halten automatisierte Fahrzeuge mitten im Verkehr plötzlich an, sind Staus oder kritische Situationen programmiert. Im EU-Projekt TransAID hat das Deutsche Zentrum für Luft- und Raumfahrt (DLR) gemeinsam mit internationalen Partnern aus Industrie und Forschung solche Situationen genau unter die Lupe genommen und Lösungsansätze entwickelt. Im Fokus stehen vor allem Kameras und Kommunikationstechnik an Straßenmasten als unterstützende Infrastruktur. Diese haben oft einen besseren Überblick und versorgen automatisierte Fahrzeuge mit zusätzlichen Informationen. So können diese Autos schwierige Situationen besser meistern.
„Damit automatisiertes und vernetztes Fahren ein Erfolg wird, benötigen wir nicht nur intelligente Fahrzeuge, sondern auch eine perpektivenerweiternde Infrastruktur, die mit den Fahrzeugen kommuniziert. Sie ist ein entscheidender Schlüssel, um viele zukunftsweisende Mobilitätskonzepte überhaupt erst möglich und effizient zu machen", erklärt Prof. Katharina Seifert, Direktorin des DLR-Instituts für Verkehrssystemtechnik in Braunschweig.
Ob an Baustellen, an komplexen Kreuzungen oder bei plötzlich auftretenden Behinderungen wie Unfällen – der Verbund von Kameras und Sensoren kann automatisierten Fahrzeugen Lösungen vorschlagen, wie sie mit schwierigen Situationen umgehen. So können sie beispielsweise den Weg durch Baustellen berechnen oder aktuelles Kartenmaterial bereitstellen, das auch kurzfristige Änderungen in der Verkehrsführung beinhaltet. Falls das dem automatisierten Fahrzeug nicht hilft, kann die intelligente Infrastruktur auch Haltepunkte vorgeben, durch die der restliche Verkehr so wenig wie möglich behindert wird. „Im Projekt haben wir gezeigt, dass die Unterstützung durch Infrastruktur die negativen Effekte auf den nachfolgenden Verkehr drastisch reduziert. Das gilt insbesondere in schwierigen Situationen, die sonst einen Nothalt verursachen würden", fasst Julian Schindler, Koordinator des Projekts am DLR-Institut für Verkehrssystemtechnik, zusammen.
Im Fokus der Untersuchungen standen zwei Situationen: die Vermeidung der Übergabe der Steuerung vom Fahrzeug an den Insassen und der Nothalt. Diesen führt das Auto durch, wenn der Fahrende nicht oder nicht schnell genug reagiert.

Zwei Versuchsfahrzeuge des DLR und ein mobiler Sensor aus dem Testfeld Niedersachsen beim Einsatz auf dem Gelände des ADAC Fahrsicherheitszentrums in Hannover Laatzen verwendet wurden.

Im ersten Schritt modellierten die Wissenschaftlerinnen und Wissenschaftler diese und weitere Situationen am Computer. Virtuell ließen sie dann Fahrzeuge mit unterschiedlichen Fähigkeiten diese Situationen durchfahren und werteten deren Verhalten aus.
Im zweiten Schritt erprobte das Projektteam von TransAID die vielversprechendsten Lösungsansätze zunächst in der Simulation und dann auf Testgeländen. Die Ergebnisse aus dem Projekt fließen ein in die Standardisierung im Bereich der Kommunikation von automatisierten und vernetzten Fahrzeugen mit der Infrastruktur. Zudem erarbeitete TransAID Richtlinien für Interessengruppen, wie Städte, Zulieferer, Behörden sowie Hersteller von Fahrzeugen und Infrastruktur.
www.dlr.de

Schweizer Tochterunternehmen gliedert sich auch namentlich in die ICS-Familie ein

Die DTec Solutions AG heißt jetzt ICS Schweiz AG und agiert mit erweitertem Portfolio vom neuen Firmenstandort bei Zürich aus. Zum 1. März 2020 haben sich Unternehmensname und Unternehmensadresse geändert: Die jetzige ICS Schweiz AG ist nach Affoltern am Albis im Kanton Zürich umgezogen. In den vergangenen vier Jahren lag der Schwerpunkt des schweizerischen Tochterunternehmens auf Software- und Systementwicklungen für die Schienenfahrzeugtechnik. In Zukunft wird die ICS Schweiz AG branchenunabhängig Kunden bedienen können, die auf sichere Prozesse in komplexen Umgebungen Wert legen. Neben dem Geschäftsfeld Mobility fokussiert sich die Expertise der ICS auf die Bereiche Industrial Engineering und Information Security. Olaf Hofer, Managing Director der ICS Schweiz AG, betont: „Unsere enormes Prozess- und Normwissen aus über 50 Jahren Erfahrung macht uns zum idealen Partner für funktionale Sicherheit und IT-Sicherheit in jeglicher Form von kritischen Systemen".
„THINK SAFE THINK ICS" umfasst alle Leistungen, die die Verfügbarkeit, die Zuverlässigkeit, den Schutz sowie die Wartbarkeit von Software und Systemen gewährleisten. Die ICS Schweiz AG verwirklicht diesen ganzheitlichen Ansatz mit einem Team aus erfahrenen System-, Software- und Testingenieuren.
www.think-safe-think-ics.de

Managing Director Olaf Hofer (stehend) mit Senior Systems Engineer Dr. Marcel Stillhart (sitzend) im Büro der ICS Schweiz AG noch vor der Corona-Pandemie.
.

MES stellt Erweiterung für MATLAB Simulink®-Editor vor

MES stellt den MES Model & Refactor® (MoRe) vor, eine Erweiterung für den MATLAB Simulink®-Editor. Sie vereinfacht und beschleunigt die Modellerstellung und das Refactoring von Modellen. Mit dem MATLAB Simulink® Editor-Plug-in werden tägliche Modellierungsaufgaben schneller und weniger fehleranfällig, insbesondere wenn es um das Refactoring von Modellen als Best Practice aus der agilen Entwicklung geht.
Als Hilfswerkzeug für die Modellierung automatisiert MoRe häufig auszuführende Modellierungsschritte. So sind automatisierte Modellierungsaktionen für folgende Bereiche verfügbar: Signal-Routing über Subsystemhierarchien, Verschieben von Blöcken mit Signalverbindungen zwischen Subsystemen, Refactoring des Modells durch Änderung der Subsystem-Partitionierung, Auto-Layout-Subsysteme wie Auto-Positionierungsblöcke oder Signal-Route-Optimierung (Linien begradigen), beschleunigte Bearbeitung von Subsystem-Schnittstellen, vereinfachte Arbeit mit Bussignalen und schnelle Datenflussanalyse.
Die Erweiterungen des Editors basieren technisch auf sl_customization.m. Die Erweiterungen von MoRe gehen jedoch darüber hinaus und bieten beispielsweise auch ein mehrstufiges Undo und Redo von Modellierungsaktionen.
Wichtige Funktionen vo MoRe sind:

- Hierarchieübergreifende Signale erstellen oder entfernen
- Subsystem-Zerlegung verbessern
- Subsystem-Schnittstellen überarbeiten
- Busse erstellen und zerlegen
- Datenfluss analysieren

www.model-engineers.com/more

MES
MODEL ENGINEERING SOLUTIONS

Step-UP!CPS: Workshops mit Industrievertretern

Die aktuellen Ergebnisse zu Konzepten und Methoden zur kontinuierlichen Entwicklung und Validierung von updatefähigen CPS des Projekts Step-Up!CPS wurden dem Industrial Advisory Board in zwei Workshops präsentiert, die sich jeweils zwei Use-Cases widmeten (mehr zum Projekt siehe SafeTRANS News 1/2020). Der erste Workshop am 12.02.2021 konzentrierte sich auf den Anwendungsbereich Automotive mit den Use-Cases

- UC1: UPDATER – UPDateable Automotive Test dEmonstratoR und
- UC2: Emergency Brake Warning Assistant on the DLR research vehicle FASCar.

Die Themen Contract-based Design, Varianten-Management, delta-based Virtual Integration Testing, Deployment und (on-line) Monitoring wurden vorgestellt, demonstriert und diskutiert. Der darauf aufbauende zweite Workshop am 01.06.2021 präsentierte die Zwischenergebnisse der Domänen Maritime und Industrie 4.0:

- UC3: hochautomatisiertes Assistenzsystem MTCAS (Maritime Traffic Alert and Collision Avoidance System)
- UC4: „Plug and Produce“ with IEC 61499 for distributed industrial control

Einige Teilnehmer des virtuellen Industrial Advisory Board Workshops des Projekts Step-Up!CPS.

Die Vertreter der im Industrial Advisory Board (IAB) vertretenen Firmen IAV, DNV-GL, AVL LIST, Vector Informatik und BTC Embedded Systems konnten sich von der Qualität der erzielten (Zwischen-)Ergebnisse überzeugen und die Anwendbarkeit und „Passgenauigkeit“ zu den jeweils eigenen Anwendungsdomänen und -prozessen abschätzen.
Das IAB bestehend aus Anwendern und Technologie-Providern als zukünftige Nutzer der Projektergebnisse ist eng ins Projekt eingebunden und agiert u. a. als Ideengeber und Konzeptprüfer. Die Ergebnisverwertung und der Transfer in die Praxis erfolgt in einem Open-Innovation Prozess über das Kompetenznetzwerk SafeTRANS und die Netzwerke der Partner. Das Projekt Step-UP!CPS wird vom Bundesministerium für Bildung und Forschung gefördert.
https://stepup-cps.de/

Step-UP!CPS

Wie künstliche Intelligenz digitale Realitäten erzeugt, um hochautomatisiertes Fahren sicher zu machen.

Philipp Slusallek, Leiter des Forschungsbereichs Agenten und Simulierte Realität des DFKI, über digitale Realitäten, die mithilfe künstlicher Intelligenz erzeugt werden.

Eine der größten ungelösten Herausforderungen bei der Erforschung von künstlicher Intelligenz und der damit limitierende Faktor ihrer intensiven Nutzung in sicherheitskritischen Anwendungen wie dem hochautomatisierten Fahren ist die Absicherung der KI-basierten Funktionen. Der verantwortungsvolle Umgang mit „künstlicher Intelligenz“ im Kontext von sicherheitsrelevanten Funktionen stellt eine besondere Herausforderung dar. Eine stringente Argumentationskette aufzubauen, die aus Expertensicht eine Absicherung von KI-Modulen hinreichend begründet, ist ebenso erforderlich wie die Entwicklung von Methoden und Maßnahmen, die dazu geeignet sind, die funktionale Sicherheit über direkte und indirekte Messmethoden zu bestimmen und zu bewerten.

Zur Definition der unterschiedlichen Stufen der Automatisierung verwenden wir die Klassifikation nach dem Standard SAE J3016 Standard[1] (siehe Abb. 1). Wir ergänzen diese Begriffe durch “KI-Anteile der Fahrautomatisierungsfunktion”. Damit bezeichnen wir Komponenten innerhalb derselben, für die wir, je nach Funktion und Ausprägung, unterschiedliche Eigenschaften beschreiben, die unserer Ansicht nach für den sicheren Betrieb der gesamten Fahrautomatisierungsfunktion notwendig sind. Die im SAE Standard erwähnten Minimalrisikozustände sind wesentliche Elemente desselben. Für jeden Zeitpunkt der automatisierten (Fahr-)Situation muss die auszuführende Aktion klar bestimmt sein. Diese Aktion wird dann als Minimalrisikomanöver (minimal risk maneuver, MRM) bezeichnet. Es gibt derzeit noch keinen MRM-Standard für hochautomatisierte Fahrzeuge.

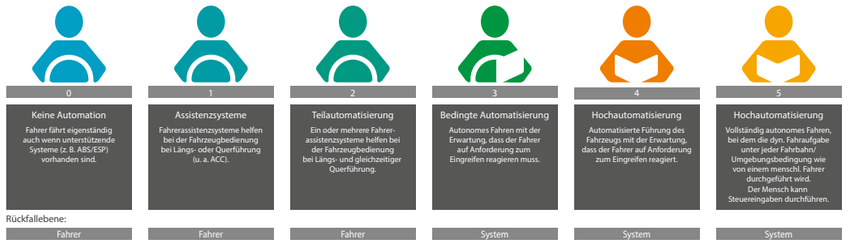


Abb. 1: SAE Levels: Klassifizierung für Kraftfahrzeuge mit Systemen zum autonomen Fahren

Die Automobilbranche ist überzeugt davon, dass höhere Automatisierungsstufen nur dann erreicht werden können, wenn künstliche Intelligenz eingesetzt wird, eine Meinung, die von uns geteilt wird. Allerdings bezeichnet man mit dem Begriff „KI“ in diesem Zusammenhang vor allen Dingen das so genannte Tiefe Lernen (engl. Deep Learning), einen Teilbereich des Maschinellen Lernens, das vor einem Jahrzehnt seinen Siegeszug in faktisch allen KI-Herausforderungen begonnen hat, in denen lernende Systeme eine Rolle spielten. Seit ein bis zwei Jahren erleben wir eine Art Renaissance einer umfassenderen Betrachtung der künstlichen Intelligenz - für Autonome Systeme und andere “kritische” Anwendungsbereiche. Dazu bietet die KI einen umfangreichen Werkzeugkasten, der weit mehr Werkzeuge enthält als maschinelles Lernen. Betrachten wir beispielhaft das Problem der Beachtung von Verkehrsregeln. Die Herausforderung besteht nicht nur darin, die Regeln selbst zu formulieren oder zu beachten. In diesem Zusammenhang haben KI-Regelsysteme bereits vor Jahrzehnten ähnlich komplexe Aufgaben gemeistert, etwa in der Steuerung von Kraftwerken und großen Industrieanlagen. Was die Verkehrsregeln schwierig macht sind Ausnahmen (in welchen Fällen darf über eine durchgezogene Linie gefahren werden), welche häufig kultur- oder sogar ortsabhängig verschieden sind. Wir halten es für wahrscheinlich, dass hierfür lernende Systeme zum Einsatz kommen werden, so dass insgesamt lernende und nicht-lernende KI-Verfahren kombiniert werden, um die Verkehrsregeln meistern zu können. Die eigentlichen Regeln werden dabei symbolisch vorgegeben (Regelsystem, Ontology), während die genaue Auslegung und Ausnahmen (was beides häufig lokal sehr verschieden ist), aus Daten gelernt werden. Allgemein geht der Trend in Richtung solcher hybriden KI-Systeme, die weder reine subsymbolische lernende Systeme, noch reine symbolische Reasoner sind. Davon verspricht man sich leistungsfähige Klassifizierer, Regressionsalgorithmen oder Prädiktoren, die eine Ende-zu-Ende Optimierung von Daten zu den jeweiligen Antworten durchführen, so wie das heute bei Deep Learning gezeigt wird. Gleichzeitig soll jedoch eine gewisses „grounding“ durch Regelsysteme erfolgen, die in der Lage sind, explizit vorgegebenes Wissen bei der Entscheidung zu berücksichtigen.

KI Module als Bestandteile von (Fahr-)Automatisierungsfunktionen werden häufig als „Black Boxes“ betrachtet. Damit ist gemeint, dass man zwar beobachten kann, welche Ausgaben sie bei welchen Eingabesignalen erzeugen, aber nicht hineinsehen kann, um nachvollziehen zu können, wie das Ergebnis zustande gekommen ist. Dies hat mehrere Gründe: zunächst ist es aufgrund der Zulieferbeziehungen im Automobilbau sehr wahrscheinlich, dass die betreffende Funktion zugeliefert wird, also von einem anderen Unternehmen als dem Automobilhersteller entwickelt wurde. Dieser wird zum Schutz seines geistigen Eigentums (Intellectual Property, IP) die innere Funktion des Moduls nicht offenlegen wollen. Des Weiteren fehlt es dem Automobilbauer möglicherweise auch an der Kompetenz, das komplexe Modul zu analysieren, das nicht im eigenen Haus entwickelt wurde. Die Hersteller sind noch immer dabei, ihre KI-Schlagkraft aufzubauen und haben dabei längst nicht das Niveau erreicht, welches die großen Internetkonzerne aufweisen. Schließlich weisen die heutigen KI-Ansätze gerade im Bereich der Erklärbarkeit Schwächen auf.

Demgegenüber könnten wir uns dasselbe KI-Modul auch als „White Box“ vorstellen. Hier hätte der Automobilhersteller sowohl die Rechte als auch die Kompetenzen, die Entscheidungen des Moduls vollständig zu durchdringen und das Modul selbst würde die nötigen Informationen dazu vollständig bereitstellen können. Allerdings kann eine „White Box“ KI auf absehbare Zeit als eine wissenschaftliche Utopie betrachtet werden. Woran vielmehr geforscht und entwickelt wird, ist die „Grey Box“ KI, in der zwar mit einer wie auch immer gearteten Einschränkung der Einsicht in die Entscheidungsprozesse zu rechnen ist, jedoch genügend Informationen verfügbar sind, um eine Plausibilisierung der Entscheidungen durchführen zu können.

Für KI-Probleme, die entsprechende Aufmerksamkeit in der wissenschaftlichen Gemeinde genießen, gibt es häufig auch gängige Metriken, also Verfahren und Maße, welche die Leistungsfähigkeit eines Ansatzes zeigen sollen. Diese Metriken sind häufig eng an das jeweilige Problem gekoppelt und berücksichtigen selten die Gegebenheiten in der späteren Anwendung. So wird beispielsweise die Leistung eines Bildsegmentierers in der Regel mit der „Intersection over Union“ gemessen, also einem Verhältnis zwischen der Schnittmenge der Pixel von Ergebnis und Wahrheit und ihrer Vereinigungsmenge. Dieses Maß lässt sehr genaue Unterschiede in der Leistung zweier Segmentierer(-varianten) zu, hat aber sehr wenig damit zu tun, ob die gesamte Umgebungswahrnehmung hinreichend gut funktioniert oder nicht. Mit anderen Worten: ob einige Pixel am Rand eines Objektes der Kategorie „Vegetation“ fälschlicherweise mit „Gebäude“ verwechselt wurden, ist für die sichere Erkennung der Fußgänger auf der Fahrbahn von nebensächlicher Bedeutung.

Im Automobilbau wendet man in der Regel das V-Modell an. Das V-Modell ist ein Vorgehensmodell, welches ursprünglich für die Softwareentwicklung konzipiert wurde und den Softwareentwicklungsprozess in Phasen organisiert. Zusätzlich zu diesen Entwicklungsphasen definiert das V-Modell auch das Vorgehen zur Validierung, indem den einzelnen Entwicklungsphasen Validierungsphasen gegenübergestellt werden.

Für die KI-Anteile in den jeweiligen Fahrautomatisierungsfunktionen haben sich noch keine durchgängigen, dem V-Modell entsprechende Verfahren durchgesetzt, da zunächst eine „Übersetzung“ der komponentenspezifischen (engeren, aber feineren) auf systemspezifische (allgemeinere, aber anwendungsrelevante) Maße erfolgen muss. Der ISO-26262-Standard ist die Grundlage für ein sicheres System, sichere Hardware und sichere Software, die im Fehlerfall einen unabhängigen und sicheren Betrieb ermöglichen. Dennoch ist man in der Branche der einhelligen Meinung, dass die ISO 26262 zur Absicherung von (Fahr-)Automatisierungsfunktionen nicht ausreicht. Diese fehlende Funktionalität behandelt nun der neuere, auf den ISO 26262:2018 aufbauende Standard, ISO/PAS 21448, der allgemein als SOTIF (Safety of the Intended Functionality) bezeichnet wird.

Zu untersuchende Problemstellungen

1. **Überwachung, Bewertung und Zulassung von künstlicher Intelligenz**

Die Verifikation und Validierung von Fahrautomatisierungsfunktionen beinhaltet von der Simulation bis zum Gesamtfahrzeug eine große Anzahl von Tests. Dazu zählen Faktoren, die die gesamte 4D-Umgebung (Kartesischer Raum inklusive der Dimension der Zeit) umfassen, einschließlich Wetter, Straßenzustand, umgebende Landschaft, Objekttextur und mögliche missbräuchliche Anwendung durch den Fahrer. SOTIF bietet bereits Methoden und Richtlinien zur Einbeziehung von Umweltszenarien für die Vorabanalyse des Konzepts und die endgültige Validierung. Das Ziel des Standards besteht darin, eine Richtlinie für die Dokumentation der verschiedenen Szenarien, der Sicherheitsanalyse dieser Szenarien, der Überprüfung der Sicherheitssituationen und der auslösenden Ereignisse sowie der Validierung des Fahrzeugs für die Umwelt mit angewandten sicheren Systemen zu schaffen. Bei der Erweiterung des SOTIF-Standards in Richtung SAE Stufen 3-5 sind es vor allem die komplexer werdenden ODDs (Level 3,4) bzw. die Forderung der ODD-freien Anwendbarkeit (Level 5), die Validierungsspezifikationen erschweren. Die Anzahl der potenziellen kritischen Szenarien, die bei einer hinreichend breiten ODD und einem SAE Level > 2 in Betracht gezogen werden muss, ist äußerst groß. Die Frage, die man sich bei der Entwicklung entsprechender funktionaler Sicherheitsstandards stellen muss, ist die, wie man in dieser großen Menge diejenigen Fälle identifizieren kann, die eine maximale Aussagekraft bezüglich der Gesamtleistungsfähigkeit der (Fahr-)Automatisierungsfunktion enthalten. Dies sind häufig die

[1] Siehe: https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic (Zugriffsdatum: 07.04.2021)

sogenannten „Randfälle“ (Corner Cases). Die künstliche Intelligenz bietet Methoden an, um diese Aufgabe zu erleichtern und zu systematisieren.

Info:

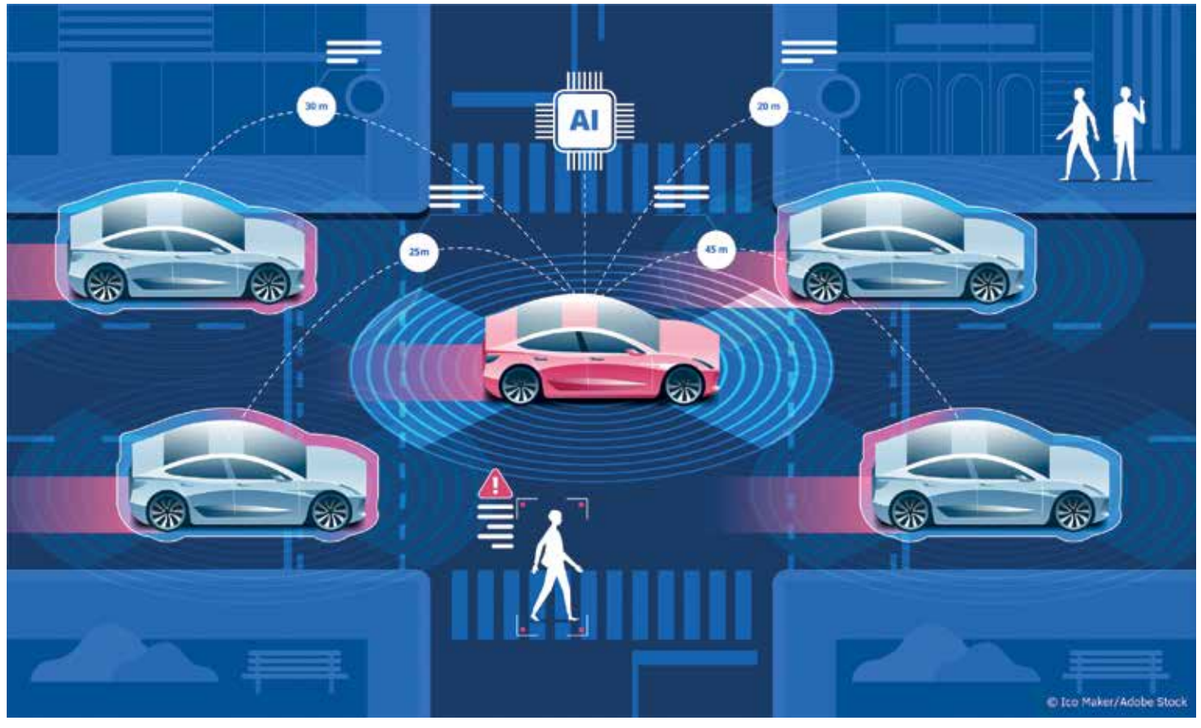
ODD - Operational Domain Definition

Die Operational Domain Definition beschreibt Betriebsbedingungen, unter denen ein gegebenes System ausgelegt ist zu funktionieren, einschließlich, aber nicht beschränkt auf Umwelt, geografische Lage und Tageszeit, das Vorhandensein oder Fehlen bestimmter Verkehrs- oder Straßeneigenschaften. Zum Beispiel kann eine ODD so definiert sein, dass ein Fahrzeug nur auf vollständig zugangskontrollierten Autobahnen bei geringem Tempo unter Schönwetterbedingungen hochautomatisiert betrieben werden kann. Die SAE Stufen 1 bis 4 berücksichtigen ausdrücklich die ODD-Beschränkungen. Im Gegensatz dazu unterliegt Level 5 keinen ODD-Beschränkungen.
Dementsprechend muss zum genauen Beschreiben eines Merkmals (mit Ausnahme von Stufe 5) sowohl die Stufe der Fahrautomatisierung als auch die ODD identifiziert werden.

Bisher ist gängige Validierungspraxis, so viele Straßenkilometer wie möglich zu sammeln, um die Verlässlichkeit einer Fahrautomatisierungsfunktion (und damit auch deren KI-Anteile) nachzuweisen. Das Sammeln von Millionen von Straßenkilometern im Realtestbetrieb führt allerdings nicht zu einer ausreichenden Abdeckung kritischer Szenarien. Darüber hinaus stellt sich das Problem der Annotation. Um eine möglichst breite Verwendbarkeit der Realdaten für Training und Validierung gewährleisten zu können, müssen Kameradaten Frame für Frame pixelgenau annotiert werden, was trotz Fortschritten im Bereich der Annotationstools und Angeboten aus Ländern mit vergleichsweise geringen Lohnkosten erhebliche zeitliche und monetäre Ressourcen erfordert. Für multisensorielle Daten, die auch Lidar und Radarinformationen enthalten, ist das Problem noch gravierender.
Demgegenüber stehen Verfahren der synthetischen Datenerzeugung durch Simulation (digitale Realität), die eine Reihe von Vorteilen bieten: die Nutzungsrechte sind nicht grundsätzlich eingeschränkt und vor allem können Parameter wie z. B. Fahrzeuggeschwindigkeiten oder Komplexität der Szene beliebig variiert werden. Ferner können riskante Aktionen beliebig oft ohne Einschränkung nachgestellt werden. Darüber hinaus können die Verfahren der digitalen Realität auch sehr einfach die für Training und Validierung benötigten ”Ground-truth Daten” liefern, da diese direkt aus dem Modell stammen. Insbesondere die Möglichkeit, in der Simulation Fahrsituationen beliebig variieren zu können, macht die digitale Realität sehr geeignet, um systematische Trainings- und Validierungsdaten zu erzeugen. Nur mit Daten einer relevanten Abdeckung kann man die Absicherung der KI-Module gewährleisten.
Die digitale Realität ist mehr als eine Simulation, sondern vielmehr eine KI-gestützte Erzeugung von komplexen Inhalten für eine Simulation. Diese Inhalte können beispielsweise menschliches Verhalten sein, das auf verschiedenen Ebenen modelliert und gelernt wird. In Bezug auf Straßenverkehrsszenarien besteht die unterste Ebene aus Bewegungsabläufen. Eine Ebene darüber ist die Planung und Ausführung von Trajektorien angesiedelt und wiederum eine Ebene darüber werden menschliche Eigenschaften wie z.B. Interessen, Ziele, Einstellungen zu bestimmten relevanten Aspekten der Welt modelliert. Auf allen genannten Ebenen kommt künstliche Intelligenz zum Einsatz, was die digitale Realität von der Simulation unterscheidet. Letztere kann in diesem Sinne als das Resultat von ersterer beschrieben werden. Digitale Realität kann auch zur Erzeugung von statischen Inhalten einer Simulation herangezogen werden. Wir arbeiten beispielsweise an einem Verfahren zur Erzeugung von Gebäudemerkmalen aus Punktewolken, um realitätsgetreue Gebäude darstellen zu können. Dies ist ein häufig unterschätzter Faktor, denn die Architektur eines Gebäudes kann relevant für das Sichtfeld und die Zugänglichkeit zur Fahrbahn sein. So ist es beispielsweise wahrscheinlicher, dass ein Fußgänger aus einer Kolonnade heraus auf die Straße tritt als durch ein Mauerwerk hindurch.

Beispiel:

Beachten wir zur Verdeutlichung folgendes Beispiel: Leonard steht am Straßenrand einer dreispurigen innerstädtischen Straße. Leonard hat gelernt, eine entsprechende Lücke zwischen den Fahrzeugen abzupassen, um sicher die Straße überqueren zu können. Leonard wartet, doch der Verkehr ist zu stark. Zu einem gewissen Zeitpunkt entscheidet sich Leonard, eine andere Route einzuschlagen. Von Natur aus ist Leonhard auf Sicherheit bedacht und er interessiert sich für Yoga und Naturkost. Er geht den Bürgersteig entlang zu einem Fußgängerüberweg und überquert die Straße dort. Er hat diese Strecke ausgewählt, weil er weiß, dass sich auf der gegenüberliegenden Seite ein Zeitschriftenladen befindet und er nicht in Eile ist. Er bleibt dort stehen, um sich Yoga-Magazine in der Auslage anzusehen. Anschließend setzt er seinen Weg über den Bürgersteig fort bis zu seinem Ziel, sein am Straßenrand geparktes Fahrzeug.



Das Beispiel beschreibt einen Demonstrator des Forschungsprojektes REACT und Leonard ist kein Mensch, sondern ein KI-Agent. Alle Facetten des menschlichen Verhaltens vom Lernen des Überquerens der Straße bis hin zum interessensbasierten Neu-Routen der Strecke aufgrund der Bedingungen wurden in dem KI-Agenten abgebildet. Seine Welt ist eine Simulation, die Simulation, in der auch hochautomatisierte Fahrzeuge lernen. Die Ausführung der Trajektorie, die Leonard einschlägt orientiert sich an dem Verhalten von Menschen. Die Daten, die hierfür verwendet wurden, berücksichtigen auch Eigenschaften bzw. Aspekte der Aufmerksamkeit, die über Eye-Tracker aufgezeichnet worden sind. Mithilfe von Imitation Learning wird das menschliche Verhalten verallgemeinert und Eigenschaften wie sicheres Verhalten oder unsicheres Verhalten kann nun in einer großen Zahl von Variationen hervorgerufen werden. Auch das Überqueren der Straße ist ein Modul, das aus Daten gelernt wurde. Hier kommt in diesem speziellen Fall ein recht einfaches effizientes Q-Learning zum Einsatz. Leonards Eigenschaften und sein prinzipielles Verhalten wird in der Agenten Modellierungen Umgebung AJAN festgehalten. Die genaue Ausführung seiner Schrittfolge wurde ebenfalls gelernt. Sodass auch Leonards ganz persönlicher Laufstil mitberücksichtigt werden kann. All diese Komponenten zusammengenommen ermöglicht es der digitalen Realität, eine sehr große Vielfalt von Simulationen zu erzeugen, ohne dass diese von menschlichen Designern ausgestaltet werden müssen.
Auch die Sensor-Modellierung ist ein Aspekt der digitalen Realität. Die Radar-Simulation spielt dabei eine sehr wichtige Rolle. Zum einen, weil Radar für hoch automatisiertes Fahren sehr wichtig ist, zum anderen, weil es wenige Werkzeuge gibt, die Radar akkurat simulieren, da Radar eine sehr viel längere Welle als Licht erzeugt und dementsprechenden Beugungseffekten unterliegt. Ein vielversprechender Weg ist, Methoden aus der Computergrafik heranzuziehen, die ursprünglich für die Simulation von Lichttransport entwickelt wurden.
Aktuell gibt es in diesem Bereich bereits sehr gute erste Ergebnisse, sodass Radar neben dem menschlichen Verhalten ein zweiter Schwerpunkt bei unserer Forschung darstellt.

2. Erarbeitung der Verifikations- und Zertifizierungskriterien für die KI-Anteile von Automatisierungsfunktionen

Der „klassische Zertifizierungsansatz“ (z. B. für Reifen) definiert typischerweise eine begrenzte Anzahl von Leistungskriterien und physischen Zertifizierungsprüfungen, um das erforderliche Sicherheitsniveau als Voraussetzung für den Markteintritt festzulegen. Solche Tests werden auf Teststrecken oder auf einem Prüfstand durchgeführt, die Anforderungen wurden über

Jahre hinweg verfeinert. Der Ansatz ist gut geeignet für Systeme mit begrenzter Komplexität, begrenzten Interaktionen mit anderen Systemen und klar definierten Systemgrenzen (typisch für mechanische Systeme/Komponenten).
Die Prüfung von (Fahr-)Automatisierungsfunktionen erfordert neue Elemente: Die Systemkomplexität und damit die Anzahl der softwarebasierten Funktionen wird hier weiter zunehmen. Bezüglich der komplexen elektronischen Steuerungssysteme nehmen die potenziell betroffenen Sicherheitsbereiche und Szenarienabweichungen weiter zu und können mit einer begrenzten Anzahl von Tests, die auf einer Teststrecke oder einem Prüfstand durchgeführt werden, nicht vollständig bewertet werden. Der bestehende Auditansatz für elektronische Steuerungssysteme sowohl in Sicherheitssystemen (z. B. ABS, ESP) als auch in Fahrerassistenzsystemen (SAE 1, SAE 2) muss weiter ausgebaut und aufgerüstet werden, um SAE 3 - 5 L3- L5-Systeme zu bewältigen.
Die Prüfung bestehender konventioneller Sicherheitsvorschriften sollte mit dem „klassischen Ansatz“ auch für Komplettsysteme (z. B. Fahrzeuge), die mit Automatisierungsfunktionen ausgestattet sind, fortgesetzt werden. Dies ist ein wesentlicher Bestandteil des Drei-Säulen-Ansatzes (siehe unten). Ergänzungen sind erforderlich, um die softwarebezogenen Aspekte angemessen abzudecken - sie werden den klassischen Zertifizierungsansatz ergänzen und nicht ersetzen.

Die drei Säulen sind: Realfahrten, Physische Tests, Audit und Assessment (z. B. mithilfe der digitalen Realität). Realfahrten ergeben

- einen Gesamteindruck des Systemverhaltens auf öffentlichen Straßen
- eine Bewertung der Fähigkeit des Systems mit realen Verkehrssituationen umzugehen. Dabei kommen standardisierte Checkliste („Führerscheinprüfung“) für Fahrautomatisierungsfunktionen zum Einsatz.

Physische Zertifizierungstests ergeben einen Abgleich der Audit-/Bewertungsergebnisse mit dem realen Verhalten in der Praxis. Es erfolgt eine Bewertung des Systemverhaltens in einer Reihe von kritischen Fällen, die entweder nicht auf öffentlichen Straßen prüfbar sind oder von denen nicht garantiert werden kann, dass sie während des realen Betriebs auftreten (weil sie ggf. zu selten sind). Zudem ist die Reproduzierbarkeit der Situationen gegeben.
Schließlich wird ein Audit des Entwicklungsprozesses (Methoden, Standards) durchgeführt, das Sicherheitskonzept (funktionale Sicherheit, Sicherheit der Nutzung) und die Maßnahmen zur Überprüfung der Integration von allgemeinen Sicherheitsanforderungen und Verkehrsregeln bewertet. In diesem Schritt kommt die digitale Realität zum Einsatz (hohe Laufleistung, Fähigkeit zur Bewältigung kritischer Situationen). Des Weiteren erfolgt eine Bewertung von Entwicklungsdaten/Feldtests und OEM-Selbsterklärungen.
Um den beschriebenen Drei-Säulen-Prozess durchführen zu können, müssen die KI-Anteile von Fahrautomatisierungsfunktionen die folgenden prinzipiellen Kriterien erfüllen: Es muss verlangt werden, dass die KI-Anteile der Fahrautomatisierungsfunktionen eine hinreichende Modularität aufweisen, da ansonsten eine Entwicklung eine Prüfkatalogs nicht möglich wäre. Das gilt vor allem für die Zertifizierungstests und das Audit. Des Weiteren ist die Erklärbarkeit der KI ein zentrales Kriterium, das auch in der rechtlichen Betrachtung an vielen Stellen eine Rolle spielt. Eine „Black Box“ lässt sich nicht im Sinne des oben skizzierten Verfahrens prüfen. Neben der Erklärbarkeit ist in erster Linie die korrekte Behandlung von Unsicherheit ein herausragendes Kriterium - eine Forderung, die an KI-Bestandteile von Fahrautomatisierungsfunktionen gestellt werden sollte. Diese wird dringend benötigt, da es unter anderem Grundlage für das Auslösen eines Minimalrisikomanövers ist: nur wenn das System erkennen kann, dass es die aktuelle Situation nicht beherrschen kann, ist eine solche Maßnahme denkbar.

Prof. Dr.-Ing. Philipp Slusallek,
Dr.-Ing. Christian Müller |
Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI)

„In modernen Autos wird die Software Teil des Primärprozesses des Autofahrens und das digitale Ökosystem zur Basis für die Funktion und Fähigkeiten.“

Dirk Giesen, Vice President of Sales EMEA bei Parasoft, über die Schlüsselrolle der Software im Automotive-Markt der Zukunft.

Die Transformation der individuellen Mobilität hin zu alternativen Antrieben macht nur Sinn mit einer digitalen Infrastruktur und Apps, damit Informationen über Software zugänglich und abrufbar sind. Zugleich treiben Maschinelles Lernen (ML) und Künstliche Intelligenz (KI) das autonome Fahren voran. Welchen Stellenwert die Software in der neuen Automobiläa einnimmt, erläutert Dirk Giesen, Vice President Sales EMEA bei Parasoft.

Wohin geht die Reise der Automobilindustrie und insbesondere bei autonomen Fahrzeugen?
Dirk Giesen: Durch die andauernde Klimadiskussion findet gerade eine massive Transformation der individuellen Mobilität hin zu alternativen Antrieben statt. Die Automobilindustrie musste sehr kurzfristig in das Thema Elektromobilität einsteigen. Allerdings lassen sich Elektrofahrzeuge nur sinnvoll betreiben, wenn sie vernetzt und in ein System eingebunden sind, sodass bestimmte Informationen (z. B. die Position des Fahrzeugs oder die Lage von Ladestationen) per App erreichbar sind. Dafür braucht es eine digitale Infrastruktur.
In bestimmten Situationen werden Autos mit ML und KI bald autonom fahren können, was Auswirkungen auf unser Gesellschaftssystem haben wird. Schon heute zeichnet sich die Verlagerung vom Besitz eines Fahrzeugs hin zum ‚Zugang‘ ab, also der Nutzung durch Leasing bis hin zu ‚Mobility-as-a-Service‘-Konzepten. Ohne Software klappt das nicht.
Das bestätigt eine Studie von McKinsey[1], nach der sich der Markt für Automobilsoftware in den nächsten zehn Jahren mehr als verdoppeln und der Markt für Verifikations- und Validierungswerkzeuge sogar verdreifachen wird. Die Entwicklung von Software wird damit zum größten Kostentreiber und eventuell sogar zur größten Bremse bei der Entwicklung neuer Fahrzeuge.

[1] Automotive software and electronics 2030. Mapping the sector’s future landscape. McKinsey & Company. 2019

Wenn Software zum entscheidenden Teil der Wertschöpfungskette wird - wie ändert dies die Verfahren zur Qualitätssicherung und Qualitätskontrolle?
Ob Klimasteuerung, ABS oder Airbag - alle höheren Funktionen in Fahrzeugen basieren auf Software auf Komponentenebene. In modernen Autos wird die Software jedoch Teil des „Primärprozesses“ des Autofahrens und das digitale Ökosystem zur elementaren Basis für die Funktion und die Fähigkeiten des Produkts. Dadurch wirkt sich ein Software-Problem massiv auf das Auto aus, mit noch schlimmeren Folgen für das Image des Herstellers und den Ruf des Modells. Um den Fehler zu beseitigen, braucht es dann nicht einen einfachen „Produktrückruf“ in die Werkstatt, sondern eine Operation am offenen Herzen – und damit eine geänderte Qualitätssicherung. Wenn immer mehr Komponenten Informationen austauschen, verlangt dies neue Entwicklungsparadigmen und auch unterschiedliche Testmethoden. Safety und Security by Design sind damit unerlässlich, und Sicherheit muss das zentrale Motiv im Softwarelebenszyklus und damit im Qualitätsprozess sein. Durch die Einführung von immer mehr Funktionalität sind die klassischen Ansätze zur Softwarequalität nicht mehr ausreichend.

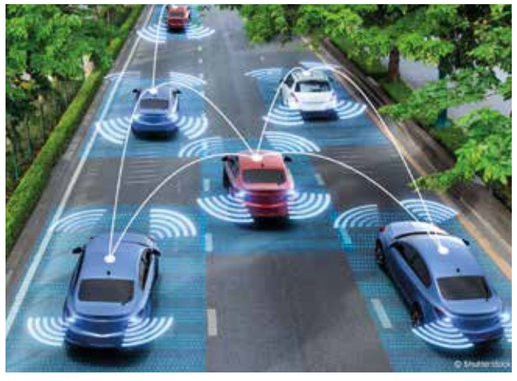
Werfen wir einen Blick auf die Software-Architektur und -Produktionslinie – welche Veränderungen kommen hier auf?
Aus Software-Sicht sehen wir ähnliche Entwicklungen, wie sie die Enterprise Software in den letzten zehn Jahren verändert haben. Software-Architekturen auf API-Basis und moderne Betriebssysteme (Linux), die IP-basierte Kommunikation verwenden (wie SOME/IP und DDS), bilden die Grundlage der neuen Software-Architektur. Neben dem Plattformwechsel geht auch die Software-Entwicklung selbst von der Wasserfall- und V-Modell-basierten Verifikation zu den modernen agilen und testgetriebenen Entwicklungsmethoden über. Dazu gehören die modernen Konzepte wie CI (Continuous Integration) und eventuell sogar CD (Continuous Deployment) von SW-Komponenten.

Wo Sie CI/CD-Integration nennen – was meinen Sie, wie diese den Software-Entwicklungsprozess beeinflussen?

CI/CD wirken wie „Steroide“ für den SW-Entwicklungsprozess. Der Einsatz von Code-Analyse, Unit-Testing und Coverage wird zu kontinuierlich durchgeführten Standardschritten. Das macht es für die Teams viel einfacher, sich mit den Reports auseinanderzusetzen und schrittweise Verbesserungen zu erzielen (statt sich mit großen Teilen der Ergebnisse erst in bestimmten Schritten des klassischen SW-Prozesses auseinanderzusetzen). So wie die Serienproduktion der Schlüssel zur Herstellung qualitativ hochwertiger Autos war, so tut CI/CD dasselbe für die SW-Produktion. Wir haben das in unseren Tools bereits implementiert, sodass Parasoft für diese neuen Zeiten gut gerüstet ist und die nötigen Werkzeuge zur Sicherstellung der Softwarequalität für die Automobilindustrie und ihre Zulieferer anbieten kann.

Wie schätzen Sie die Entwicklung in der Automobilbranche in Bezug auf autonome Fahrzeuge und Standards wie AUTOSAR, SOTIF, SAE 21434, UL 4600 und ISO 26262 ein?

Ganz offensichtlich erlebt die Automobilindustrie eine rasante Evolution. Es ist heute normal, dass Autos, die bereits verkauft und auf der Straße unterwegs sind, Software-Updates Over-the-Air erhalten. Diese Art der Entwicklung und insbesondere die von fortschrittlichen Fahrerassistenzsystemen (ADAS) bringen neue Herausforderungen in Bezug auf Sicherheit und Schutz mit sich. Es beruhigt mich, dass es unterschiedliche Standards je nach Einsatzbereich gibt, um die Gefahren im Vorfeld bestmöglich zu vermeiden. Darunter adressieren Normen wie die ISO 26262 die funktionale Sicherheit bei der Entwicklung elektrischer und elektronischer Systeme (E/E), die Antrieb, dynamische Regelsysteme sowie Fahrerassistenzsysteme umfassen. Zusätzlich bieten Plattformen wie AUTOSAR eine offene, standardisierte Software-Layer-Architektur, die die Sicherheit weiter verbessert, einschließlich Richtlinien für die Verwendung der Sprache C++14 bei der Entwicklung von kritischen und sicherheitsrelevanten Systemen.



Die zunehmende Komplexität und Unbekanntheit der neuen Technologien, zusammen mit Veränderungen in der internen und externen Umgebung, haben zu Sicherheitsbelangen geführt, die diese Standards nicht abdecken. Daraus entstanden weitere Ausprägungen von ISO 26262 wie SOTIF (Safety of the Intendedly Functionality). SOTIF hilft dabei, den Missbrauch der beabsichtigten Funktionalität zu analysieren und zu verhindern, sofern dadurch ein unsicheres Szenario entsteht. Beispielsweise eine Situation, in der sich das Fahrzeug während der Fahrt aufgrund eines initiierten Software-Updates abschaltet.

Standards wie SAE J3061, die durch ISO/SAE 21434 ersetzt wurden, verlangen die Durchführung einer ersten Bedrohungsanalyse und Risikobewertung (TARA Thread Analysis and Risk Assessment) zur Bewertung von potenziellen Bedrohungen in Bezug auf den Betrieb, die Privatsphäre und andere Faktoren, von denen ein Verkehrsteilnehmer/Fahrer betroffen sein kann. Ist das Risiko für eine bestimmte Bedrohung ausreichend hoch, ist ein Cybersicherheitsprozess erforderlich.

Schließlich gibt es speziell für den vollautonomen Fahrzeugbetrieb Normen wie die UL 4600. Sie konzentriert sich auf die Erstellung eines Sicherheitsnachweises für den Einsatz von Fahrzeugen des SAE Levels 4/5. Wie die Sicherheit von autonomen Fahrzeugen auf öffentlichen Straßen getestet werden kann, unterliegt wieder einer anderen Norm.

Welche Bedeutung haben diese Normen für das Verhältnis zwischen OEM und Zulieferer?

Generell spielen die Standards eine ganz entscheidende Rolle für die Sicherheit in der Automobilindustrie. OEMs tragen die Haftungskosten für die Auslieferung von unsicheren Fahrzeugen an die Massen. Zur Risikominimierung müssen die OEMs diese Standards übernehmen und einhalten – und sie sollten die gleiche Qualität und Einhaltung von ihren Zulieferern verlangen. Denn eine Schwachstelle in einer Komponente kann die Sicherheit des gesamten Systems untergraben, die möglichen Folgen können unter Umständen verheerend sein. Darum haben wir in Zusammenarbeit mit einigen unserer Kunden aus der Automobilbranche kundenspezifische Programmierstandards entwickelt, die MISRA, AUTOSAR C++14, CERT, CWE und andere kundenspezifische Regeln beinhalten – diese sind vom OEM und seinen Zulieferern anzuwenden. So stellen wir sicher, dass über die gesamte Lieferkette hinweg das gleiche Qualitätsniveau der Software besteht.

Zusätzlich bieten wir mit C/C++test eine einheitliche Testlösung, die Unit-Tests und strukturelle Code-Coverage-Funktionalität beinhaltet. Als Besonderheit unterstützt diese Lösung einen breiten Satz von Hardware-Targets und Entwicklungs-Ökosystemen, die Zulieferer und OEMs mit unterschiedlichen Entwicklungsinfrastrukturen nutzen können. Vorteilhaft ist auch, dass C/C++test vom TÜV SÜD für den Einsatz auf sicherheitskritischen Systemen zertifiziert wurde.

MISRA Dashboard: So könnte im Backup ein schneller Einblick aussehen, der über die MISRA-Konformität von Entwicklungslösungen informiert. (Bild: Parasoft)

Die Anforderungen an Audits und Konformitätsreports steigen zusehends für viele Firmen. Das ist eine enorme Herausforderung. Welche Unterstützung bietet Ihr Unternehmen?

Für uns, die wir mit unseren Tools und Lösungen sicherheitskritische Märkte wie die Automobilindustrie adressieren, ist die Unterstützung für Programmierstandards und Sicherheitsanforderungen eine Kernkompetenz. Wir sind führend bei Technologien für Coding-Standards, Unit-Testing, Coverage-Messung und Traceability des Codes als auch der Anforderungen. Entwickler erhalten bei uns auch neuere Tools für die interne als auch externe API-Validierung. Unsere C/C++-Entwicklungstestlösung integriert mehrere Testtechnologien in einem Tool. Teams können das Parasoft-Tooling einfach übernehmen, um Automobilstandards wie AUTOSAR, MISRA und ISO 26262 zu erfüllen. Benutzerdefinierte Konformitätsberichte und fortschrittliche Analysen zeigen genau auf, worauf sich die Entwicklungsanstrengungen konzentrieren müssen. Wie erwähnt, sind die Tools hierfür TÜV-zertifiziert und sie werden mit einem Tool-Qualifizierungs-Kit geliefert.

Noch ein Ausblick: Wie bewerten Sie den „eigenen“ SW-Entwicklungsprozess im Vergleich zum „Zukauf“ von SW-basierten Komponenten von Lieferanten?

Es zeigt sich heute schon: In den kommenden Jahren wird die Software zum wichtigsten Teil eines modernen Fahrzeugs und seines digitalen Ökosystems – und damit zum entscheidenden Faktor. Tatsächlich bauen sich die Hersteller das Wissen und das geistige Eigentum für die SW-Entwicklung selbst auf. So wie der Bau des Motors oft als Kernkompetenz angesehen wurde, wird dies im nächsten Jahrzehnt für die Software gelten. Ein sicheres Zeichen dafür ist, dass Volkswagen den Anteil der In-House entwickelten Software in den nächsten 5 Jahren von 10% auf 60% erhöhen möchte[2].

Vielen Dank für das Gespräch!

[2] https://www.volkswagenag.com/de/news/stories/2019/06/volkswagen-is-developing-more-of-its-own-software.html

Dirk Giesen

Dirk Giesen ist verantwortlich bei Parasoft für die Teams im Außendienst, Inside Sales und die Distributoren in EMEA. Die Teams streben langfristige, für beide Seiten nutzbringende Partnerschaften mit den Kunden an, und unterstützen sie, um Software kontinuierlich und effizient zu erstellen, wenn sie ihre Agile, DevOps, Konformität und sicherheitskritischen Entwicklungsinitiativen verfolgen.

Dirk Giesen hat einen Abschluss in Informatik und breite Erfahrung durch die Zusammenarbeit mit Kunden aus den Märkten High-Tech, Embedded und Business-IT. Bevor er in 2006 bei Parasoft einstieg, bekleidete er Positionen bei Telelogic (in 2006 von IBM übernommen), bei QA-Systems in der Distribution für Benelux und Deutschland sowie beim Benelux-Distributor Koning en Hartman.

When and how to generate test cases automatically.

The creation of test cases for embedded software is often a time-consuming task. The question is: Can automatic test generation help to increase the efficiency? This article describes use cases and methods for automatic test generation on software unit level and system level.

The size and complexity of embedded software is growing exponentially, in particular in the automotive industry. As one consequence, the manual creation of a sufficient amount of test cases becomes more and more challenging. But the automatic generation of test cases has always been a controversial topic. While some people dream about stopping any manual test activities, others say that test generation is not allowed. But who is right?

Traditional Embedded Software Development

Let's have a quick look at the possible test goals for which we can generate test cases:

1. **Structural coverage goals** come from the model or code directly. This includes, but is not limited to, Statement, Decision and MD/DC coverage. As a rule, it is intended that these test goals are covered by test cases. If those goals cannot be covered, it could be useful to have a closer look. It might be possible to have dead code which should be avoided in your production code.

2. **Robustness coverage goals** are also derived from the code and include, for instance, Division-by-Zeros and critical Down Casts. In contrast to the structural coverage goals, this condition is undesirable because it could have a critical impact on the robustness of your system.

3. **Drive-To-State goals** are user defined and represent specific states of the system under test (SUT). This determines confirmation of whether or not certain states can be reached, and what input combinations would create those states. This is also useful for monitoring a critical state that should not be covered by any input combination.

4. **Requirements-based test cases** can also be automatically generated, and are based on a machine-readable representation of the requirement previously created by the user. This is also called a "Formal Requirement" because it has a clearly defined syntax and semantics, and also describes timing constraints if applicable.

With these test goals in mind, we can have a look at available technologies to create these test cases. Basically, there are two technologies available on the market.

Random

The most common approach to generate test data is to generate random input data and to check what test goals are covered based on the generated data. This is done on an instrumented version of a model or code. To make this approach more efficient, a heuristic can control in what ranges random data is generated.
The advantage of this approach is that it is quite fast and it can be easily implemented. However, depending on the concrete implementation, you might get many redundancies and probably very long stimuli vectors. In addition, it can only show that a certain test goal can be covered. However, this method is unable to determine if a test goal like a Division-by-Zero can occur. This approach only makes sense for generating stimuli vectors for structural test goals.

Complete

The second approach is called Model Checking. Please note, that this method should not be confused with a guideline checker in an environment like Simulink. Model Checking originated in the early 1980s was originally invented by two research groups in the United States (Clark, Emmerson, McMillan) and France (Quielle/Sifakis). Model Checking is an efficient search procedure for finite state machines to determine whether they fulfill a specification expressed in temporal logic. To optimize this approach symbolic model checking or reduced ordered binary decision diagrams have been introduced.
A model checker performs a complete analysis of the behavior of a system against a specific static or temporal property and proves if this property holds or if it can be violated. In the case of a violation, a counter example is provided that enables the user to debug the violation. Complete analysis means that all possible runs of a system will be analyzed within one analysis task and deliver complete mathematical proof of the results. To generate stimulus vectors or test cases with this method, the Model Checker provides a counter example when a supposedly unreachable test goal can be covered. This approach can be used for all test goals mentioned before.

Scenario-based Virtual Validation for ADAS/AD

For ADAS/AD systems (where a safety-critical software is able to partially or completely take over the control of the vehicle), new standards like SOTIF lead to the need to perform a scenario-based virtual validation of the complete system. There are even already activities in the ASAM group to create a standardized language to describe these scenarios (OpenSCENARIO).

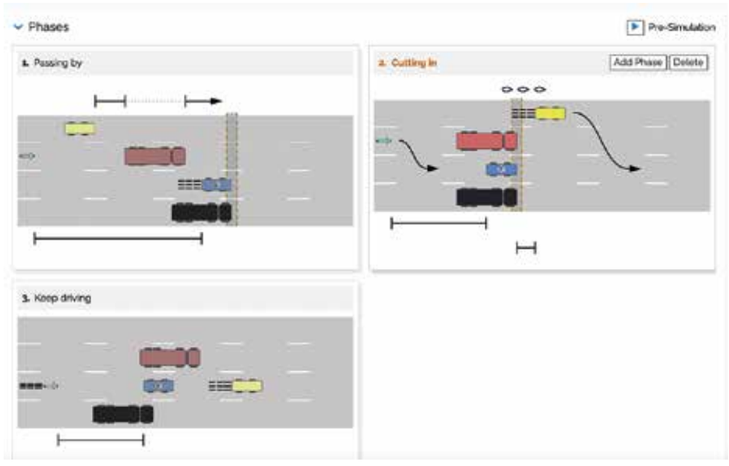


Figure 1: BTC Scenario-Based Engineering Platform

But it is also obvious that the needed number of scenarios can't be created manually. Recorded real-world scenarios can help, but recording the needed number of scenarios is economically infeasible.
To solve this, BTC proposes an intuitive and graphical high-level language to describe abstract traffic scenarios. The language describes an abstract scenario in multiple phases, each being modeled in a graphical way. These abstract scenarios are the basis for all subsequent steps in the validation process including automatic test generation and automatic scenario observation. The actual test cases (or concrete simulation scenarios) need to be generated with a smart strategy, on one hand avoiding a test explosion problem, on the other hand providing a statistical reasoning for completeness to enable homologation.

Despite being a proprietary language, BTC is aiming for full compatibility with the OPENScenario Standard and is therefore actively participating in the corresponding ASAM groups.

Conclusion

Automatic test generation is a powerful approach to deal with the growing complexity in embedded software projects. But the generated tests can only be as good as the input we provide to the test generator. If we don't provide any information, we can still generate structural tests for the software unit test, which are very valuable for use cases like Back-to-Back Test and Regression Test. For generating tests which take the desired behavior of the system or software into account, we need to provide information about the requirements in a machine-readable language.

Authors:
Markus Gros /
Wolfgang Meincke,
BTC Embedded Systems AG

AbsInt GmbH
www.absint.com

Airbus Operations GmbH
www.airbus.com

AVL Software and
Functions GmbH
www.avl.com

Robert Bosch GmbH
www.bosch.de

BTC Embedded Systems AG
www.btc-es.de

DB Netz AG
www.deutschebahn.com

Deutsches Forschungszentrum
für Künstliche Intelligenz GmbH
www.dfki.de

Deutsches Zentrum für
Luft- und Raumfahrt
www.dlr.de

embeteco GmbH & CO. KG
www.embeteco.com

Esterel Technologies GmbH c/o
ANSYS Germany GmbH
www.esterel-technologies.com

fortiss GmbH
www.fortiss.org

Fraunhofer-Verbund
IUK-Technologie
www.iuk.fraunhofer.de

FZI
www.fzi.de

Hella KGaA Hueck & Co.
www.hella.com

IAV GmbH Ingenieurgesellschaft
Auto und Verkehr
www.iav.com

ICS GmbH
www.think-safe-think-ics.de

INGenX Technologies GmbH
www.ingenx.tech

ITK Engineering GmbH
www.itk-engineering.de

Model Engineering
Solutions GmbH
www.model-engineers.com

OFFIS Institut für Informatik
www.offis.de

Parasoft Deutschland GmbH
www.parasoft.de

SIEMENS AG
www.siemens.de

TTTech Computertechnik AG
www.tttech.com

TÜV Nord Mobilität
GmbH & Co. KG
www.tuev-nord.de

Universität Bremen
www.uni-bremen.de

TU Braunschweig
www.tu-braunschweig.de

Carl von Ossietzky
Universität Oldenburg
www.uni-oldenburg.de

Verified Systems
International GmbH
www.verified.de