

MORGEN DENKER MAGAZIN

 **Fraunhofer**
IESE

Das Journal für Fans der digitalen Zukunft



**Driving the Future –
Technologie fährt sicher voraus**



Die beiden Institutsleiter des Fraunhofer IESE, Prof. Dr.-Ing. habil. Peter Liggesmeyer (links) und Prof. Dr.-Ing. Jörg Dörr (rechts) verfolgen ein gemeinsames Ziel: intelligente und sichere Mobilität.

Liebe Leserinnen und Leser,

wir stehen an einem Wendepunkt der Mobilität. Automobile und Nutzfahrzeuge entwickeln sich rasant weiter – von mechanisch geprägten Produkten hin zu hochkomplexen, softwaregetriebenen und vernetzten Gesamtsystemen. Fahrzeuge nehmen wahr, treffen Entscheidungen und unterstützen Menschen zunehmend autonom. Damit wächst unsere Verantwortung: für Sicherheit, Verlässlichkeit und Vertrauen.

Mit dieser Ausgabe des MORGEN DENKER Magazins richten wir den Blick genau auf diesen Wandel. Wir zeigen, wie sich die steigende Komplexität moderner Fahrzeuge beherrschen lässt – und welche Antworten Forschung und Industrie heute finden müssen. Denn je mehr Funktionen automatisiert oder KI-basiert umgesetzt werden, desto wichtiger wird es, dass Systeme stabil, nachvollziehbar und über den gesamten Lebenszyklus kontrollierbar bleiben. Gerade im Automotive- und Nutzfahrzeugbereich hat jede technische Entscheidung unmittelbare Auswirkungen in der realen Welt.

Die Beiträge dieses Hefts greifen zentrale Fragen der Zukunftsmobilität auf: Wie integrieren wir Künstliche Intelligenz sicher in Fahrzeuge? Wie gehen wir systematisch mit Unsicherheiten um, die sich nicht vollständig eliminieren lassen?

Und wie gestalten wir autonome Funktionen so, dass sie Menschen zuverlässig unterstützen – statt sie zu überfordern? Unsere Erfahrungen zeigen klar: Funktionale Sicherheit und Cybersecurity dürfen nicht getrennt betrachtet werden. Erst ihr Zusammenspiel macht Innovation langfristig tragfähig.

Besonders wichtig ist uns der Transfer unserer Forschung in die Praxis. Anhand konkreter Projekte wird deutlich, wie neue Methoden, Architekturen und Werkzeuge ihren Weg in reale Entwicklungs-, Absicherungs- und Freigabeprozesse finden – sowohl im Pkw-Umfeld als auch bei Nutzfahrzeugen. Genau hier zeigt sich der Mehrwert angewandter Forschung.

Als Institutsleitung des Fraunhofer IESE ist es unser Anspruch, den Wandel in der Automotive-Branche aktiv mitzugestalten. Wir wollen Orientierung geben, Vertrauen schaffen und Innovation verantwortungsvoll in die Anwendung bringen. Die Beiträge dieser Ausgabe stehen exemplarisch für diesen Weg.

Wir wünschen Ihnen eine anregende und inspirierende Lektüre – und freuen uns, wenn sie Ihnen neue Impulse für die Mobilität von morgen liefert.


Peter Liggesmeyer


Jörg Dörr

Inhalt

Autonome Systeme: Sicherheit entsteht im Zusammenspiel	6
Sicherheit autonomer Systeme als Netzwerk	8
Sicherheit für KI im Fahrzeug	10
Intelligente Sicherheit für die urbane Mobilität von morgen	11
Wenn das Fahrzeug den Menschen verstehen muss	12
Autonome Systeme unter Kontrolle	14
Safety trifft Security	15
»Autonomik ist der nächste große Paradigmenwechsel«	17
Software auf Rädern	20
Virtuelle Absicherung für das Software-Defined Vehicle	22
Unsicherheit messbar machen	23
3 Fragen an	24
Impressum	26





Autonome Systeme: Sicherheit entsteht im Zusammenspiel

Warum KI, Safety, Security, Regulierung und Vertrauen nicht getrennt betrachtet werden können

Autonome Systeme funktionieren besonders gut dort, wo die Welt berechenbar ist: in Lagerhallen, Produktionsumgebungen oder klar strukturierten Logistikprozessen. Sobald autonome oder teilautonome Systeme jedoch öffentliche, dynamische Räume betreten, ändert sich die Lage. Im urbanen Straßenverkehr müssen sie mit unvorhersehbarem menschlichem Verhalten, Mischverkehr, wechselnden Umweltbedingungen und komplexen rechtlichen Rahmenbedingungen umgehen.

Dabei wird deutlich: Sicherheit ist kein einzelnes technisches Merkmal. Sie entsteht aus dem Zusammenspiel funktionaler Sicherheit, Cybersecurity, Regulierung, Haftung und gesellschaftlicher Akzeptanz. Wie dieses Zusammenspiel wirkt, lässt sich nicht nur technisch erklären – man muss es erzählen.

Sicherheit im entscheidenden Moment – eine fiktive Story

Ein Morgen im Nieselregen. Der Verkehr ist dicht. Isa sitzt im Auto auf dem Weg zur Arbeit, unterstützt von einem teilautonomen System – ohne bewusst darüber nachzudenken. Genau solche alltäglichen Situationen sind die eigentliche Bewährungsprobe autonomer Systeme.

Ein Lieferwagen fährt voraus, daneben ein schlecht beleuchteter E-Scooter, kaum sichtbar im Regen. Die Sensoren erfassen ihn nur unscharf: Reflexionen, Bewegung und Wetter überlagern die Konturen. Die KI trifft keine eindeutige Entscheidung, stattdessen erkennt sie ihre Unsicherheit und meldet sie.

Weil die Unsicherheit bekannt ist, greift die funktionale Sicherheit. Das Fahrzeug von Isa bleibt defensiv und vermeidet riskante Manöver. Diese Reaktion ist kein spontaner Effekt, sondern das Ergebnis bewusster Systemauslegung: Was darf ein System tun – und was bewusst nicht?

All das setzt Vertrauen in die Daten voraus, denn Menschen verzeihen Maschinenfehler deutlich weniger als menschliche. Ein einzelnes Ereignis kann Vertrauen dauerhaft zerstören. Sensoren und Software müssen unverfälscht arbeiten, Systeme vor Angriffen geschützt sein.

Das weiß auch der Flottenbetreiber autonomer Fahrzeuge, der die autonomen Systeme im realen Einsatz verantwortet. Er blickt nicht auf einzelne Fahrzeuge, sondern auf Zustände. Ein System meldet erhöhte Unsicherheit – aber genau dafür sind Prozesse definiert. Es besteht kein Handlungsbedarf. Dass er nicht eingreifen muss, ist das Zeichen funktionierender Sicherheit.

Der Mensch bleibt Teil des Systems. Isa ist aufmerksam, aber nicht perfekt. Ihr Blick geht kurz zur Seite, die potenzielle Gefahr liegt woanders. Das Fahrzeug gleicht aus und reagiert ruhig. Systeme müssen auch dann sicher funktionieren, wenn Menschen müde, abgelenkt oder routiniert sind.

Am Ende dieses Morgens passiert nichts. Isa kommt an und der Verkehr fließt weiter. Dass all diese Ebenen zusammenspielen, ist kein Zufall. Es ist das Ergebnis klarer Normen und regulatorischer Rahmenbedingungen. Für Forschende sind sie Werkzeuge zur Beherrschung von Komplexität. Für Betreiber Absicherung. Für Nutzerinnen und Nutzer unsichtbar – aber wirksam. Und genau so ist Sicherheit in autonomen Systemen gedacht.

Die Geschichte zeigt: Sicherheit ist keine Produkteigenschaft. Sie entsteht im Zusammenspiel von Technologie, Mensch, Regeln und

Verantwortung. Wie dieses Zusammenspiel in der Praxis gestaltet wird, hängt vom jeweiligen Anwendungsfeld ab – und hier bringt das Fraunhofer IESE seine gebündelte Expertise ein:

100-prozentige KI-Sicherheit gibt es nicht – nur messbare Wahrscheinlichkeiten und Vertrauen durch Transparenz

KI lässt sich nicht vollständig testen, sondern nur über Wahrscheinlichkeiten, Qualitätskennzahlen und klar definierte Einsatzgrenzen absichern.

Genau hier setzt das Fraunhofer IESE an – mit **Methoden zur Messung von KI-Qualität, zur Quantifizierung von Restunsicherheiten und zur ingenieurmäßigen Absicherung von KI in sicherheitskritischen Systemen.**

Ohne Cybersecurity keine Safety – bei autonomen Systemen entscheidet das Zusammenspiel

Mit der wachsenden Vernetzung autonomer Systeme steigt nicht nur die funktionale Komplexität, sondern auch die **Angriffsfläche für gezielte Cyberangriffe.**

Deshalb verbindet das Fraunhofer IESE Safety und Security von Anfang an zu einem **integrierten Sicherheitsansatz.** Denn Cybersecurity ist kein reines IT-Thema mehr, sondern integraler Bestandteil funktionaler Sicherheit.

Autonome Systeme sprengen klassische Rollen – Hersteller, Betreiber und Gesetzgeber müssen Sicherheit gemeinsam neu denken

Je sicherheitskritischer ein autonomes System ist, desto schwieriger wird die **Trennung zwischen Hersteller und Betreiber.** Hat der Hersteller die Nutzungsbedingungen nicht angemessen beschrieben oder hat der Betreiber nicht ausreichend mitgedacht bei der Verwendung des Systems? Schwer zu sagen, wenn der Hersteller nicht genau weiß, wie sich das System in unbekannten Situationen verhalten wird und der Betreiber nicht alle Gefahrensituationen vorhersehen kann.

Gleichzeitig steigen mit wachsender Vernetzung auch regulatorische Anforderungen und Haftungsfragen. Sicherheit ist längst nicht mehr nur eine technische, sondern ebenso eine organisatorische, rechtliche und gesellschaftliche Aufgabe.

Das Fraunhofer IESE **integriert diese Dimensionen in tragfähige Lösungen** – technisch robust, regulatorisch abgesichert und im Betrieb verlässlich.

Autonome Systeme erfordern Sicherheit über alle Ebenen hinweg – von der Entwicklung bis zum realen Betrieb.



Sicherheit autonomer Systeme als Netzwerk

Warum Sicherheit bei KI neu gedacht werden muss

Dazu im Interview: Dr. Rasmus Adler, Research Manager »Autonome Systeme« am Fraunhofer IESE

Mit autonomen Systemen verschiebt sich der Maßstab: Sicherheit bedeutet nicht mehr, jeden Fehler auszuschließen, sondern Risiken transparent zu machen und beherrschbar zu halten. Im folgenden Interview erläutert Dr. Rasmus Adler, wie sich Sicherheit heute messen, gestalten und verantworten lässt – und welche Rolle die Lösungen des Fraunhofer IESE dabei spielen.

In einem Presseinterview haben Sie mal gesagt, dass autonome Systeme erst richtig funktionieren, wenn man ihre Grenzen versteht. Wie unterscheidet sich KI-basierte Sicherheit von klassischer Safety?

Bei klassischen Systemen kann man nahezu jede Ausführungsbedingung testen. Systeme, die auf Künstlicher Intelligenz basieren, arbeiten hingegen mit Wahrscheinlichkeiten – das lässt sich nicht vollständig durch Tests abdecken. Die Frage lautet daher nicht »Wie mache ich KI perfekt?«, sondern »Wie mache ich KI beherrschbar?«. Sicherheit entsteht durch messbare Unsicherheiten, klar definierte Einsatzgrenzen und transparente Qualitätskennzahlen. Hier setzt unser Ansatz an: Wir quantifizieren Restfehler und entwickeln Methoden, um die Qualität von KI-Systemen in sicherheitskritischen Kontexten zuverlässig messbar zu machen. Dazu gehören z. B. Model-based Safety-Engineering-Werkzeuge wie unser Tool safeTbox, die die Integration funktionaler Sicherheit in komplexe Systeme unterstützen.

Die Öffentlichkeit nimmt oft einzelne Vorfälle wahr und schließt daraus auf generelle Unsicherheit. Wie begegnet man dieser Erwartungshaltung?

Menschen verzeihen Fehler bei Maschinen deutlich weniger als bei Menschen. Ein einziger Vorfall kann Vertrauen nachhaltig beschädigen, auch wenn Millionen anderer Situationen korrekt verlaufen. Deshalb brauchen wir nicht nur robuste Technik, sondern auch Erklärbarkeit und Nachvollziehbarkeit – das heißt, Systeme müssen nicht nur funktionieren, sondern auch darlegen können, warum Entscheidungen getroffen wurden. Zusätzlich arbeiten wir an Konzepten wie AI-gestützter Sicherheits- und

Risikoanalyse, etwa im Projekt QAI4SE, das zeigt, wie KI selbst

helfen kann, Unsicherheiten früher zu erkennen und Sicherheitsanalysen effizienter zu machen.

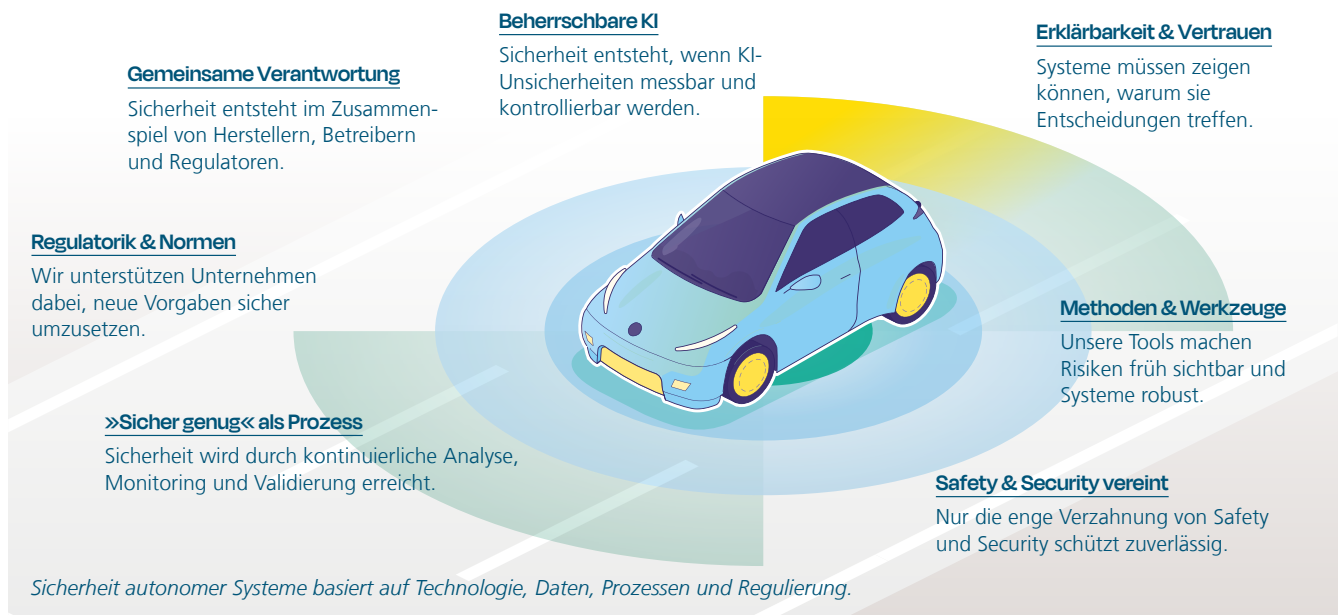
Ein zentrales Thema ist die Verzahnung von Safety und Security – wie sehen Sie diese Verbindung?

Safety und Security dürfen nicht isoliert gedacht werden. Cyberangriffe auf autonome Systeme können direkt sicherheitsrelevant werden – ein manipuliertes Sensordatenbild führt schnell zu falschen Entscheidungen. Deshalb betreiben wir am IESE integrierte Safety-und-Security-Forschung, die beide Disziplinen zusammenführt, statt sie getrennt zu behandeln. Security-Engineering-Methoden, die Systeme und Daten gegen Angriffe schützen, sind heute ein Grundpfeiler funktionaler Sicherheit.

Wie übersetzt sich diese Forschung in konkrete Lösungen für die Praxis?

Unsere Lösungen reichen von modularer Risiko- und Sicherheitsarchitektur bis zu konkreten Werkzeugen für Entwickler und Betreiber. Neben safeTbox zur Absicherung sicherheitskritischer Systeme bieten wir z. B. Konzepte und Tools für die datenbasierte Sicherheitsanalyse, die Entwickler dabei unterstützen, frühzeitig Risiken zu identifizieren. Im Predictive Autonomy Lab arbeiten wir zudem an empirischen Methoden zur besseren Erfassung von menschlicher Assistenz und Fahrerzuständen, um Systeme mit realistischen Verhaltensmodellen abzustimmen.

Gesetzgebung wie die EU-KI-Verordnung und der Cyber Resilience Act verschärfen Anforderungen.



Was bedeutet das für Unternehmen?

Diese Regulierungen verlangen nicht nur technische Nachweise, sondern auch organisatorische und prozessuale Maßnahmen – und das über den gesamten Lebenszyklus eines Systems. Betreiber und Hersteller müssen gemeinsam Risiken bewerten und absichern. Funktionale Sicherheit allein reicht nicht mehr; sie muss durch kontinuierliche Überwachung, Security-Updates und geeignete Risikoargumentation ergänzt werden.

Ein Beispiel unserer Arbeit ist das Projekt LOPAAS (Layers of Protection Architecture for Autonomous Systems). Dort entwickeln wir gemeinsam mit Partnern neue Architekturkonzepte, die Safety-Argumentationen für autonome Fahrzeuge unterstützen und in Normungsgremien eingebracht wurden – ein Schritt hin zu standardisiertem, praxisnahem Sicherheitsnachweis.

Damit sprechen Sie eine strukturelle Verschiebung an. Wie verändert sich dabei die Zusammenarbeit zwischen Hersteller und Betreiber?

Sicherheit ist heute kein singuläres Produktmerkmal mehr, sondern ein gemeinsamer Prozess. Hersteller bringen technische Kompetenz ein, Betreiber Kenntnis des realen Einsatzumfelds. Regulatoren legen Rahmenbedingungen fest. Nur wer diese Perspektiven zusammenbringt, kann tragfähige Sicherheitskonzepte entwickeln. Diese gemeinsame Verantwortung ist kein elegant formulierter Begriff – sie ist technische und organisatorische Realität.

»Sicherheit entsteht durch messbare Unsicherheiten, klar definierte Einsatzgrenzen und transparente Qualitätskennzahlen.«

Zum Schluss: Wie kann man objektiv erkennen, ob ein autonomes System »sicher genug« ist?

Das ist das zentrale Spannungsfeld: Es gibt keine absolute Sicherheit. Aber es gibt messbare Ergebnisse – über Risikoanalysen, Einsatzgrenzen, kontinuierliche Monitoringprozesse, Test- und Validierungsframeworks. Ob ein System »sicher genug« ist, hängt vom Kontext ab, vom Risiko, das die Gesellschaft akzeptiert, und davon, wie transparent Entscheidungen getroffen werden. Sicherheit ist kein Zustand – sie ist ein kontinuierlicher, gesteuerter Prozess.



Dr. Rasmus Adler

Research Manager »Autonome Systeme«



Weitere Infos:

www.iese.fraunhofer.de/de/leistungen/funktionale-sicherheit.html

Safe AI Engineering – ein Forschungsprojekt für vertrauenswürdiges automatisiertes Fahren

Safe AI Engineering ist ein vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) gefördertes Forschungsprojekt, das neue Maßstäbe für die Sicherheit KI-basierter Fahrfunktionen im automatisierten Fahren setzt. Über eine Laufzeit von drei Jahren (2025–2028) entwickeln 24 Partner aus Industrie und Wissenschaft gemeinsam Methoden, mit denen Künstliche Intelligenz im Fahrzeug über ihren gesamten Lebenszyklus hinweg sicher, nachvollziehbar und zulassungsfähig gestaltet werden kann.

Der Einsatz von KI gilt als Schlüssel für automatisiertes Fahren – gleichzeitig steigen damit die Anforderungen an Absicherung und Sicherheitsnachweise erheblich. Klassische Verfahren stoßen bei lernenden, datengetriebenen Systemen an ihre Grenzen. Safe AI Engineering adressiert genau diese Herausforderung und verfolgt einen ganzheitlichen Ansatz, der Sicherheit nicht als nachgelagerten Schritt, sondern als integralen Bestandteil des Entwicklungsprozesses versteht.

Sicherheit über den gesamten KI-Lebenszyklus

Im Zentrum des Projekts steht die Entwicklung einer durchgängigen Methodik zur Absicherung von KI-Funktionen – von der Planung über die Entwicklung und Tests bis hin zu Betrieb, Monitoring und kontinuierlicher Verbesserung. Ein begleitender, praxisnaher Sicherheitsnachweis spielt dabei eine zentrale Rolle, insbesondere im Hinblick auf zukünftige Zulassungsverfahren für automatisierte Fahrzeuge.

Das Fraunhofer IESE bringt in Safe AI Engineering seine langjährige Expertise in Systems Engineering, Safety Engineering und der methodischen Integration von KI ein.

Von Datenqualität bis Laufzeitüberwachung

Zu den Kerninnovationen des Projekts gehört die vereinheitlichte Nutzung hochwertiger Trainings- und Validierungsdaten, einschließlich synthetischer Daten. Diese können systemübergreifend eingesetzt werden und ermöglichen eine nachhaltigere Datennutzung bei gleichzeitig reduzierten Kosten. Ergänzend werden erklärbare und robuste Absicherungsmethoden entwickelt, die eine bessere Bewertung der Leistungsfähigkeit von KI-Modellen erlauben.

Ein weiterer Fokus liegt auf der evidenzbasierten Überwachung von KI-Modellen im Betrieb, um deren Qualität auch zur Laufzeit kontinuierlich zu bewerten und zu verbessern. Die Methodik wird exemplarisch an einer KI-Perzeptionsfunktion zur Fußgängererkennung erarbeitet und in mehreren Anwendungsszenarien mit steigender Komplexität erprobt – von statischen Szenen bis hin zu realitätsnahen Verkehrssituationen.

Beitrag zur sicheren Mobilität der Zukunft

Safe AI Engineering ist Teil der VDA-Leitinitiative autonomes und vernetztes Fahren und gehört zur zweiten Generation der sogenannten KI-Familie. Langfristig soll das Projekt einen Standard für die Absicherung KI-basierter Funktionen im automatisierten Fahren etablieren. Fahrzeughersteller und Zulieferer profitieren von einer durchgängigen, wirtschaftlich nutzbaren Methodik, während Behörden auf transparente und vergleichbare Sicherheitsnachweise zurückgreifen können. Für die Nutzenden bedeutet dies sichere und zuverlässige KI-Funktionen im Fahrzeug – und damit mehr Vertrauen in automatisierte Mobilität.



Weitere Infos: <https://safe-ai-engineering.de/>

Intelligente Sicherheit für die urbane Mobilität von morgen

Hitachi und Fraunhofer IESE entwickeln Sicherheitslösungen für autonome Shuttles

Um eine neue Generation urbaner Mobilität sicher und praxisnah umzusetzen, haben Hitachi Ltd. und das Fraunhofer IESE ihre Kompetenzen in einer langjährigen Partnerschaft gebündelt. Im Fokus steht die Entwicklung innovativer Safety-Engineering-Methoden für autonome Shuttles – erprobt anhand eines Beispielszenarios, das auf dem Bus-Rapid-Transit-System (BRT) in Japan basiert. BRT-Straßen kreuzen reguläre Fahrspuren sowie Fußgängerüberwege und schaffen damit komplexe Interaktionsszenarien, die hohe Anforderungen an die Fahrzeugsicherheit stellen.

Dynamisches Risikomanagement statt Worst-Case-Denken

Klassische Sicherheitsmodelle basieren häufig auf sehr konservativen Worst-Case-Annahmen, also auf der Betrachtung der ungünstigsten denkbaren Situationen. Dies führt zwar zu einem hohen Sicherheitsniveau, jedoch auch zu ineffizientem Verhalten, etwa durch unnötige Stopps.

Gemeinsam mit Hitachi haben die Experten des Fraunhofer IESE daher einen dynamischeren Ansatz entwickelt. Die Methode »SINADRA« ermöglicht eine situationsbewusste Risikoabschätzung zur Laufzeit, das heißt, Risiken werden während des Betriebs kontinuierlich anhand der aktuellen Situation bewertet. »ConSerts« ermöglichen es auf SOTIF-Fehler (Safety of the Intended Functionality) während der Laufzeit zu reagieren und das Systemverhalten gezielt anzupassen, um weiterhin Sicherheit zu garantieren. Darunter versteht man sicherheitskritisches Fehlverhalten automatisierter Fahrfunktionen, das nicht durch technische Defekte entsteht, sondern durch Grenzen der Funktion selbst, durch Umwelteinflüsse oder durch Fehlbedienung.

Ergänzt wird dieser Ansatz durch das Symbiotic-Safety-Konzept von Hitachi, bei dem System und Umgebung stärker gemeinsam betrachtet werden, um Sicherheit zu gewährleisten. Die entwickelten Modelle wurden in ausführbare Software überführt und sowohl in Simulationen als auch in einer realen Testumgebung auf dem Hitachi-Campus in Japan erfolgreich getestet. Die Ergebnisse zeigen: weniger unnötige Stopps bei gleichbleibendem Sicherheitsniveau.

Von passiver Dokumentation zu aktiver »Safety Assurance«

Gemeinsam wurde ein modellbasierter Ansatz entwickelt, der sogenannte Safety Cases – strukturierte Nachweise und Argumentationen zur Systemsicherheit – von passiven Dokumenten in aktive Mechanismen zur Absicherung überführt.

»Durch unsere lang-jährige Zusammenarbeit mit dem Fraunhofer IESE konnten wir zeigen, dass eine dynamische, situationsbewusste Absicherung die Praxistauglichkeit autonomer Shuttles erheblich verbessern kann, ohne die Sicherheit zu beeinträchtigen.«

Satoshi Otsuka, Ph.D.
Chief Researcher,
Hitachi Ltd.



Durch die systematische Rückverfolgbarkeit von Safety-Case-Elementen mit Entwicklungsartefakten und Sicherheitsartefakten, also mit konkreten Ergebnissen aus der Systementwicklung und dem Sicherheitsprozess wie Anforderungen, Modellen oder Tests, können aufwändige Absicherungsprozesse teilweise automatisiert werden. Diese Verknüpfung ist im Open-Dependability-Exchange-Metamodell (ODE) formal beschrieben, einem standardisierten Modell zur Strukturierung sicherheitsrelevanter Informationen.

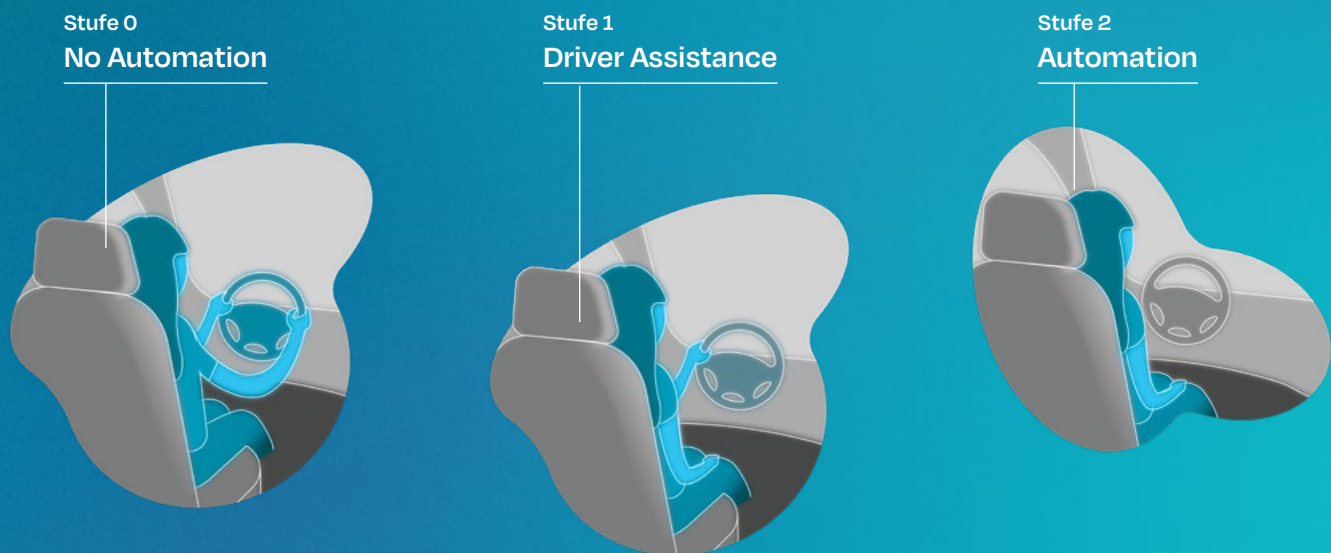
Ein zentraler Aspekt ist dabei die sogenannte ODD-Abdeckung (Operational Design Domain). Diese beschreibt die Betriebsbedingungen, unter denen ein automatisiertes Fahrsystem sicher betrieben werden kann, beispielsweise bestimmte Wetterverhältnisse, Straßenarten oder Verkehrssituationen. Für die systematische Überprüfung dieser Abdeckung innerhalb eines Sicherheitsnachweises wurde eine eigene algorithmische Lösung entwickelt. Insgesamt ermöglicht der Ansatz eine durchgängige und effektive Absicherung automatisierter Fahrsysteme über den gesamten Lebenszyklus hinweg.

Langjährige Partnerschaft mit Zukunftsperspektive

Die mehrjährige Zusammenarbeit zwischen dem Fraunhofer IESE und Hitachi zeigt, wie eine vertrauensbasierte, internationale Partnerschaft technologische Innovation nachhaltig vorantreiben kann. Die entwickelten Methoden sind auf weitere Anwendungsfelder übertragbar und stärken Hitachis Position im Bereich sicherer autonomer Systeme.

Weitere Infos: <https://www.iese.fraunhofer.de/de/referenz/hitachi-ltd-urbane-mobilitaet.html>





Wenn das Fahrzeug den Menschen verstehen muss

Fahrerzustandserkennung als Grundlage teilautomatisierten Fahrens

Für das teilautomatisierte Fahren sind zuverlässige Systeme zur Erkennung des Fahrerzustands eine zentrale Voraussetzung. Denn Assistenz- und Automatisierungsfunktionen können ihre Wirkung nur dann sicher entfalten, wenn sie wissen, womit der Mensch am Steuer gerade beschäftigt ist – und ob seine Aufmerksamkeit noch ausreicht, um die Fahraufgabe zu übernehmen. Moderne Fahrzeuge nutzen dafür eine Kombination aus Innenraumkameras und weiteren Sensoren: Kopfhaltung, Blickrichtung, Augenöffnung und Lidschlagsrate liefern Hinweise auf Aufmerksamkeit oder Ermüdung. Ergänzend erfassen Lenkrad- und Sitzsensoren, ob der Fahrer aktiv lenkt oder seine Körperhaltung verändert. Ein schlafender Fahrer lässt sich so klar identifizieren – doch bereits davor kündigt sich ein Aufmerksamkeitsverlust durch subtilere Veränderungen an, etwa langsameren Lidschlag oder einen lockereren Griff am Lenkrad. In solchen Situationen können Assistenzsysteme gezielt eingreifen, etwa durch akustische Warnungen, haptische Signale oder Hinweise im Cockpit.

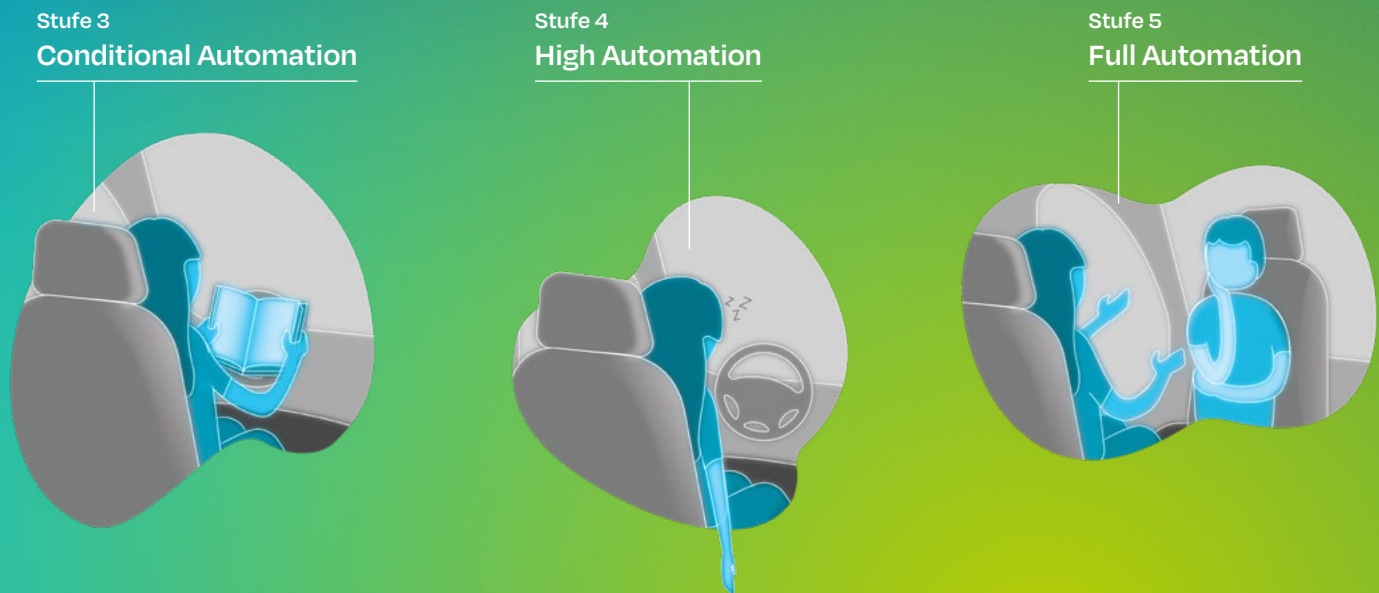
Warum Künstliche Intelligenz unverzichtbar ist

Die Vielzahl dieser Messdaten macht deutlich, warum Künstliche Intelligenz eine zentrale Rolle bei der Fahrerzustandserkennung

spielt. Einzelne Messwerte sind kaum aussagekräftig, da Fahrverhalten und Aufmerksamkeit stark individuell geprägt sind. KI-basierte Systeme lernen daher zunächst einen Normalzustand des jeweiligen Fahrers und erkennen anschließend Abweichungen davon. Dazu kombinieren sie Informationen etwa zum Blickverhalten, zur Körperhaltung und zu Reaktionszeiten auf Systemaufforderungen. Gerade in solchen komplexen, hochdimensionalen Datensätzen liegt eine besondere Stärke von KI: Muster zu erkennen, die mit klassischen regelbasierten Verfahren kaum erfassbar wären.

Sicherheit und Unsicherheit in KI-basierten Systemen

Mit dem Einsatz von KI stellen sich neue Fragen an Sicherheit und Zuverlässigkeit. Während im klassischen Sicherheitsengineering alle relevanten Reaktionspfade systematisch getestet werden können, ist dies bei lernenden Systemen prinzipiell nicht möglich – ihre möglichen Zustände und Reaktionen sind praktisch unendlich. Eine gewisse Unsicherheit bleibt daher selbst bei größter Sorgfalt bestehen. Die IESE-Forschungsprojekte wie Safe AI Engineering und CONTROL setzen genau hier an: Ziel ist es, diese Unsicherheiten messbar zu machen und Systeme so zu gestalten, dass sie angemessen darauf reagieren



Fünf Stufen der Autonomie: vom Assistenzsystem zur vollständigen Selbststeuerung

– etwa durch vorsichtigeres Fahrverhalten, reduzierte Geschwindigkeit oder kontrolliertes Ausweichen. Methoden zur Quantifizierung von Unsicherheiten im Maschinellen Lernen sind bereits national über die DIN SPEC 92005 standardisiert und werden aktuell im WIPANO-Projekt UncertAlnty mit Blick auf generative KI weiterentwickelt und in internationale Normungsprozesse eingebracht. Ergänzend rückt auch die Cybersecurity in den Fokus, denn jede Sicherheitslücke kann bei autonomen Systemen unmittelbar zu einem Safety-Risiko werden.

Adaptive Mensch-Maschine-Interaktion

Ein weiteres Potenzial KI-basierter Fahrerzustandserkennung liegt in einer adaptiveren Mensch-Maschine-Interaktion. Warnungen und Eingriffe sollten nicht pauschal erfolgen, sondern den Fahrerzustand mit dem situativen Kontext abwägen. Erkennt ein System beispielsweise eine Gefahrensituation, während der Fahrer in eine andere Richtung blickt, kann eine Warnung sinnvoll sein – selbst wenn der Fahrer grundsätzlich aufmerksam erscheint. Umgekehrt lassen sich unnötige Warnungen vermeiden, wenn der Fahrer die relevante Situation bereits erfasst hat. Besonders wichtig ist diese intelligente Priorisierung bei Nutzfahrzeugen und Arbeitsmaschinen, bei denen das Fahren oft nur eine von mehreren automatisierten Aufgaben ist. Die permanente manuelle Überwachung aller Funktionen würde hier schnell die menschlichen Fähigkeiten überfordern.

Wenn Zuverlässigkeit zum Risiko wird

Eng damit verknüpft ist das Out-of-the-Loop-Phänomen: Je zuverlässiger ein System arbeitet, desto stärker sinkt die Aufmerksamkeit des Menschen bei der Überwachung. Paradoxerweise kann dies das Unfallrisiko erhöhen.

Klassische Gegenmaßnahmen – etwa die permanente Aufforderung, das Lenkrad zu halten – schmälern jedoch den Nutzen der Automatisierung. Ziel aktueller Forschung ist es daher, situationsabhängig zu bestimmen, ob und welche Art von Überwachung notwendig ist, und den Fahrer rechtzeitig einzubinden. Während bei Level-3-Systemen dafür typischerweise wenige Sekunden zur Verfügung stehen, können Level-4-Fahrzeuge selbstständig einen sicheren Zustand erreichen, ohne dass der Mensch eingreifen muss.

Warum Level 5 auf absehbare Zeit unrealistisch bleibt

Vor diesem Hintergrund wird auch deutlich, warum eine vollständige Level-5-Automatisierung weiterhin als große Herausforderung gilt. Während Level 4 an klar definierte Einsatzbedingungen wie bestimmte Strecken oder Wetterlagen gebunden ist, soll Level 5 unter allen Bedingungen funktionieren. Selbst bei großen technologischen Fortschritten wird der sichere Einsatz autonomer Systeme jedoch immer von Randbedingungen abhängen – etwa von der physikalischen Grenze der Fahrbarkeit bei Glatteis. Wahrscheinlicher ist daher, dass diese Bedingungen schrittweise weniger einschränkend werden. Entscheidend ist dabei auch das Geschäftsmodell: Ein privat genutztes Fahrzeug unterliegt anderen Anforderungen als ein betriebenes System. Diese Unterschiede werden in den Automatisierungsstufen bislang kaum berücksichtigt, spielen für die praktische Umsetzung jedoch eine zentrale Rolle.

Weitere Infos:

<https://www.iese.fraunhofer.de/de/trend/autonomes-fahren.html>



Autonome Systeme unter Kontrolle

Forschungsprojekt CONTROL – Risiken beherrschen in offenen Verkehrsumgebungen



Controlling Risk for Highly Automated Transportation Systems
Operating in Complex Open Environments

CONTROL ist ein vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) gefördertes Forschungsprojekt, das neue Ansätze für die sichere Nutzung autonomer Systeme auf Straße und Schiene entwickelt. Über eine Laufzeit von drei Jahren arbeiten 24 Partner aus Industrie und Wissenschaft seit Oktober 2025 gemeinsam daran, wie autonome Pkw, Lkw, Busse und Züge auch in offenen, hochdynamischen Verkehrsumgebungen zuverlässig betrieben werden können – selbst dann, wenn sich Rahmenbedingungen unerwartet ändern.

Autonomes Fahren gilt als Schlüsseltechnologie für die Mobilität der Zukunft. Es verspricht mehr Komfort, höhere Effizienz, geringere Emissionen und neue Mobilitätsangebote wie autonome People Mover oder fahrerlose Gütertransporte. In der Praxis sind heutige Systeme jedoch meist auf klar definierte Einsatzbedingungen beschränkt. In der realen Welt treffen sie auf seltene, aber sicherheitskritische Situationen – sogenannte Long-Tail-Events – etwa plötzlich auftauchende Hindernisse, eingeschränkte Sicht oder stark wechselnde Witterungsbedingungen. Genau hier setzt CONTROL an.

Unsicherheiten systematisch beherrschen

Im Zentrum des Projekts steht die Frage, wie autonome Systeme mit Unsicherheit umgehen können. CONTROL entwickelt dafür eine domänenübergreifende Sicherheitsargumentation, die Unsicherheiten im Fahrzeugbetrieb erfasst, bewertet und kontrollierbar macht. Diese Erkenntnisse fließen direkt in die Architektur autonomer Systeme ein, sodass Fahrzeuge situationsabhängig reagieren können – etwa durch angepasste Geschwindigkeit, vorsichtiges Fahrverhalten oder kontrolliertes Ausweichen.

Ergänzt wird dieser Ansatz durch neue Qualitätsmetriken, adaptive Sensorfusion sowie eine simulationsgestützte Validierung. Die entwickelten Methoden werden im Projektverlauf in Versuchsträgern der beteiligten Partner praxisnah erprobt – sowohl auf der Straße als auch auf der Schiene.

Das Fraunhofer IESE bringt im Projekt CONTROL seine methodische Expertise im Bereich Systems Engineering und Sicherheit

komplexer Systeme ein. Der Fokus liegt dabei auf der strukturierten Betrachtung von Unsicherheiten sowie deren Integration in die Entwicklung und Absicherung autonomer Systeme. Darüber hinaus übernimmt das Fraunhofer IESE den wissenschaftlichen Co-Lead im Arbeitspaket zur domänenübergreifenden Sicherheitsargumentation. Im Mittelpunkt stehen dabei die Entwicklung einer Gesamtargumentationsstruktur in GSN sowie die Ableitung und Analyse von Safety Performance Indikatoren aus dem Sicherheitsargument. Das Institut baut dabei auf seiner langjährigen Erfahrung mit Argumentationsmethoden und dem safeTbox-Werkzeug auf, die in Projekten wie DEIS, SESAME und weiteren nationalen und internationalen Forschungsvorhaben entwickelt wurden.

Grundlage für neue Mobilitätsstandards

CONTROL ist Teil der VDA-Leitinitiative autonomes und vernetztes Fahren und baut auf den Ergebnissen früherer methodischer Projekte wie PEGASUS und VVM auf. Die im Projekt entwickelten Konzepte sollen langfristig die Wettbewerbsfähigkeit der deutschen Industrie stärken und eine Grundlage für neue Standards schaffen – von automatisierten Fahrzeugen auf Straße und Schiene bis hin zu weiteren Anwendungsfeldern wie industrieller Automation oder Robotik.

Mit seinem Fokus auf seltene, aber sicherheitskritische Ereignisse leistet CONTROL einen wichtigen Beitrag dazu, autonome Systeme robuster, transparenter und vertrauenswürdiger zu machen – und damit einen entscheidenden Schritt in Richtung alltagstauglicher autonomer Mobilität.

Weitere Infos: www.control-projekt.de



Safety trifft Security

Ganzheitliche Absicherung vernetzter Mobilität

Mit der zunehmenden Digitalisierung und dem stetig wachsenden Softwareanteil moderner Fahrzeuge wachsen Safety und Security untrennbar zusammen. Funktionale Sicherheit allein genügt nicht mehr – automatisierte und vernetzte Systeme müssen gleichzeitig vor Cyberangriffen geschützt werden. Gerade im Automotive-Umfeld ist daher ein integrierter Ansatz erforderlich, der Safety- und Security-Engineering systematisch verbindet und den das Fraunhofer IESE konsequent umsetzt.

Safety: Predictive Autonomy Lab (PAL)

Im modernen Fahrsimulator-Labor analysiert das Fraunhofer IESE menschliches Fahrverhalten in sicherheitskritischen Situationen. Durch eine realitätsnahe Simulation von Umweltbedingungen und Verkehrssituationen lassen sich kausale Zusammenhänge in den Entscheidungen der Fahrer erkennen. Umfangreiche Sensortechnik wie Eye-Tracker zur Blick- und Aufmerksamkeitsanalyse sowie Sensoren zur Erfassung physiologischer Vitalparameter erlauben Rückschlüsse auf Stress, kognitive Belastung und Situationsbewusstsein der Fahrer. Zusätzlich ermöglicht eine Fußgänger-simulation mit VR-Brille und VR-Plattform die realitätsnahe Untersuchung von Interaktionen zwischen Fahrern, automatisierten Fahrzeugen und ungeschützten Verkehrsteilnehmenden. Diese Erkenntnisse fließen direkt in die Verbesserung von Fahrerassistenz- und Automatisierungssystemen ein – insbesondere in die Auslegung präziserer Warn- und Interventionsstrategien.

Methodischer Ansatz mit Praxisbezug

Die im PAL entwickelten Lösungen werden fest in etablierte Safety-Engineering- und dynamische Risikomanagementprozesse eingebettet. Interdisziplinäre Teams aus Safety Engineers, Psychologen und Fachbereichsexperten arbeiten gemeinsam an maßgeschneiderten Konzepten – abgestimmt auf Systemkontext und reale Nutzungsszenarien. Human-in-the-Loop-Simulationen sorgen für eine valide Absicherung menschlicher Faktoren in sicherheitskritischen Fahrsituationen.

Intelligente Fahrerüberwachung

Konventionelle Driver Monitoring Systeme (DMS) stoßen zunehmend an ihre Grenzen: Sie berücksichtigen oft nur Worst-Case-Annahmen und interne Fahrzeugdaten, was zu unnötigen Warnungen und Frustration bei den Nutzern führt. Im PAL hingegen werden externe Fahrsituationen, das aktuelle Risiko sowie Systemmängel in die Bewertung der Fahreraufmerksamkeit integriert.

Das Ergebnis sind präzisere, akzeptanzsteigernde Warn- und Interventionsstrategien für Fahrerüberwachungssysteme (Driver Control Assistant Systems).

Mehrwert für die Automobilindustrie

Das Predictive Autonomy Lab verbindet empirische Forschung mit Safety Engineering und bietet klare Vorteile:

- Verbesserte Systemperformance durch valide Fahrer-Verhaltensmodelle und Digitale Zwillinge menschlicher Zustände
- Reduktion von Fehlalarmen dank situationssensitiver und risikobewusster Sicherheitsmodelle
- Kosteneffiziente Sicherheitsargumentation und -validierung, z. B. für Fahrerübernahme- oder Überwachungskonzepte
- Unterstützung bei Normen- und Standardkonformität in einem sich dynamisch entwickelnden regulatorischen Umfeld
- Höhere Kundenakzeptanz durch nutzerzentrierte, weniger intrusive Assistenzsysteme

Sicherheit als Innovationsbeschleuniger

Mit dem Predictive Autonomy Lab bietet das Fraunhofer IESE der Automobilindustrie eine leistungsfähige Plattform, um Sicherheit, Effizienz und Nutzerakzeptanz automatisierter Fahrfunktionen gezielt zu steigern. Die Kombination aus empirischer Fahrerhaltensforschung und systematischem Safety Engineering macht Sicherheit zum Treiber nachhaltiger Innovation.

Weitere Infos:

www.iese.fraunhofer.de/predictive-autonomy-lab



Security: Lernlabor Cybersicherheit »Sicheres Cloud-Computing«

Mit dem Lernlabor Cybersicherheit »Sicheres Cloud-Computing« bietet das Fraunhofer IESE gemeinsam mit der Hochschule Worms eine praxisnahe Umgebung für Weiterbildung und Technologietransfer im Bereich IT- und Cloud-Security. Ziel ist es, Fach- und Führungskräfte zu befähigen, sichere Cloud-Architekturen zu entwickeln, regulatorische Anforderungen umzusetzen und Cyber Risiken wirksam zu beherrschen.

Im Mittelpunkt stehen interaktive Trainingsformate mit realitätsnahen Übungsszenarien – von sicheren Entwicklungsprozessen über Schwachstellenanalysen bis hin zu Penetrationstests in isolierten Cloud-Testumgebungen. Kreative Schulungsräume und das spezialisierte Security-Lab ermöglichen es, Angriffs- und Verteidigungsszenarien praxisnah zu erproben.

Weitere Infos zum Lernlabor und das aktuelle Kursangebot:
www.iese.fraunhofer.de/lernlabor-cloud-computing



SEMINARTIPP

Das eintägige Seminar »Automotive Cybersecurity« des Fraunhofer IESE vermittelt praxisnah die Grundlagen des Security Engineerings nach ISO/SAE 21434. Dabei lernen Teilnehmende, wie Sicherheitsbedrohungen systematisch analysiert und daraus konkrete Security-Anforderungen abgeleitet werden. Dieses Seminar eignet sich besonders für alle, die den Bezug zwischen Safety und Security besser verstehen möchten – inklusive der Verbindung zu Methoden wie STPA, die auch im Automotive-Kontext immer wichtiger werden.

Mehr Infos:

<https://www.iese.fraunhofer.de/seminar-automotive-cybersecurity>



Fazit: Ganzheitliche Absicherung als Lösung

Für die Automobilbranche entsteht so ein klarer Mehrwert: Das PAL stärkt die Safety von Fahrerassistenz- und Automatisierungssystemen, während das Lernlabor die notwendige Cyber-Resilienz von Cloud-Diensten und softwarebasierten Fahrzeugfunktionen sicherstellt. Zusammen entsteht so am Fraunhofer IESE ein integrierter Ansatz für vertrauenswürdige, sichere Mobilitätssysteme.

»Autonomik ist der nächste große Paradigmenwechsel«

Die Wissenschaft zu autonomen Systemen auf die nächste Stufe heben

Dazu im Interview: Prof. Dr.-Ing. habil. Peter Liggesmeyer, Institutsleiter des Fraunhofer IESE

Autonome Fahrzeuge, intelligente Stromnetze, automatisierte Zelltherapien – viele technologische Entwicklungen weisen in eine gemeinsame Richtung: Systeme sollen zunehmend selbstständig handeln. Prof. Liggesmeyer plädiert dafür, diese Entwicklung wissenschaftlich neu zu ordnen – unter dem Dach eines eigenen Wissenschaftsgebiets: der Autonomik.



Weitere Infos: <https://autonomik.de/>



»Jetzt ist der Zeitpunkt gekommen, das Wissenschaftsgebiet Autonomik zu gestalten.«

Herr Professor Liggesmeyer, was genau verstehen Sie unter Autonomik?

Autonomik fasst quer durch alle Anwendungsbereiche die Inhalte zusammen, die für die Autonomie von Systemen relevant sind. Ich beobachte überall eine Entwicklung hin zu hochautomatisierten bis hin zu vollständig über lange Zeiträume autonom handelnden Systemen. Selbstverständlich unterscheiden sich die Anforderungen an diese Systeme, aber es gibt eben auch gemeinsame Herausforderungen und vermutlich auch ähnliche Lösungen dafür. Man kann sich schon fragen, warum wir derzeit diese Lösungen pro Anwendungsgebiet suchen, anstatt die Ähnlichkeiten zu nutzen, um durch gemeinsame Antworten Synergien zu schaffen.

Ich sehe Autonomik als das Wissenschaftsgebiet, das diese gemeinsamen Herausforderungen für die Entwicklung und den Betrieb autonomer Systeme identifiziert und querschnittlich Lösungen dafür erforscht. Sie knüpft an existierende Disziplinen wie die Informatik – insbesondere die Künstliche Intelligenz –, den Maschinenbau und die Elektrotechnik an. Sie wirft wissenschaftliche Fragestellungen auf, besitzt ohne Zweifel ein hohes wirtschaftliches Potenzial und erfordert die Auseinandersetzung mit gesellschaftlichen Perspektiven.

Der Maschinenbau hat mechanisiert, die Elektrotechnik elektrifiziert, die Informatik digitalisiert – und die Autonomik wird Systeme selbstständig machen. Natürlich nicht zwingend vollständig, sondern entsprechend dem gewünschten Autonomisierungsgrad.

Viele setzen Autonomie mit KI gleich. Ist Autonomik einfach ein anderes Wort für Künstliche Intelligenz?

Nein. Autonome Systeme sind ohne KI kaum vorstellbar, benötigen aber weitere Technologien. KI ist ein wichtiges Werkzeug: sie kann ganz unterschiedliche Ziele verfolgen, nicht nur Autonomie. KI-Agenten zahlen auf das Thema Autonomik ein; ich sehe das als eine Realisierungsmöglichkeit für bestimmte Anwendungen. Autonomik ist meines Erachtens jedoch deutlich breiter aufgestellt.

Ein System ist erst dann wirklich autonom, wenn es über längere Zeiträume selbstständig auf unvorhergesehene Ereignisse reagieren kann. Andernfalls bleiben Einsatzdauer und -umgebung stark begrenzt. Autonomik soll das gesamte System über lange Zeiträume hinweg einschließlich seiner Verlässlichkeit betrachten.



Prof. Dr.-Ing. habil. Peter Liggesmeyer,

Institutsleiter des Fraunhofer IESE und
Leiter des Lehrstuhls Software Engineering:
Dependability, RPTU Kaiserslautern-Landau

Warum wird diese Fähigkeit gerade jetzt so wichtig?

Unverzichtbar sind autonome Systeme dort, wo Herausforderungen so kompliziert oder gar komplex sind oder Reaktionszeiten so kurz, dass der Mensch nicht mehr angemessen eingreifen kann. Darüber hinaus können autonome Lösungen beispielsweise in der Industrie 4.0 oder beim autonomen Fahren als Komfortfunktion erwünscht sein. Doch in vielen zentralen Bereichen werden wir nicht wirklich vorankommen, wenn wir nicht lernen, autonome Systeme verlässlich zu konstruieren und zu betreiben. Wie Verlässlichkeit garantiert werden kann, ist eine zentrale wissenschaftliche Fragestellung.

Sie sprechen von einem Paradigmenwechsel.

Was steht auf dem Spiel?

Derzeit vollzieht sich ein grundlegender Paradigmenwechsel durch autonome Systeme. Wenn wir ihn verschlafen, werden wir nicht nur in der zugrunde liegenden Technologie, sondern auch in ihren Anwendungsbereichen zurückfallen. Das hätte negative Konsequenzen für viele wichtige Branchen. Wenn wir jedoch schnell genug sind, kann die Autonomik einen erheblichen positiven wirtschaftlichen Effekt entfalten. Es geht um technologische Souveränität und Zukunftsfähigkeit.

Ein zentrales Beispiel ist die Energiewende. **Warum braucht sie Autonomik?**

Mit dem Ausbau erneuerbarer Energien steigt die Zahl der Einspeiser – von privaten Haushalten bis zu großen Anlagen. Gleichzeitig ist die Energieerzeugung durch Wind und Sonne volatil: Mal gibt es zu viel Strom, mal zu wenig. Um diese Schwankungen auszugleichen, müssen Anlagen koordiniert gesteuert, Speicher intelligent genutzt und Energie überregional verteilt werden. Das Gesamtsystem ist zu groß und zu komplex, als dass Menschen es vollständig überblicken könnten.

Damit die Energiewende gelingt, müssen hier autonome Lösungen entwickelt werden – und dafür braucht es intensive Forschung.

Eine andere prominente Anwendung ist das autonome Fahren. Ist die Lage dort vergleichbar?

Beim autonomen Fahren ist die gesellschaftliche Notwendigkeit weniger zwingend als bei der Energieversorgung – hier handelt es sich zunächst um ein »Nice-to-have«.

Aber industriepolitisch ist das Thema hochrelevant. Die deutsche Automobilindustrie war jahrzehntelang auf mechanische Perfektion ausgerichtet. Mit dem Software-Defined Vehicle hat die Informatik einen Paradigmenwechsel ausgelöst: Softwarefunktionen wurden zum entscheidenden Kaufargument.

Autonome Systeme markieren nun die nächste Stufe dieser Entwicklung. Wer hier technologisch führend ist, definiert zukünftige Märkte. Mutige Forschung in der Autonomik kann somit ein starker Innovationsmotor für die Branche sein.

Noch existenzieller erscheint der Einsatz in der Medizin. Wie ordnen Sie hier die Autonomik ein?

In der Krebsbehandlung bieten Zelltherapeutika wie die CAR-T-Zelltherapie hohe Heilungschancen. Sie sind jedoch aufgrund der aufwendigen manuellen Herstellung sehr teuer und nur begrenzt verfügbar. Eine automatisierte Produktion erfordert hochflexible Abläufe, die letztlich autonom realisiert werden müssen. Gelingt das, ließen sich die Kosten deutlich senken und die verfügbare Menge erheblich steigern. Das ist ein Beispiel dafür, wie autonome Systeme nicht nur wirtschaftliche Effekte erzeugen, sondern konkret Menschenleben verbessern oder sogar retten können.

Wie soll aus Ihrer Sicht die Autonomik wissenschaftlich verankert werden?

Wir müssen Autonomik systematisch als eigenständiges Wissenschaftsgebiet entwickeln. Der Begriff ist bewusst in Anlehnung an die Informatik geprägt. Es geht darum, ein theoretisches Fundament zu schaffen und klar zu definieren, welche Kompetenzen notwendig sind, um exzellente autonome Systeme zu entwickeln.

Ich sehe Autonomik als ein wichtiges Wissenschaftsgebiet. Ob sich daraus langfristig eine eigenständige Disziplin entwickelt, wird sich zeigen. Deutschland könnte sich hier als weltweiter Vorreiter positionieren.

Autonome Systeme beginnen gerade, unsere Welt massiv zu verändern. Meine Mitstreiter, unter anderem Prof. Wahlster und Prof. Kagermann, und ich spüren diese Morgendämmerung. Jetzt ist der Zeitpunkt gekommen, das Wissenschaftsgebiet Autonomik zu gestalten.

Software auf Rädern

Wie Software-Defined Vehicles den Wandel der Fahrzeugentwicklung prägen

Dazu im Interview: Dr. Pablo Oliveira Antonino, Department Head Virtual Engineering am Fraunhofer IESE

Software wird zunehmend zum zentralen Innovationstreiber in der Fahrzeugentwicklung. Mit dem Wandel hin zu Software-Defined Vehicles verändern sich Architektur, Entwicklungsprozesse und Validierung grundlegend. Digitale Zwillinge und Simulation spielen dabei eine Schlüsselrolle. Wie dieser Transformationsprozess konkret aussieht und welche Chancen sich daraus ergeben, erklärt Dr. Pablo Oliveira Antonino im Interview.

Warum spielt Software heute eine so zentrale Rolle in der Fahrzeugentwicklung?

Die Automobilindustrie befindet sich in einem grundlegenden Umbruch: Fahrzeuge entwickeln sich von elektromechanischen Produkten hin zu softwaregetriebenen Systemen. Das ist keine Vision mehr, sondern Realität. Ein großer europäischer Automobilhersteller hat kürzlich kommuniziert, dass künftig bis zu 40 Prozent der Wertschöpfung eines Fahrzeugs softwarebezogen sein werden. Software definiert heute Fahrverhalten, Sicherheit, Konnektivität und die Weiterentwicklung über Updates – sie spielt eine ganz zentrale Rolle.

Ist das Software-Defined Vehicle ein neues Konzept – und was zeichnet es konkret aus?

Das zugrunde liegende Prinzip existiert bereits seit mehr als zehn Jahren. Neu ist weniger die Idee als vielmehr die Konsequenz, mit der sie heute umgesetzt wird. Früher wurden sicherheitskritische Funktionen sehr konservativ und stark elektromechanisch umgesetzt. Heute laufen Steuerung und Logik über viele Controller und Rechner im Fahrzeug. Ein Kunde aus dem Nutzfahrzeugbereich hat das einmal treffend formuliert: »Wir waren ein Mechanical-Engineering-Unternehmen – und plötzlich sind wir ein Software-Unternehmen.«

Ein Software-Defined Vehicle ist ein Fahrzeug, dessen Funktionalität primär durch Software bestimmt wird. Die Hardware wird dabei zu einer standardisierten Plattform. Unsere Digitalen Zwillinge und Simulationen sind in diesem Kontext besonders relevant. Sie ermöglichen eine prädiktive Validierung komplexer Systeme und reduzieren Entwicklungs- und Integrationsrisiken erheblich. Ohne skalierbare virtuelle Tests wäre die Entwicklung moderner Software-Defined Vehicles wirtschaftlich kaum tragfähig.

Warum reichen reale Tests für moderne Fahrzeuge nicht mehr aus?

Die Komplexität ist schlicht zu hoch. Für autonome oder teilautonome Fahrzeuge gibt es Studien, die zeigen: Um alle relevanten Szenarien real zu testen, müsste ein Fahrzeug rechnerisch 88-mal die Strecke zwischen Erde und Sonne zurücklegen. Das ist offensichtlich unmöglich. Virtuelle Validierung ist daher alternativlos und eine zwingende Voraussetzung.

Welchen Mehrwert bietet der Fahrsimulator in der Validierung?

Der Fahrsimulator ist für uns ein wichtiges Entwicklungstool. Er integriert Digitale Zwillinge und Algorithmen in realistische Fahrszenarien. Wir können gezielt Störungen einbringen und beobachten, wie sich das Fahrzeug verhält – nicht nur im Code, sondern für den Fahrer spürbar. Dieses Konzept wird als »Driver in the Loop« bezeichnet. So werden komplexe Wechselwirkungen verständlich und greifbar.

Was macht FERAL zum Schlüsselwerkzeug?

Fraunhofer FERAL ist ein modulares Simulations- und Co-Simulations-Framework, das am Fraunhofer IESE entwickelt wurde. Es ermöglicht die Erstellung Digitaler Zwillinge eingebetteter Assets und integriert Softwarefunktionen, Netzmodelle sowie E/E-Plattformen in einer gemeinsamen Co-Simulationsumgebung. Ein zentrales Merkmal ist die gezielte Fehlerinjektion, die eine frühzeitige Fehlererkennung und systematische Absicherung erlaubt. Dadurch werden physische Prototypen reduziert, Validierungszyklen verkürzt und die Time-to-Market von Fahrzeugen deutlich beschleunigt.

Weitere Infos: <https://www.iese.fraunhofer.de/de/abteilung/virtual-engineering.html>



Warum ist dieser Ansatz bei Nutzfahrzeugen besonders relevant?

Nutzfahrzeuge operieren häufig in sehr speziellen und unvorhersehbaren Einsatzumgebungen – etwa in der Landwirtschaft, im Mining oder auf Baustellen. Ausfallzeiten bedeuten hier sofort wirtschaftlichen Schaden. Viele dieser Fahrzeuge sind im Prinzip »Factories on Wheels«. Wenn ein System ausfällt, steht im schlimmsten Fall eine komplette Wertschöpfungskette still. Genau hier zeigt sich der besondere Mehrwert softwaregetriebener Fahrzeugarchitekturen.

»Ohne skalierbare virtuelle Tests mit Tools wie FERAL wäre die Entwicklung moderner Software-Defined Vehicles wirtschaftlich kaum tragfähig.«



*Fahrsimulator im Einsatz:
Digitale Zwillinge und Softwarefunktionen
werden getestet und für die Fahrzeug-
entwicklung erlebbar gemacht.*

Gibt es konkrete Praxisbeispiele aus der Wirtschaft?

Ein erfolgreiches Projekt ist unsere Zusammenarbeit mit dem südkoreanischen Unternehmen Perseus Co., Ltd. Wir arbeiten gemeinsam an Lösungen für Software-Defined Vehicle, insbesondere an der virtuellen Absicherung von Hypervisor-Technologien. Ein Hypervisor koordiniert mehrere Betriebssysteme auf einer gemeinsamen Hardwareplattform. Wir bauen mit FERAL Digitale Zwillinge auf, um komplette Systemarchitekturen inklusive Software, Hardware und Kommunikation frühzeitig zu validieren. So lassen sich Leistungsfähigkeit, Robustheit und Ressourcenkonflikte bereits in einer virtuellen Umgebung analysieren.

Eine weitere langfristige Partnerschaft besteht mit dem amerikanischen Unternehmen Balanced Engineering LLC. Als Business Partner bündeln wir unsere Kompetenzen im Bereich Virtual Engineering und tragen sie gemeinsam in internationale Märkte. Beispielsweise haben wir ein Projekt zur virtuellen Validierung autonomer Fahrzeuge in der Landwirtschaft umgesetzt. Dazu wurde eine Simulationsumgebung geschaffen, die realistische landwirtschaftliche Szenarien – etwa unterschiedliche Wetterlagen und Hindernisse – nachbildet. Das reduziert teure Feldtests und steigert die Effizienz autonomer Agrarsysteme.

Auch mit John Deere GmbH & Co. KG haben wir im Bereich digitaler Agrartechnologien erfolgreich zusammengearbeitet. Dabei konnte eine KI-Anwendung flexibel und zuverlässig auf einer modernen Testinfrastruktur installiert und evaluiert werden – ein bedeutender Meilenstein für die Weiterentwicklung datengetriebener Agrarsysteme. Die Kooperation zeigt, wie virtuelle Validierung konkrete Innovationsschritte in der Landwirtschaft ermöglicht.

Was bedeutet all das für die Zukunft des autonomen Fahrens?

Wenn Digitale Zwillinge und Simulation konsequent eingesetzt werden, entstehen Fahrzeuge, die sicherer, kostengünstiger, schneller reparierbar und funktional flexibler sind. Autonomes Fahren wird dadurch realistisch und beherrschbar – auch wenn Regulierung und gesellschaftliche Akzeptanz natürlich ebenfalls eine Rolle spielen.



Dr. Pablo Oliveira Antonino
Department Head Virtual Engineering

Virtuelle Absicherung für das Software-Defined Vehicle

Fraunhofer IESE und Perseus Co., Ltd. bündeln ihre Kompetenzen für die Mobilität von morgen

In einem gemeinsamen strategischen Forschungs- und Entwicklungsprojekt im Bereich Software-Defined Vehicle arbeiten das Fraunhofer IESE und das südkoreanische Technologieunternehmen Perseus Co., Ltd. eng zusammen. Ziel der Kooperation ist es, innovative Virtualisierungs- und Simulationstechnologien zusammenzuführen und so neue Maßstäbe für die Entwicklung und Absicherung komplexer Fahrzeugsoftware zu setzen.

Software-Defined Vehicles (SDV) stehen für einen Paradigmenwechsel in der Automobilindustrie: Funktionen werden zunehmend softwarezentriert entwickelt und flexibel aktualisiert. Gleichzeitig steigen die Anforderungen an Sicherheit, Performance und Nachweisbarkeit – insbesondere, wenn sicherheitskritische und nicht-sicherheitskritische Anwendungen gemeinsam auf leistungsfähigen zentralen Steuergeräten betrieben werden. Genau hier setzt die Zusammenarbeit an.

Technologien intelligent verknüpft

Im Mittelpunkt steht die Integration des Virtual-Engineering-Frameworks FERAL des Fraunhofer IESE mit dem Hypervisor PEGASUS von Perseus. Durch diese Kombination entsteht eine leistungsfähige virtuelle Entwicklungs- und Testumgebung für moderne Fahrzeugarchitekturen.

Die gemeinsame Lösung ermöglicht es, gemischte Laufzeitumgebungen realitätsnah zu simulieren und systematisch zu analysieren. Digitale Zwillinge und virtuelle Prüfstände schaffen die Voraussetzung – noch bevor physische Prototypen verfügbar sind. Über Co-Simulationen lassen sich Software-, Hardware- und Umgebungsmodelle koppeln, sodass Ende-zu-Ende-Tests unter praxisnahen Bedingungen durchgeführt werden können.

Neben funktionalen Tests stehen dabei auch Leistungskennzahlen wie Latenz, Ressourcenverteilung, Robustheit und Fehlerausbreitung im Fokus. So gewinnen Hersteller frühzeitig Transparenz über das Verhalten komplexer Systemarchitekturen.

Effizienzgewinne entlang des gesamten Entwicklungsprozesses

Die enge technologische Verzahnung unterstützt moderne Continuous-Engineering-Ansätze und ermöglicht häufige,

automatisierte Tests bereits in frühen Entwicklungsphasen. Das reduziert Iterationsschleifen, verkürzt Entwicklungszyklen und minimiert den Bedarf an kostenintensiven physischen Testaufbauten.

Darüber hinaus trägt die virtuelle Absicherung dazu bei, Zertifizierungsprozesse für sicherheitskritische Systeme deutlich zu beschleunigen – von bislang 18 Monaten auf bis zu sechs Monate. Durch strukturierte, reproduzierbare Testszenarien und belastbare Nachweise können Entwicklungs- und Zulassungszeiten signifikant reduziert werden.

Internationale Partnerschaft für die Mobilität von morgen

Die Zusammenarbeit verbindet die methodische und technologische Expertise des Fraunhofer IESE im Bereich Virtual Engineering und Systemvalidierung mit der Hypervisor-Technologie von Perseus für moderne SDV-Architekturen.

Gemeinsam schaffen die Partner eine skalierbare Grundlage für sichere, flexible und zukunftsfähige Fahrzeugplattformen. Die Kooperation zeigt, wie internationale Industrie- und Forschungsakteure ihre Stärken bündeln können, um den Wandel hin zu softwarezentrierten Fahrzeugarchitekturen aktiv zu gestalten – effizient, innovationsorientiert und mit klarem Fokus auf Qualität und Sicherheit.

»Mit der Virtualisierungs- und Verifizierungskompetenz von Fraunhofer IESE wird Perseus die Zukunftssicherheit unserer Technologien unter Beweis stellen. Unser Hypervisor ermöglicht die sichere Ausführung kritischer und nicht-kritischer Anwendungen auf gemeinsamer Hardware – eine Schlüsseltechnologie im SDV-Zeitalter.«



Dr. Sang-bum Suh, CEO von Perseus

Unsicherheit messbar machen

UncertAlnty – ein WIPANO-Projekt für verlässliche KI-Systeme

UncertAlnty (Uncertainty Quantification in AI-Systems for International Compliance) ist ein vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) gefördertes WIPANO-Projekt, das den systematischen Umgang mit Unsicherheit in KI-Systemen voranbringt. Über eine Laufzeit von 30 Monaten arbeiten Partner aus Wirtschaft, Forschung und Normung gemeinsam daran, Unsicherheiten in KI eindeutig zu beschreiben, messbar zu machen und international zu standardisieren.

Künstliche Intelligenz eröffnet neue Möglichkeiten für Fahrzeuge, Maschinen und Anlagen – insbesondere in sicherheitsrelevanten Anwendungen. Gleichzeitig lassen sich bei datengetriebenen, lernenden Systemen einzelne Ergebnisse prinzipbedingt nicht garantieren. Für einen sicheren und rechtskonformen Einsatz wird es daher entscheidend, Leistungsgrenzen transparent zu machen und Unsicherheit nachvollziehbar zu quantifizieren. Genau hier setzt UncertAlnty an.

Von der DIN SPEC zum internationalen Standard

Im Mittelpunkt des Projekts steht die Entwicklung der internationalen technischen Spezifikation ISO/IEC TS 25223 »Guidance and requirements for uncertainty quantification in AI systems«. Aufbauend auf der nationalen DIN SPEC 92005 wird der bisherige Fokus vom Maschinellen Lernen auf KI-Systeme insgesamt erweitert – einschließlich hybrider und generativer KI-Ansätze. Ziel ist es, eine einheitliche Terminologie sowie technische Leitlinien und Anforderungen zur Unsicherheitsquantifizierung zu definieren, die alle Phasen des KI-Systemlebenszyklus abdecken.

Damit leistet UncertAlnty einen zentralen Beitrag zur internationalen Normung und schafft eine Grundlage für branchenübergreifende Standards. Die Ergebnisse fließen in relevante internationale Gremien ein und bilden eine wichtige Referenz für weitere Normen im Umfeld von KI, funktionaler Sicherheit und Systems Engineering.

Rechtssicherheit für Hochrisiko-KI

Ein wesentlicher Treiber des Projekts ist der steigende Bedarf an Rechtssicherheit beim Einsatz von KI, insbesondere vor dem Hintergrund der europäischen KI-Verordnung (AI Act). Deren Anforderungen lassen Interpretationsspielräume, die durch harmonisierte Normen konkretisiert werden müssen. Für Unternehmen, Prüforganisationen und Behörden wird die Quantifizierung von Unsicherheit damit zu einem Schlüsselthema.

Gerade bei sicherheitsrelevanten eingebetteten KI-Systemen stoßen klassische Sicherheitsnormen an ihre Grenzen, da sie KI-Komponenten häufig nicht auf dem sicherheitskritischen Pfad vorsehen. UncertAlnty adressiert diese Lücke und unterstützt die Entwicklung von Normen, mit denen KI-basierte Funktionen sicher eingesetzt werden können, ohne ihre Potenziale unnötig einzuschränken.

Fraunhofer IESE im Projekt UncertAlnty

Verlässliche KI ist ein zentrales Fokusthema am Fraunhofer IESE, unter anderem mit einer zertifizierten Weiterbildung. Das Institut verfügt über langjährige Expertise in der Quantifizierung und im Management von KI-Unsicherheit aus zahlreichen Forschungs- und Industrieprojekten und hat mit seinen Vorarbeiten maßgeblich zur Entwicklung der DIN SPEC 92005 beigetragen, bei der es zudem den stellvertretenden Obmann stellte. Diese Erfahrung fließt in UncertAlnty ein und unterstützt die Weiterentwicklung international anschlussfähiger Standards.

Beitrag zu vertrauenswürdiger KI

Mit UncertAlnty werden zentrale Grundlagen für die vertrauenswürdige Nutzung von KI geschaffen. Das Projekt stärkt die internationale Anschlussfähigkeit deutscher Normungsaktivitäten und unterstützt Unternehmen dabei, KI-Systeme sicher, nachvollziehbar und konform zu entwickeln. Damit leistet UncertAlnty einen wichtigen Beitrag zur Wettbewerbsfähigkeit und zur sicheren Einführung KI-basierter Technologien in sicherheitskritischen Anwendungsfeldern.



Weitere Infos: <https://www.iese.fraunhofer.de/de/referenz/uncert-ainty.html>

3 Fragen an ...

... Michael Höh, Solution Architect Guidance & Automation, European Technology Innovation Center Kaiserslautern, John Deere GmbH & Co. KG



Wie viel Effizienzgewinn bringt KI wirklich in die Softwareentwicklung – und wo bleibt menschliche Expertise unverzichtbar? Dieser Frage ging John Deere gemeinsam mit Studierenden der RPTU Kaiserslautern und dem Fraunhofer IESE im Capstone-Projekt nach. Unter dem Motto »Alles ist erlaubt« und »so viel KI wie möglich« entstand nicht nur eine leichtgewichtige Simulation für automatisiert fahrende Traktoren, sondern auch ein klarer Blick auf Chancen und Grenzen KI-gestützter Entwicklung. Welche Erkenntnisse besonders überraschten, erzählt Michael Höh im Interview.

1 Welche strategische Rolle spielt Künstliche Intelligenz heute in der Entwicklungsarbeit von John Deere? Wo stehen Sie aktuell – und welche weiteren Ziele streben Sie mit dem Einsatz von KI an?

Ich würde die Frage lieber aus meiner Sicht hier am Standort Kaiserslautern beantworten, da bei diesem Thema aktuell enorm viel passiert und wir alle ständig neue Möglichkeiten kennenlernen. Und diese Möglichkeiten wollen wir natürlich ausnutzen, dabei aber auch Rahmenbedingungen einhalten. Gerade in der Softwareentwicklung stehen uns die wichtigen Modelle zur Verfügung und wir müssen nicht unbedingt »Token« zählen. Jede KI-Anfrage resultiert in einer bestimmten Anzahl von Token und diese erzeugen auch Kosten. D.h. der Einsatz der KI ist nicht umsonst. Aus meiner aktuellen Sicht lohnt er sich aber.

Ich würde sagen, wir sind zurzeit in einer Entdeckungs- und Ausprobierphase: von großer Begeisterung, aber auch manchmal genervter Enttäuschung. Ich glaube, wenn wir das Werkzeug KI soweit verstanden haben, können wir den Entwicklungsprozess verschlanken und schneller Innovationen für unsere Kunden anbieten.

Ich vergleiche die Softwareentwicklung gerne mit der Leber beim Menschen: Sie macht alles mit und wächst dabei – bis ein bestimmter Punkt erreicht ist. Und wenn man dann reagieren muss, ist es schwierig. Vielleicht beginnt man sogar ein neues Projekt. In der Regel kann man nicht auf bestimmte Teile verzichten und muss diese ausschneiden und einsetzen.

Das ist oft viel manuelle Arbeit und Anpassungen im Code und den Unit Tests. Hier kann die KI sehr gut unterstützen. Wir testen das mit zum Teil großen Code-Bereichen und schauen uns die Ergebnisse an. Diese sind vielversprechend, insbesondere mit Blick auf die Umsetzungszeit.

Betrachtet man den gesamten Entwicklungszyklus: In welchen Phasen generiert KI aus Ihrer Sicht den größten Mehrwert? Wo zeigen sich bereits messbare Effizienz- oder Qualitätsgewinne?

Als jemand, der die Softwareentwicklung seit vielen Jahren begleitet, sehe ich natürlich vor allem diesen Bereich. Und es ist beeindruckend, einem KI-Agenten dabei zuzuschauen, wie schnell und systematisch Code durchsucht, analysiert oder erstellt wird. Die damit erzielten Gewinne sind nicht nur messbar, sondern auch regelmäßig an der Kaffeemaschine beim Gespräch mit Kollegen hörbar. Ein aus meiner Sicht nicht zu unterschätzender Mehrwert ist die Öffnung der Softwareentwicklung für Leute ohne oder mit wenig Programmiererfahrung (Vibe-Coding). Zum Beispiel der Systemingenieur, der eine Idee hat und diese direkt prototypisch umsetzen kann, um schnelles Feedback zu bekommen. Zeitlich unschlagbar zum klassischen Beschreiben der Idee, der Beauftragung, den Iterationen usw.

Ich glaube, auch mit der KI als Copilot erlebt das Pair-Programming eine Renaissance. Ich habe mir immer schwergetan, das außerhalb spezieller Gründe wie Fehlerfindung oder bestimmter Designentscheidungen zu leben. Mit der KI ist das anders und ich finde es zum einen sehr angenehm, aber auch enorm hilfreich und wahrscheinlich effizienter als ein menschlicher Kollege.

Ein weiteres Beispiel ist ein Klassiker: Code-Dokumentation! Separate Dokumente laufen immer Gefahr, nicht den letzten Code-Änderungen zu entsprechen. Damit wird ihr Wert relativiert und man müht sich dann letztendlich doch durch den Code. Und beim Code kann man über Kommentare diskutieren: Braucht man Kommentare oder ist der Code selbsterklärend? Und wenn Kommentare oder Dateibesreibungen, sind diese aktuell und entsprechend mitgepflegt? Ich glaube, durch die KI wird der Klassiker früher oder später verschwinden, da jegliche Dokumentation »on demand« erzeugt werden kann und diese immer dem aktuellen Code-Stand entspricht. Das stellt einiges auf den Kopf.

Im Rahmen unseres gemeinsamen Capstone-Projekts haben Studierende KI intensiv eingesetzt. Welche ihrer Ergebnisse haben Sie besonders beeindruckt oder sogar überrascht – und welche Erkenntnisse fließen in Ihre Entwicklungsarbeit ein?

Mich hat besonders der verbale Austausch mit einem KI-Agenten beeindruckt, um Anforderungen zu ermitteln. Zum einen, weil das Gespräch sehr natürlich war, aber auch wissend, wie schwierig es ist, gute Anforderungen zu ermitteln. Ich glaube, generell hat die KI auch geholfen, die Kreativität der Studierenden schnell im Kontext umzusetzen. Die meisten hatten wenig oder keinen landwirtschaftlichen Hintergrund. Diese Lücke war kaum spürbar bzw. wurde sehr schnell geschlossen.

Überrascht war ich über die Menge und Bandbreite an bearbeiteten Themen in sehr kurzer Zeit. Die Studierenden haben auch sehr gut den Spagat hinbekommen, die KI-Möglichkeiten zu entdecken, zu erforschen und praktisch am Projekt »Simulator von landwirtschaftlichen Maschinen mit KI« auszuprobieren. Bei jedem Iterations-Meeting konnte etwas gezeigt werden, was mir als »Kunde« auch sehr geholfen hat.

Ich glaube, durch das Capstone-Projekt fließen viele Erkenntnisse in die Entwicklungsarbeit ein, auch außerhalb der eigentlichen Softwareentwicklung. Wir arbeiten bei John Deere an kamera-basierten Automatisierungen, zum Beispiel beim automatisierten Befüllen eines Anhängers mit Erntegut. Hier müssen wir uns neben der Softwareentwicklung, die mit der schnellen Technologie-Entwicklung Schritt halten muss, mit unterschiedlichen Disziplinen wie Bildverarbeitung, Steuer- und Regelungstechnik sowie Datenmanagement beschäftigen. Und das Gesamtsystem funktioniert natürlich besonders gut, wenn alles passt und aufeinander abgestimmt ist. Hier hilft die KI nicht nur den erfahrenen Mitarbeitern, sondern insbesondere neuen Mitarbeitern. Ähnlich wie den Studierenden im Capstone-Projekt, für die erst einmal vieles oder sogar alles neu war. Wir haben in Capstone zum Teil bewusst keine internen Informationen oder Experten bereitgestellt, um zu verstehen, was möglich ist. So haben die Studierenden die Anbindung an unser John Deere Operations Center komplett eigenständig mit der KI und verfügbaren Online-dokumentationen realisiert. Oft wird eine Schnittstellen-API nur erklärt, aber mit der KI bekommt man sofort etwas, das man ausprobieren und starten kann. Das hat in sehr kurzer Zeit sehr gut geklappt und ist sicherlich eine große Unterstützung für neue Mitarbeitende oder welche, die die Domäne wechseln. Ein Ergebnis, dass sich KI weniger gut für die Erstellung von zum Beispiel Architekturdiagrammen eignet, ist mittlerweile wohl schon wieder überholt. Aber das passt zur hohen Dynamik im Bereich Künstliche Intelligenz, mit der man Schritt halten muss... und vielleicht ein nächstes Capstone-Projekt triggert.





Impressum

Redaktion & Interviews

Claudia Reis, Dipl.-Kauffrau (verantw.)

Fabienne Bäcker, M.A.

Layout & Satz

Bettina Wassermann, Diplom-Industriedesignerin (FH)

Druck

FLYERALARM GmbH, Würzburg

Ihr Ansprechpartner für Automotive

Ralf Kalmar

Head of Business Development

Tel. +49 631 6800-1603

ralf.kalmar@iese.fraunhofer.de

Ihre Ansprechpartnerin für PR und Marketing

Claudia Reis

Team Leader

Corporate Communications &
Technology Marketing

Tel. +49 631 6800-0

presse@iese.fraunhofer.de

www.iese.fraunhofer.de

Bildquellen

Cover, S. 2, 7, 15, 21: Fraunhofer IESE/Bettina Wassermann | S. 4-5: GettyImages/RistoArnaudov, Viaframe; Unsplash/ClintPatterson; Fraunhofer IESE | S. 9: GettyImages/anilyanik | S. 12-13, S. 26: Fraunhofer IESE | S. 17: Getty Images/Viaframe, MirageC, Marga Buschbell-Steeger; Fraunhofer IESE | S. 19: GettyImages/ Just_Super, Fraunhofer IESE | S. 24: John Deere

© 2026 Fraunhofer IESE

Verlässliche digitale Systeme – Fraunhofer IESE.

Kontakt

Fraunhofer IESE
Fraunhofer-Platz 1
67663 Kaiserslautern

Tel. +49 631 6800-0
info@iese.fraunhofer.de
www.iese.fraunhofer.de

#STAYCONNECTED

