Die SARS COVID 19 Pandemie hat große Auswirkungen auf unser aller Arbeitsleben. Homeoffice, Kurzarbeit, Verschiebungen, Umgestaltungen oder gar Aufgabe von Projekten sind nur einige der Folgen, mit denen wir alle lernen mussten zu leben. Auch SafeTRANS ist von diesen Veränderungen betroffen. Physische Treffen sind kaum noch möglich, die Arbeit in den Arbeitskreisen und Projekten, aber auch das Netzwerken und der Wissenstransfer, z. B. durch SafeTRANS Industrial Days, sind erschwert oder gar unmöglich.
Dennoch: „Die Welt dreht sich weiter“ und die großen Umbrüche, die sich in den letzten Jahren und Monaten im Technologiefeld eingebettete und cyber-physisches Systeme abzeichneten, realisieren sich zunehmend. SafeTRANS ist aktiv an der Gestaltung dieser Umbrüche beteiligt (siehe Übersichtsartikel ab Seite 8). Die als Draft-Dokument veröffentlichte Roadmap zu Safety, Security, and Certifiability of Future Man-Machine Systems zeichnet ein umfassendes Bild der zukünftigen Herausforderungen für die Entwicklung, Validierung und Zertifizierung von hochvernetzten, „intelligenten“, autonomen, mit Menschen interagierenden und kooperierenden CPS (siehe Artikel zu diesem Fokusthema ab Seite 12 sowie das Interview mit Götz Anspach von Broecker ab Seite 16). Die Roadmap dient auch als Input für die Neuauflage der ECSEL SRIA, die wiederum die Grundlage für die zukünftigen „Calls for project proposals“ der ECSEL Joint Undertaking und ihrer Nachfolge im nächsten Rahmenprogramm sein wird (siehe Artikel Seite 11). Der Aufbau und die Vernetzung von Project Advisory Boards in mittlerweile zwei öffentlich geförderten Projekten (siehe Artikel Seite 22 und 23) bilden einen weiteren Schwerpunkt unserer aktuellen Aktivitäten.

Ich wünsche Ihnen ein informatives Lesen dieses Magazins. Bleiben Sie gesund und treten Sie gerne mit uns in Kontakt!

Jürgen Niehaus | Geschäftsführer SafeTRANS

SafeTRANS
SAFETY IN TRANSPORTATION SYSTEMS

NEWS

SafeTRANS News 1/2020

Umbrüche gestalten!

© krass99/Adobe Stock

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:
Airbus SE, BTC Embedded Systems, DLR, ECS SRIA, OFFIS, SafeTRANS, Springer-Verlag GmbH, TÜV NORD Mobilität - IFM,
Seite 12: tawanlubfah/Adobe Stock (ehemals fotolia), Titelseite: krass99/Adobe Stock

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

Ausgabe:
SafeTRANS News 1/2020 werden im Juli 2020 veröffentlicht und kostenlos abgegeben.

Die Rechte für alle Beiträge in den SafeTRANS News, auch Übersetzungen, sind dem Herausgeber vorbehalten.
Reproduktionen, gleich welcher Art, ob Fotokopie, Mikrofilm oder Erfassung in Datenverarbeitungsanlagen,
sind nur mit schriftlicher Genehmigung des Herausgebers und vollständiger Quellenangabe erlaubt.
Bei der Weiterleitung zu Inhalten von Dritten übernimmt SafeTRANS für diese Inhalte keine Verantwortung.

SafeTRANS News 1/2020

Aktuelle Meldungen 4
Auf den Punkt gebracht und relevant.

SafeTRANS fit für die Zukunft: Ausrichtung, Themen und Umsetzung 8
Eine Analyse des Themenfeldes CPS und die Positionierung von SafeTRANS.

ECS SRIA 2021: *Embedded Software* und *Complex Systems* verankert 11
Die neue ECS SRIA 2021 wird in diesem Jahr veröffentlicht.

Fokus:
Safety, Security, and Certifiability of Future Man-Machine Systems 12
SafeTRANS veröffentlicht hochaktuelle Roadmap zu vernetzten, komplexen CPS mit einer Klassifizierung der Komplexitätsabschätzung.

Interview zum Fokusthema:
„Ein Bewusstsein schaffen, wie verschiedene Branchen auf derselben Basis aufsetzen und Synergien entstehen können.“ 16
Götz Anspach von Broecker, AIRBUS, im Interview.

Neues DLR-Forschungsinstitut für „Systems Engineering für zukünftige Mobilität“ 21
Das neue Institut wird in Oldenburg entstehen und aus dem OFFIS-Bereich Verkehr aufgebaut.

Forschungsprojekt national: Step-UP!CPS 22

Forschungsprojekt europäisch: ArchitectECA2030 23

Resümee: ACPS Days 2019, Berlin 24
Die SafeTRANS Autonomous Cyber-Physical Systems Days boten eine einmalige Plattform für den Expertenaustausch.

SafeTRANS Mitglieder: TÜV NORD Mobilität - IFM 26

Aktuelle Meldungen

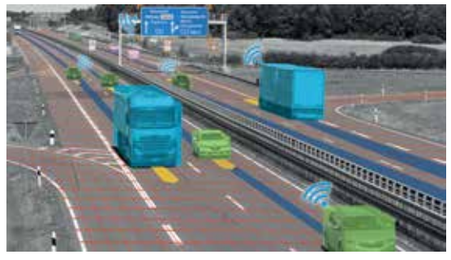
Neues aus dem Forschungs- und Wirtschaftsumfeld

embeteco: Das Strategieberatungs- und Entwicklungsunternehmen ist neues SafeTRANS-Mitglied

Seit 2020 ist die embeteco GmbH & Co. KG neues Mitglied im Verein SafeTRANS. embeteco begleitet Unternehmen und Regionen als strategischer Partner bei der digitalen Transformation, setzt digitale Innovationen um, unterstützt bei der Strategieentwicklung, beim Aufbau eines Innovationsmanagements und hilft bei der Akquise und Durchführung von Förderprojekten.
Im Schwerpunkt Cyber-physische Systeme konzipiert, entwickelt und implementiert embeteco skalierbare Softwarelösungen und beschreitet neue Wege in eigenen Smart-City-Forschungsprojekten. Dazu verfügt embeteco über eine umfassende methodische und technologische Expertise im Bereich der nutzerzentrierten Produktentwicklung und im Platform Engineering.
Für embeteco ist die Mitgliedschaft eine Stärkung der Vernetzung mit relevanten Akteuren in den Bereichen sicherheitskritische und autonome Systeme. Die Mitarbeit bei SafeTRANS schafft Synergien zwischen Industrieforschung, Wissenschaft und Forschungsvorhaben sowie die Möglichkeit zum Transfer der Ergebnisse in den Mittelstand.
www.embeteco.com

Testfeld Niedersachsen offiziell eröffnet

Den Verkehr der Zukunft auf die Straße zu bringen – das ist der Anspruch des Testfelds Niedersachsen. Nach Abschluss der letzten Aufbauarbeiten in den vergangenen Monaten können nun automatisierte und vernetzte Fahrzeuge getestet, Fahrverhalten und Verkehrsfluss erfasst und analysiert werden. Am 8. Januar 2020 wurde das Testfeld offiziell vom Deutschen Zentrum für Luft- und Raumfahrt (DLR) mit Gästen aus Politik und Wirtschaft eröffnet.
Mit einem Knopfdruck starteten Prof. Karsten Lemmer, DLR-Vorstand für Energie und Verkehr, Dr. Bernd Althusmann, Niedersächsischer Minister für Wirtschaft, Arbeit, Verkehr und Digitalisierung, Björn Thümler, Niedersachsens Minister für Wissenschaft und Kultur sowie Thomas Jarzombek, MdB und Koordinator der Bundesregierung für die deutsche Luft- und Raumfahrt, eine erste Übertragung der Erfassungstechnik auf der Autobahn 39 bei Braunschweig. Anschließend konnten sie sich in Forschungsfahrzeugen selbst ein Bild von der Strecke und den Nutzungsmöglichkeiten des Testfelds machen.
Prof. Lemmer betonte bei der Eröffnung: „Das Testfeld Niedersachsen ist wichtig, damit wir die Vorteile, die uns die Technologie des automatisierten und vernetzten Fahrens bietet, in der Praxis nutzbar machen können. Mit den gewonnenen Forschungserkenntnissen schafft das DLR bessere Entscheidungsgrundlagen für die Transformation unserer Mobilität – hin zu einem optimierten Verkehrsfluss und weniger Ressourcenverbrauch."



Darstellung der Prozessierung (Quelle: DLR)

Auch Thomas Jarzombek freute sich, dass das Testfeld Niedersachsen nun seinen Betrieb aufnehmen kann, und sagte: „Unternehmen, die Wissenschaft und Start-Ups benötigen Räume, in denen sie innovative Technologien und Lösungsansätze erproben und weiterentwickeln können. Mit dem Testfeld Niedersachsen schaffen wir eine national und international herausragende Infrastruktur zur Erforschung und Entwicklung intelligenter Mobilitätslösungen. Das Ziel ist es, dass die Mobilität der Zukunft hier in Deutschland entwickelt und auch auf die Straße gebracht wird."
Das Testfeld Niedersachsen wird Stück für Stück in Betrieb genommen. An der A39 sind jetzt 71 Masten errichtet. Sie können die Verkehrsteilnehmer und alle anderen Objekte im Verkehrsraum anonymisiert erfassen. So erlangen die Wissenschaftler beispielsweise Aufschluss darüber, was zukünftige Assistenz- und Automationssysteme leisten müssen. Dafür können die Masten untereinander sowie mit den entsprechend technisch ausgerüsteten Fahrzeugen kommunizieren.
Zusätzlich zu den fest verbauten gibt es mobile Masten, die Tests auch abseits der Autobahn ermöglichen. Dadurch ist die Analyse und Unterstützung automatisierter Fahrmanöver an unterschiedlichen Orten und auf verschiedenen Straßentypen möglich.
Einen weiteren wichtigen Bestandteil des Testfelds Niedersachsen – neben den Straßen und Autobahnen – bilden die hochgenaue Karte und die Simulation der gesamten Strecke. Hier kann vorab bereits getestet werden, was später auf der Straße zur Realität wird. Dieses Zusammenspiel unterschiedlicher Entwicklungs- und Testmethoden beziehungsweise -werkzeuge macht das Testfeld Niedersachsen einzigartig.
Das Testfeld ist eine offene Forschungs- und Entwicklungsplattform. Es bietet Raum für den wissenschaftlichen Dialog und soll gemeinsam mit seinen Nutzern dazu beitragen, die automatisierte und vernetzte Mobilität der Zukunft zu gestalten.
Die Wissenschaftler des DLR-Instituts für Verkehrssystemtechnik werden die auf dem Testfeld erhobenen Daten nutzen, um spezielle verkehrliche Situationen wie Stauenden, Einfädelsituationen und Überholmanöver genauer unter die Lupe zu nehmen. Daraus lassen sich Funktionen für automatisierte und vernetzte Fahrzeuge entwickeln oder verbessern. Außerdem werden Methoden und Konzepte für die Zulassung von automatisierten Fahrzeugen in Deutschland weiterentwickelt und auf der Straße praktisch erprobt. An oberster Stelle steht dabei immer das Ziel, den motorisierten Verkehr sicherer und effizienter zu machen, den Komfort für den Fahrer zu erhöhen und Emissionen zu verringern.
www.dlr.de

Hohes Engagement durch SafeTRANS in Advisory Boards

Bisher hat SafeTRANS als Verein, der Knowhow vorwettbewerblicher akademischer Forschung und Industrie für sicherheitskritische Embedded/Cyber-physical Systems bündelt, u. a. Forschungsagenden (mit-) gestaltet und hochkarätige FuE-Projekte initiiert. Nun übernimmt SafeTRANS Aufgaben bei der Begleitung europäischer und nationaler Forschungsprojekte als Moderator und Partner in sogenannten Advisory Boards.
Ein Advisory Board vertritt die nicht direkt im Projekt eingebundene Institutionen, die aber zum weiteren Stakeholder-Kreis gehören. Dies können große und kleine Unternehmen aus allen Teilen der Zulieferkette (OEMs, Zulieferer, Tool-Hersteller, Consulting), Forschungsinstitute, Standardisierungsgremien und/oder Zertifizierungsbehörden sein, die mit ihrem Knowhow die Partner in den Projekten unterstützen, allerdings selbst keine Projektpartner sind.
Ziele und Vorteile der Advisory Boards:

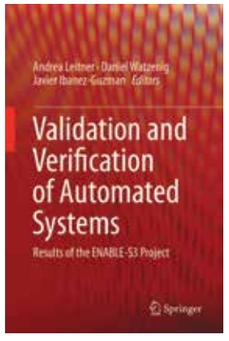
- schnelle und direkte Rückmeldung von industriellen Experten an die Projektpartner, z. B. hinsichtlich Anpassungen, Überprüfung von Ergebnissen
- Wissen über aktuelle Grundlagenforschung für die Industrievertreter
- Austausch auch hinsichtlich anderer relevanter FuE-Projekte (Vermeidung von Dopplungen)
- Verbesserung der Nachhaltigkeit der Projektergebnisse durch höhere industrielle Verwertbarkeit und Standardisierungsaktivitäten
- Koordinierter Wissenstransfer zwischen Forschung und Industrie auf nationaler und europäischer Ebene
- Zusammenfassung und Kommunikation der (FuE-) Ergebnisse

Aktuell verantwortet SafeTRANS das Advisory Board im nationalen Projekt Step!UP CPS (mehr zum Projekt Seite 22), in dem folgende Unternehmen mitarbeiten:
AVL LIST GmbH, BTC Embedded Systems AG, Denso Automotive Deutschland GmbH, DNV-GL Maritime Class Development, IAV GmbH Ingenieurgesellschaft Auto und Verkehr, NXP Semiconductor Germany GmbH, Vector Informatik GmbH
Darüber hinaus wird SafeTRANS im europäischen Projekt ArchitectECA2030 (Koordinator: Infineon Technologies AG), im Juli 2020 startete, alle Aktivitäten des Advisory Boards steuern (mehr zum Projekt Seite 23). Weitere Mandate zur Initiierung/Koordinierung von sowie die Mitarbeit in Advisory Boards werden folgen.
Haben Sie Interesse an Aktivitäten rund FuE-Wissenstransfer, dann sprechen Sie uns gerne an!
E-Mail: franziska.griebel@safetrans-de.org

Validation and Verification of Automated Systems – Resultate von ENABLE-S3 als Buchveröffentlichung

Das überaus erfolgreiche europäische Verbundprojekt ENABLE-S3 endete im Juni 2019 regulär. Nun sind die wichtigsten Ergebnisse zum Thema Testen automatisierter Systeme in sechs Anwendungsdomänen in Buchform zusammengefasst. Dabei werden alle relevanten Aspekte des Testens automatisierter Systeme abgedeckt, einschließlich Testmethoden sowie Testumgebungen. Darüber hinaus enthält das Buch Artikel über ergänzende internationale Aktivitäten aus den USA und Asien, um die globale Bedeutung des Themas hervorzuheben und die breite Palette von Aspekten abzudecken, die auf globaler Ebene behandelt werden müssen.
ENABLE-S3 zielte darauf ab, die heutigen kostenintensiven Überprüfungs- und Validierungsverfahren durch fortschrittlichere und effizientere Methoden zu ersetzen.
Mehr zum Projekt ENABLE-S3: www.enable-s3.eu

Leitner, Andrea, Watzenig, Daniel, Ibanez-Guzman, Javier (Eds.). Validation and Verification of Automated Systems. Results of the ENABLE-S3 Project. Springer. 2020



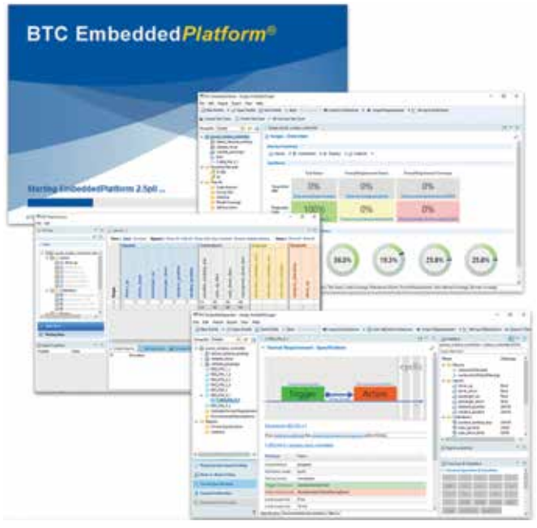
Interdisziplinäres Forschungszentrum für Human-Cyber-Physical Systems gegründet

Ob Sprachassistenten wie Siri und Alexa, Smart Home Systeme, intelligente Energienetze oder autonome Fahrzeuge: Die Digitalisierung lässt die physische und virtuelle Welt im Alltag immer mehr verschmelzen. Menschen und Maschinen arbeiten immer intensiver zusammen und Maschinen übernehmen zunehmend Aufgaben, die bisher Menschen erledigt haben. Welche technischen und gesellschaftlichen Herausforderungen diese sogenannten „Human-Cyber-Physical Systems“ (HCPS) mit sich bringen und wie sie verantwortlich gestaltet werden können, erforschen Oldenburger Wissenschaftler in zahlreichen Projekten. Um die Aktivitäten zu bündeln und Synergien zu schaffen, wurde Ende Juli das interdisziplinäre Forschungszentrum „Human-Cyber-Physical Systems: Safety, Acceptance, Social and Cultural Embeddedness“ (kurz: FZ HCPS) an der Universität Oldenburg eingerichtet.
Daran beteiligt sind – neben Professor*innen und Wissenschaftler*innen der Universität Oldenburg und des OFFIS – die Jade-Hochschule, das Deutsche Zentrum für Luft- und Raumfahrt (DLR) sowie das Fraunhofer Institut für Digitale Medientechnologie IDMT. Zum Direktor wurde Prof. Dr. Werner Damm (SafeTRANS-Vorstand) gewählt, stellvertretender Direktor ist der Psychologe Prof. Dr. Christoph Herrmann. Jürgen Niehaus wurde zum Geschäftsführer des FZ ernannt (ebenfalls Geschäftsführer SafeTRANS).
https://uol.de/fzhcps/

CARL VON OSSIETZKY universität OLDENBURG
Forschungszentrum Human-Cyber-Physical Systems
Safety, Acceptance, Social and Cultural Embeddedness

Neue Version BTC EmbeddedPlatform 2.5 verfügbar

Die BTC Embedded Systems AG bringt mit dem neuen Major Release BTC EmbeddedPlatform 2.5 viele neue Features und Verbesserungen für seine ISO 26262 zertifizierten Test-Lösungen. Hierbei enthalten sind insbesondere die neuen Version BTC EmbeddedTester 4.5, BTC EmbeddedSpecifier 2.5 und BTC EmbeddedValidator 5.5.
Neben der bereits vorhandenen Unterstützung für Simulink, dSPACE TargetLink und handgeschriebenem C-Code wird ab sofort auch der Code Generator Embedded Coder von TheMathworks unterstützt. Für eine optimale Prozessintegration und Automatisierung wurden weiterhin die Anbindungen an IBM Doors, PTC Integrity, Siemens Polarion und Jenkins verbessert.
Für den Requirements-basierten Test ist es nun möglich, einen Testfall mit mehreren Kalibrations-Datensätzen zu verknüpfen, sodass dieser automatisch mehrfach ausgeführt wird. Kalibrations-Datensätze werden zentral pro Testprojekt verwaltet und können manuell erstellt oder importiert/exportiert werden. Zusätzlich wurde die Unterstützung von Enumerations verbessert. Diese werden automatisch aus dem System-under-Test (z.b. Simulink) ausgelesen und sind bei der Testfallerstellung komfortabel aus einem Drop-Down Menu auswählbar.
Das neue AddOn „Requirements Analysis“ ermöglicht die Analyse sicherheitskritischer Requirement auf Konsistenz, Korrektheit und Vollständigkeit (oder auch CCC=Consistency, Correctness, Completeness). Die Konsistenz-Prüfung führt eine vollständig automatische Analyse durch um Widersprüche in einer Menge von Requirements aufzudecken. Korrektheit bedeutet, dass Anforderungen auch tatsächlich die gewünschte Funktionalität beschreiben. Dies lässt sich mithilfe von Testfällen überprüfen, die sozusagen auf den Requirements ausgeführt werden; man könnte hier von einer „Requirements-in-the-loop“ Simulation sprechen. Vollständigkeit liegt vor, wenn die vorhandenen Requirements für ein bestimmtes System immer zu einem eindeutig definierten Ausgangsverhalten führen. Diese drei Methoden erlauben es, die Qualität sicherheitskritischer Anforderungen in einer sehr frühen Entwicklungsphase zu überprüfen und zu verbessern.
Die BTC Embedded Systems AG ist ein Tool-Anbieter für intelligente, automatisierte und ISO 26262 zertifizierte Testlösungen mit dem Schwerpunkt auf Matlab Simulink sowie generiertem oder hand-geschriebenem Seriencode. Die BTC Embedded Systems AG feiert dieses Jahr ihr 20-jähriges Bestehen und ist aktuell mit über 150 Mitarbeitern an den Standorten Oldenburg, Berlin, Detroit, Tokio, Nagoya, Shanghai, Paris und Timisoara präsent.
www.btc-es.de



AbsInt-Tool Astrée erfüllt die NIST-Kriterien

Das Nationalinstitut für Standards und Technologie, NIST, ist die US-Bundesbehörde für Standardisierungsprozesse, die unter anderem für die Sicherheit in der Informationstechnik zuständig ist. Im Rahmen der SATE-VI-Erhebung untersuchte das Institut Tools zur statischen Analyse vom C-Code. Im Ergebnis haben nur zwei Tools die NIST-Testkriterien erfüllt: Astrée und Frama-C.
Astrée wurde auf 28 Sätzen von Benchmarks mit insgesamt 18954 Fehlern unterschiedlichster Natur getestet. Alle 18954 wurden von Astrée entdeckt. Dazu zählten unter anderem arithmetische Überläufe, Pufferüberläufe, ungültige Zeigermanipulationen, Division durch Null, Benutzung uninitialisierter Variablen, mehrfache Deallokation, Endlosschleifen, toter Code und vieles mehr. Darüber hinaus entdeckte Astrée in den Benchmarks Tausende unbeabsichtigter Fehler.
Der Abschlussbericht des NIST betont Astrées außerordentliche Präzision, sowohl im Hinblick auf die Analyseergebnisse als auch auf das Analysemodell an sich. Der vollständige Bericht wurde in Mai 2020 veröffentlicht und steht als kostenloser PDF-Download auf der NIST-Webseite zur Verfügung:
nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8304.pdf

www.absint.com

AbsInt

SafeTRANS – Fit für die Zukunft: Ausrichtung, Themen und Umsetzung

Internationale Studie bestätigt: Ohne Embedded Software und die Beherrschung komplexer Systeme werden technologische und damit auch gesellschaftliche Herausforderungen nicht zu bewältigen sein.

Anhand einer Analyse des SafeTRANS „Stamm-Technologiefeldes“ Embedded und Cyber-Physical Systems werden die Aktivitäten von SafeTRANS erläutert und anschließend deren gesellschaftliche und ökonomische Bedeutung eingeordnet. Die europäische Studie zu „Embedded Intelligence: Trends and Challenges“[1] verdeutlicht die technische und wirtschaftliche Bedeutung eingebetteter Systeme und CPS im Rahmen elektronischer Komponenten und Systeme. Die zusammenfassende Bestandsaufnahme der strategischen Ausrichtung wissenschaftlicher und industrieller Forschung und Entwicklung sowohl im nationalen als auch im europäischen Umfeld bestätigt die große Bedeutung der Koordinierung starker Partner für zukunftsweisende Lösungen.

ACPS – autonom, vernetzt und anpassungsfähig

Computing Systems durchdringen unser tägliches Leben, größtenteils eingebettet, z. B. in Consumer Electronics, medizinischen Geräten, in der Energieversorgung oder dem Transportbereich, um nur wenige Einsatzgebiete zu nennen. Dank kontinuierlicher Weiterentwicklung der Leistungsfähigkeiten von Soft- und Hardware rücken verstärkt hochautomatisierte bzw. gar autonome CPS (ACPS) bzw. Gruppen von ACPS und Systems-of-Systems (SoS) in den Fokus. ACPS und SoS ermöglichen die Vernetzung einer Vielzahl von Dingen und Anwendungen zu größeren Einheiten (Abb. 1). Die Systeme erlauben, u. .a. durch hochleistungsfähige Sensoren, bessere Vernetzung und funktionsstärkere Software, neue Funktionen, wie beispielsweise die eigenständige Anpassung an sich verändernde Umwelten und selbstständiges Agieren in dynamischen Situationen. Dazu können diese Systeme typisch ihre eigenen Fähigkeiten anpassen, mit möglicherweise unvorhergesehenem Verhalten – beispielsweise durch Aktualisierungen von Soft- oder Hardware im Feld und/oder durch „Lernen“. Die Anwendungen sind auf heterogenen Systemen verteilt realisiert, mit einer Vielzahl von Ressourceneinschränkungen und müssen erhöhte Anforderungen an (Cyber-)Sicherheit aufgrund verstärkter Kommunikation durch zunehmende Vernetzung, zum Teil mit Cloud-basierten Diensten, erfüllen. Hinzu kommt bei SoS im Unterschied zu CPS in Einzelsystemen, dass die Steuerung nicht zentral erfolgt, sondern durch das Zusammenwirken der Einzelsysteme quasi zur Laufzeit entsteht.

Hierarchie der CPS-Systeme:

Abb. 1: Stufen des Vernetzungsgrades von Systemen

Um die vielfältigen Einsatzmöglichkeiten dieser Systeme nutzen zu können, müssen hohe Anforderungen an Sicherheit und Beherrschbarkeit gewährleistet sein. Bei Entwicklung, Test und Absicherung spielen Verständlichkeit und (Fehler-)Nachvollziehbarkeit eine entscheidende Rolle, um trotz extrem hoher Komplexität und teilweise nicht vorhersehbaren Konstellationen die Sicherheit der Systeme prüfen und sicherstellen zu können. Die Entwicklung der Systeme sowie das kontinuierliche Testen der korrekten Ausführung der „richtigen“ Funktionen muss, neben der Funktionalität an sich, durch neue Verfahren und (Zertifizierungs-) Methoden abgedeckt werden, da der „Raum der möglichen Verhalten“ zu groß ist, um umfassend getestet werden zu können.

Aktivitäten für zukunftsfähige ACPS

Der Aufbau dieser Systeme und die Gewährleistung ihrer Sicherheit, Zuverlässigkeit, Lebensdauer und Zertifizierung erfordern innovative Technologien in den Bereichen Modellierung, Software-Engineering, modellbasiertes Design, Verifikation und Validierung sowie virtuelles Engineering, auch unter wirtschaftlichen Aspekten. Diese Entwicklungen und speziell die Absicherung durch neue Entwicklungs-, Testmethoden und Werkzeuge hat SafeTRANS bereits in der Roadmap „Hochautomatisierte Systeme“ (2017) aufgezeigt. Die Ergebnisse der Roadmap flossen u. a. ein in die Strategiepapiere europäischer Förderinstrumente, wie die ECS SRA 2018 und 2019[2]. In Fortführung der Roadmap zu hochautomatisierten Systemen setzt sich SafeTRANS mit Herausforderungen selbstlernender, komplexer Systeme im Arbeitskreis „Resiliente, lernende und evolutionäre Systeme“ auseinander, der 2018 startete und seine Ergebnisse in der Forschungsroadmap „Safety, Security, and Certifiability of Future Man-Machine Systems“[3] Ende 2019 veröffentlicht hat. Die Roadmap beschreibt erstmalig eine systematische Kategorisierung der Komplexität zukünftiger ACPS in verschiedene Dimensionen, entlang derer sich diese Komplexität entwickelt. Auf Basis dieser Komplexitätsdimensionen wird der Forschungs- und Entwicklungsbedarf sowohl für die CPS selbst als auch für zugehörige Test-, Validierungs- und Zertifizierungsverfahren abgeleitet (mehr zur Roadmap ab Seite 12.)

Die Roadmap „Safety, Security, and Certifiability of Future Man-Machine Systems“ wird durch den Arbeitskreis „Branchenübergreifende Prozesse, Methoden und Technologien für Safety und Security hochautomatisierter Systeme“ ergänzt. Der AK erarbeitet und analysiert auf Grundlage eines Continuous Development (DevOps)-Ansatzes eine Konkretisierung der relevanten Themen aus der Komplexitätsdimension „Integrität und Zertifizierung“ der umfassenderen, abstrakteren Roadmap „Safety, Security, and Certifiability of Future Man-Machine Systems“.

Plattformen und Interoperabilität sind und waren seit jeher ein wichtiges Thema für ACPS. Dies gilt sowohl für die Systeme selbst - insbesondere für den Aufbau von sektorübergreifenden Lösungen z.B. im Bereich SmartCity - als auch für den Bereich der Entwicklungsprozesse, in der eine Fülle von unterschiedlichen Methoden und Werkzeugen zum Einsatz kommt.

Plattformen, Interoperabilität und die zugehörigen Standardisierungen sind daher seit den Anfängen in 2006 ein wichtiges Thema für SafeTRANS. SafeTRANS setzt sich für Interoperabilitätsstandards bei Entwicklungswerkzeugen- und -plattformen ein. Durch Abstimmung von großen europäischen FuE-Projekten sowie im nationalen Bereich wird Entwicklungsknowhow weitergegeben, werden Forschungsergebnisse nachhaltig genutzt und Standardisierungsprozesse vorbereitet (CESAR, MBAT, SPES, SPES-XT, EANBLE-S3, StepUp!-CPS, ….).

Darüber hinaus verstärkt SafeTRANS sein Engagement im Bereich Wissenstransfer und Begleitung von FuE-Projekten durch den Aufbau und die Moderation sogenannter Advisory Boards zu bestehenden öffentlich geförderten Projekten.

In einem Advisory-Board sind Unternehmen aus allen Teilen der Wertschöpfungskette (Forschungsinstitute, Universitäten, OEMs, Zulieferer, Tool-Hersteller, Consulting) der betreffenden Branchen vertreten, die mit ihrem Knowhow Partner in FuE-Projekten unterstützen, allerdings selbst keine Projektpartner sind. Advisory-Boards vereinfachen eine schnelle und direkte Rückmeldung von Experten an die Projektpartner und ermöglichen den beteiligten Akteuren schnellen Zugang zu Wissen über aktuelle Grundlagenforschung. Durch den koordinierten Wissenstransfer zwischen Partnern in und außerhalb des Projekts in einem schlanken Prozess schaffen Advisory-Boards „Öko-Systeme“ zur Unterstützung von Forschung und Entwicklung (mehr zu Advisory-Boards siehe Seite 5).

Um neben den Projekt-getriebenen Aktivitäten ein öffentliches Forum für Austausch und Networking nutzen zu können, hat SafeTRANS das Symposium „SafeTRANS Industrial Day“ etabliert. Der SafeTRANS Industrial Day richtet sich mit domänenübergreifenden Fachvorträgen, Demonstrationen und Diskussionsrunden an Entscheider und Entwickler und ermöglicht mit einem hochkarätigen Programm Wissen auszutauschen, neue Kontakte zu knüpfen sowie vorhandene zu vertiefen (mehr zum letzten SafeTRANS Industrial Day auf Seite 23).

ACPS und Wertschöpfung

Die eng miteinander und mit Menschen agierenden (A)CPS erfordern neue Formen der Mensch-Maschine Interaktion (Schlagwort: „Von Assistenz zu Kooperation“). Entsprechende Kommunikations- und Kooperationsstrategien werden zunehmend in Software realisiert, um Flexibilität und Update-Fähigkeit zu erreichen. Dies bedingt einen Wandel in den Wachstumsraten der einzelnen Stufen der Wertschöpfungskette. Aktuell liegt der größte Teil der Wertschöpfung in Bereichen mit unter 10 % Software-Anteil (elektronische Kom-

[1] Embedded Intelligence: Trends and Challenges. A Study by Advancy. ARTEMIS-IA (Hrsg.). 2019

[2] ECS Electronic Compoments & Systems. Strategic Reseach Agenda 2018 (2019). AENEAS, ARTEMIS-IA, EPoSS (Hrsg).

[3] Safety, Security, and Certifiability of Future Man-Machine Systems. Arbeitskreis Resiliente, lernende und evolutionäre CPS. SafeTRANS (Hrsg.). 2019

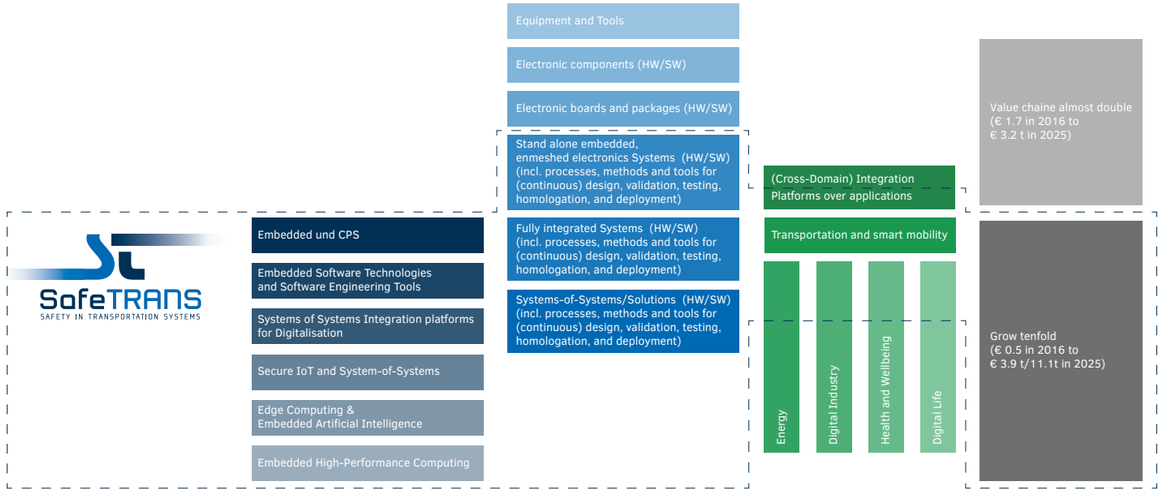


Abb. 2: Der SafeTRANS-Fokus auf Technologiefelder (dunkles Blau) in Zusammenhang mit Bereichen der monetären Wertschöpfung (helles Blau) und der prognostizierten Wertsteigerung (Grau). Die von Experten empfohlen anwendungsübergreifenden integrierten Plattformen in Grün. (Quelle: Grafik SafeTRANS, Inhalte aus: Embedded Intelligence: Trends and Challenges. A Study by Advancy. ARTEMIS-IA (Hrsg.). 2019)

ponenten, Boards, etc.)[4]: Die Werterzeugung wird sich von Produkten hin zu (System-)Lösungen verschieben (siehe Abb. 2). Besonders die Bereiche sich selbst regulierender Netzwerke (KI) und dynamisch vernetzter Dinge und Anwendungen werden zukünftig an Bedeutung gewinnen. So ist eine anwendungsorientierte Grundlagenforschung für Industrie und Forschungsinstitutionen erforderlich, um Innovationen und Lösungen für automatisierte oder autonome CPS und SoS zu schaffen und sich in einem globalen Wettbewerb behaupten zu können.

SafeTRANS kann und wird seine Aktivitäten zur Unterstützung national und europäisch abgestimmter Forschung und Entwicklung verstärken, indem:

- domänenübergreifend Experten der gesamten Wertschöpfungskette zusammengebracht werden, um FuE-Aktivitäten zu planen, durchzuführen und Lösungen zu entwickeln
- Maßnahmen zur Stärkung und Intensivierung der Kooperation von starken Industrievertretern mit hochkarätigen Forschungsinstituten
- die politische Sichtbarkeit der Themen unterstützt wird
- die bereits angegangene Öffnung der Transportdomäne gegenüber anderen Domänen weiter vorangetrieben wird
- Standardisierungsmaßnahmen für Entwicklungswerkzeuge unterstützt werden.

Trotz und gerade wegen der aktuellen gesellschaftlichen Herausforderungen werden ACPS nicht an Bedeutung verlieren, sondern bei der Funktionalität und Steuerung medizinischer, Energie- und Transportsysteme immer bedeutender. Sie sind und werden zu einem wesentlichen Rückgrat und Bestandteil jeder Lösung für die gesellschaftlichen Herausforderungen. Um so wichtiger, dass die Entwicklung, Überprüfung und der Sicherheitsnachweis nachvollziehbar und anpassbar sind und bleiben.

[4] Embedded Intelligence: Trends and Challenges. A Study by Advancy. ARTEMIS-IA (Hrsg.). 2019

Embedded Software und *Complex Systems* in ECS SRIA verankert

Die von AENEAS, ARTEMIS-IA und EPoSS gemeinsam erstellte „Electronic Components & Systems Strategic Research and Innovation Agenda“ (ECS SRIA) wird derzeit neu erarbeitet.

Elektronische Komponenten und Systeme sind eine Grundlage der digitalen Wirtschaft. Um die EU-Forschung hinsichtlich ECS ausrichten zu können, entwickeln die drei europäischen Industrieverbände AENEAS, ARTEMIS-IA und EPoSS, die Großunternehmen, KMU, Universitäten und Forschungsinstitute umfassen, eine gemeinsame strategische Forschungsagenda. Diese wird aktuell in der vierten Auflage für 2021 neu erarbeitet. Die ECS SRIA identifiziert wichtige Forschungsprioritäten, technologische Herausforderungen und Anwendungsbereiche, um die digitale Zukunft Europas mitzugestalten.

Im Gegensatz zu den vergangenen beiden Versionen der SRA, bei denen es sich im Wesentlichen nur um Anpassungen und Fortschreibungen der 2017 erstmalig erstellten gemeinsamen SRA handelte, wird die vierte Auflage als sogenanntes „großes Update“ völlig neu strukturiert. Dies erlaubt eine Anpassung und Schwerpunktsetzung der FuE-Themen an die aktuelle und zukünftige Entwicklung von Embedded und Cyber-Physical Systems. Die ECS SRIA 2021 wird aus zwei Hauptteilen bestehen:

- Dem Richtlinienpapier Part A, welches der Einführung in die ECS SRIA 2021 sowie als eigenständiges Dokument für strategische Entscheidungen dient und
- den detaillierteren Themenbeschreibungen im zweiten Teil, Part B, der auf einem Bottom-up-Ansatz basiert und u. a. Projektmanager bei der Ausgestaltung europäischer Verbundprojekte unterstützt.

Im Teil A werden soziale Herausforderungen und deren digitaler Bezug, die europäische Wettbewerbsfähigkeit und nachhaltige Wirtschaft, Umsetzungsempfehlungen und die Positionierung der ECS SRIA im europäischen FuE-Umfeld thematisiert. Ebenso werden Ergebnisse der EU-Studie zu Embedded Intelligence[1] aufgegriffen, die Handlungsempfehlungen zur Stärkung der Software-intensiven Bereiche beinhalten.

Der zweite Teil beschreibt FuE-Herausforderungen aus Industrie und Grundlagenforschung. War die SRA in den vergangenen Versionen noch zweidimensional strukturiert in Anwendungs- und Technologiefelder, so besitzt die neue SRIA eine dreidimensionale Struktur: Anwendungsfelder wie Mobilität, Energie, Medizin und weitere beschreiben die Ziele und erwarteten Applikationen. Dies wird komplementiert durch Technologieentwicklungen, die zum einen entlang eines Technology Stacks angeordnet sind, zum anderen querschnittlich zu diesem Stack liegen (vgl. Abb 1). Im Technology-Stack sind insbesondere die Ebenen „Embedded Software and beyond“ sowie „Complex Systems“ neu im Vergleich zu vorangegangenen Versionen der SRA. Damit erhält der Software-Bereich auf europäischer FuE-Ebene mehr Sichtbarkeit, was zur Stärkung von Software-intensiven Verbundprojekten beiträgt. Gemeinsam mit Horst Pfuegel (AVL) und Ralf Popp (edacentrum) verantwortet Jürgen Niehaus (SafeTRANS CEO) das Kapitel „Archcitectures and Design: Methods and Tools“, in dem kontinuierliche Lebenszyklus umspannende Entwicklungsprozesse (DevOps und continuous system integration), Referenzarchitekturen und Plattformen sowie die zur Entwicklung moderner ACPS benötigten Methoden und Werkzeuge das zentrale Thema sind.

Die ECS SRIA 2021 bildet die Grundlage für Projekte des EU-Förderprogramms ECSEL und damit die Basis für den kommenden ECSEL-Call in 2021. Darüber hinaus strahlt die ECS SRIA aus auf das neu zu entwickelnde europäische Forschungsrahmenprogramm (Nachfolger für Horizion 2020), die Joint Undertaking Key Ditigal Technologies, EU-Lighthouse-Initiativen sowie weitere EU-Förderinstrumente (u. a. EUREKA's PENTA/EURIPIDES und „Important Project of Common European Interest“, IPCEI). Voraussichtlich ab Q3 2020 wird die ECS SRIA 2021 als Draft verfügbar sein. Die Veröffentlichung ist für Ende 2020 geplant.

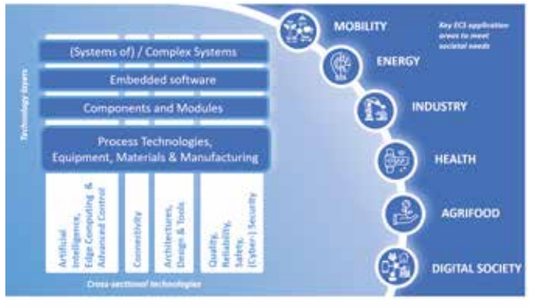


Abb. 1: Inhaltl. Struktur der zukünftigen ECS SRIA 2021, Part B.

[1] Embedded Intelligence: Trends and Challenges. A Study by Advancy. ARTEMIS-IA (Hrsg.). 2019

“Safety, Security, and Certifiability of Future Man-Machine Systems” - SafeTRANS veröffentlicht Roadmap und Positionspapier

Die Raodmap liefert erstmalig eine Klassifikation der Fähigkeiten zukünftiger mit Menschen interargierender CPS sowie der damit verbundenen Herausforderungen für Forschung und Entwicklung.

Ob Mobilität, Energie, Gesundheit, Produktion: Die technischen Antworten auf Herausforderungen der Zukunft basieren auf komplexen, vernetzten, digitalen Systemen, welche Entscheidungs- und Führungsprozesse für und in Kooperation mit Menschen treffen. Dieses geschieht oft auf der Basis von lernenden und adaptiven Entscheidungsverfahren und immer öfter auch anwendungsdomänenübergreifend. Um die Chancen solcher großen, vernetzten, sich selbst ändernder Systeme vollständig nutzen und gleichzeitig die entstehenden Risiken beherrschen zu können, hat SafeTRANS erstmalig eine systematische Aufstellung der Komplexität dieser Systeme entwickelt. Anhand von fünf Komplexitätsdimensionen leitet sich eine Roadmap mit zeitlicher Abschätzung der benötigten technologischen Verfügbarkeiten ab. Ziel ist es, höchste Sicherheitsanforderungen für digitale Lösungen sicherheitskritischer Anwendungen mit dem Merkmal „Quality Made in Germany“ etablieren zu können.

Das Positionspapier und die Roadmap über „Safety, Security, and Certifiability of Future Man-Machine Systems“ stellen einen hochaktuellen, domänenunabhängigen Ansatz zur qualitativen Analyse der Komplexität zukünftiger mit Menschen interagierender Cyber-Pysical Systems vor und betrachten die mit jedem Komplexitätszuwachs resultierenden Herausforderungen zur Sicherung der Qualität (funktionale Sicherheit und Sicherheit der intendierten Funktion sowie Cyber-Sicherheit). Die ins Detail gehende Roadmap widmet sich den Herausforderungen hinsichtlich Umsetzung und legt eine zeitliche Abschätzung der Beherrschung der benötigten Technologien vor. Es werden Fragestellungen verschiedener Anwendungen aufgegriffen, wie sie z. B. in Verbundprojekten der Automobilindustrie zur Qualitätssicherung und Zulassung autonomer Fahrzeuge oder in der Risikobewertung des Einsatzes von KI-Methoden in medizinischen Anwendungen, in der Wirkungsforschung im Energiesektor oder unter ethischen Aspekten in den Sozial- und Geisteswissenschaften behandelt werden. Die in Roadmap und Positionspapier dargestellte ganzheitliche Metrik basiert auf fünf Komplexitätsdimensionen und bildet die Grundlage zur Erfassung der Qualitätsanforderungen unabhängig von Branchengrenzen. Mithilfe dieser Metrik kann die Qualität resilienter, evolutionärer, lernender Systeme gesichert werden und Investitionen in Forschung und Entwicklung können zum richtigen Zeitpunkt erfolgen. (Auszüge aus dem Inhalt ab Seite 14.)

Disruptive Veränderungen

Die bisher als Draft erschienen Versionen von Roadma und Positionspapier waren im Dezember 2019 die Grundlage des Symposiums „Safety, Security, and Certifiability of Future Man-Machine Systems“, das im Rahmen der ACPS Days veranstaltet wurde (siehe Seite 24). Während des Symposiums wurden die Dokumente einschlägigen Verbänden vorgestellt und mit hochrangigen Vertretern u. a. der Siemens AG, Robert Bosch GmbH, Fraunhofer Gesellschaft, dem DFKI und DLR besprochen, um die Abstimmung mit anderen Domänen, Verbänden und der Politik weiter voranzutreiben.
Dr. Johannes Helbig (Business Transformation Institute) machte in seiner Keynote anhand von konkreten Beispielen deutlich, dass die Beherrschbarkeit großer, vernetzter, digitaler Systeme der Schlüssel für die Wettbewerbsfähigkeit in der zukünftigen digitalen Ökonomie sein wird und hierbei insbesondere die Qualitätssicherung eine entscheidende Rolle für die Erschaffung von vertrauenswürdigen und damit marktfähigen und erfolgreichen Systemen spielt
Die durch die zukünftigen Mensch-Maschine Systeme ausgelösten Veränderungen sind unaufhaltsam und maßgeblich für unsere Gesellschaft, Umwelt und Ökonomie, sodass die Beherrschbarkeit der neuen Systeme eine konzertierte gemeinsame Anstrengung von Politik, Wirtschaft und Wissenschaft erfordert. Einen strategischen Ansatz für ein abgestimmtes Vorgehen in Forschung und Entwicklung bilden das Positionspapier und die Roadmap zu Safety, Security, and Certifiability. Aktuell wird der Draft dieser Papiere mit Vertretern der einschlägigen Industrieverbände sowie der Politik diskutiert und ggfs. erweitert. Ebenso erfolgt eine Erweiterung um konkrete weitere Anwendungsbeispiele und um sogenannte Querschnittsthemen (wie Umgang mit Daten, Ethik, usw.) sowie die Konkretisierung der Handlungsempfehlungen, die in einem weiteren Symposium in Q4 2020 vorgestellt werden.
SafeTRANS als Herausgeber konnte bei der Erstellung der Dokumente auf vielfältige Erfahrungen im Bereich Strategieentwicklung und Themenevaluierung für zukünftige Forschungsvorhaben zurückgreifen (u. a. auf das domänenübergreifende Papier „Nationale Roadmap Embedded Systems“ aus dem Jahr 2009, weitere branchenspezifische Forschungsstrategie-Dokumente sowie die kontinuierliche Mitarbeit an der europäischen Strategic Research Agenda des EU-Förderinstruments ECSEL, siehe Seite 11).

Hintergrund und Umsetzung

Das Positionspapier „Safety, Securitiy, and Certifiability for Future Man-Machine Systms“ ist eine Essenz der Roadmap von knapp 130 Seiten, das im Rahmen des SafeTRANS-Arbeitskreises über resiliente, lernende und evolutionäre Cyber-Physical Systems in mehreren Workshops von Experten aus Industrie und Wissenschaft erarbeitet worden ist. Die Ko-Leitung des Arbeitskreises hatten Prof. Dr. Werner Damm (SafeTRANS) und Peter Heidl (Robert Bosch GmbH) inne.
Neben der Diskussion der aktuell in einer Draft-Version vorliegenden Roadmap und des Positionspapiers mit Industrieverbänden werden derzeit die Inhalte in einem parallelen Prozess auf weitere Anwendungsdomänen ausgeweitet.
Die strategischen, übergeordneten Themen der Komplexitätsdimension „Integrity and certification“ aus Roadmap/Positionspapier werden darüberhinaus durch den SafeTRANS-Arbeitskreis „Branchenübergreifende Prozesse, Methoden und Technologien für Safety und Security hochautomatisierter Systeme“, kurz: PMT4S&S, hinsichtlich Forschungsthemen zur Erreichung der benötigten Fähigkeiten aufbereitet und schließen einen Abgleich vorhandener und fehlender Methoden/Prozesse/Technologien ein. Der Arbeitskreis PMT4S&S wird von Dirk Geyer (AVL Software and Functions GmbH) und Martin Rothfelder (Siemens) geleitet und seine Ergebnisse in Q3 in 2020 vorstellen.

Abb. 1: Podiumsgespräch während des Symposiums (v.l.n.r.): Haimo Huhle (ZVEI), Bernhard Evers (Siemens Mobility GmbH), Rebekka Weiß (BITKOM), Prof. Dr. Katharina Seifert (Direktorin Institut für Verkehrssystemtechnik, DLR), Dr. Johannes Helbig (Managing Director Business Transformation Institute) und Prof. Dr. Peter Liggesmeyer (Institutsleiter Fraunhofer IESE)

Im Folgenden wird auf die wichtigsten Inhalte der Dokumente zu „Safety, Security, and Certifiability of Future Man-Machine Systems“ eingegangen.

Inhalte I: Komplexitätsdimensionen

Ausgangsfragen für die Roadmap waren: Wie können wir die Komplexität digitaler Mensch-Maschine-Systeme bewerten? Wie einen Zugang zu notwendigen Maßnahmen zur Qualitätssicherung gewinnen?
Das Positionspapier und die Roadmap stellen die Ergebnisse einer Analyse zahlreicher realer, komplexer Systeme vor, auf deren Basis fünf Dimensionen – teilweise mit Untergruppen – mit jeweils dimensionsspezifischen Skalen zur Bewertung der Komplexität identifiziert wurden (siehe Abbildung 2). Die Komplexität einer Applikation wird dabei aus Sicht des Systems gemessen, das die Applikation realisiert. Diese relative Bewertung trägt dem Rechnung, dass ein und dieselbe Aufgabe für ein System leicht, für ein anderes schwer zu lösen ist, je nach Stärke des Systems. Der Begriff System bezeichnet dabei je nach Aggregationsstufe ein einzelnes technisches System, eine Gruppe, ein homogenes oder heterogenes Kollektiv von Menschen und technischen Systemen (siehe Seite 8, Abb. 1). Gemeinsam ist allen diesen Systemausprägungen:

- die Abgrenzung zwischen dem Egosystem und einem umgebenden Kontext, der unterschiedlich komplex gestaltet sein kann und
- der Fähigkeit, diesen Kontext über eine Systemschnittstelle „wahrzunehmen“, also eine digitale oder mentale Repräsentation des aktuellen Kontextes zu erstellen.

Die fünf identifizierten Komplexitätskategorien

- Context
- Strength
- Responsibility and reflection
- Integrity and certification
- Cooperation

sind unterteilt in Abstufungen bis hin zu Fähigkeiten und Fertigkeiten vollumfänglicher resilienter, lernender und evolutionärer Mensch-Maschine-Systeme. Beispielhaft soll hier die Komplexitätsdimension Stärke vorgestellt werden: (System-)Stärke bezeichnet die Fähigkeiten des Egosystems seine (selbstgesteckten) Ziele erreichen zu können. Dies wird umso eher gelingen, umso höher oder größer die Intelligenz des Systems ist, umso besser es sich an sich verändernde Umfeldbedingungen anpassen kann, also welche Evolutionsfähigkeiten es besitzt, und mit welchem Grad an Autonomie es ausgerüstet ist (siehe Skalen „Strength“ in Abb. 2).

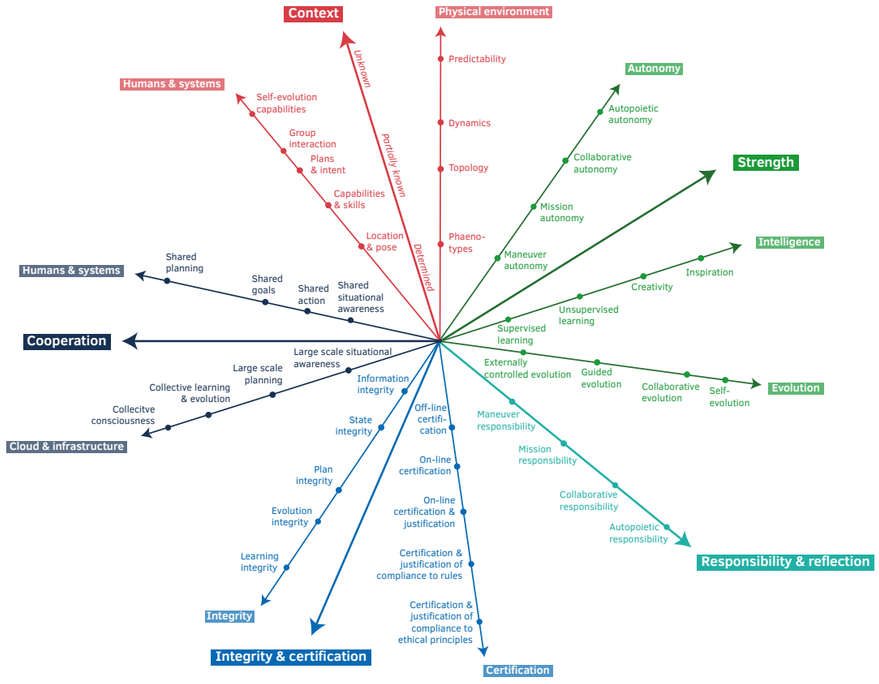


Abb. 2: Dimensionsspezifische Skalen zur Bewertung der Komplexität von Mensch-Maschine-Systemen

Inhalte II: Roadmap-Diagramm mit zeitlicher Abschätzung

Basierend auf den benötigten Fähigkeiten (siehe Skalenwerte) erfolgt eine zeitliche Einschätzung des Erreichens der einzelnen Ausbaustufen in jeder der untersuchten Komplexitätsdimensionen (siehe Abbildung 3). Die zeitliche Einordnung wird in der Roadmap detailliert anhand der Analyse konkreter technologischer Fähigkeiten vorgenommen.

Inhalte III: Handlungsempfehlungen

Um diese Entwicklungen tatsächlich realisieren zu können, ist es notwendig, dass Forschung, Industrie und Politik zielgerichtet zusammen wirken. Dafür wurden zehn Handlungsempfehlungen zur Absicherungs des Qualitätsmerkmals „Made in Germany“ formuliert, die sich an Management und Politik gleichermaßen richten.

Abb. 4: Roadmap (rechts) und Positionspapier (links) „Safety, Security, and Certifiability of Future Man-Machine Systems“. Hrsg.: SafeTRANS. 2019. Verfügbar unter: http://www.safetrans-de.org/de/Aktivitaeten/Roadmapping.php

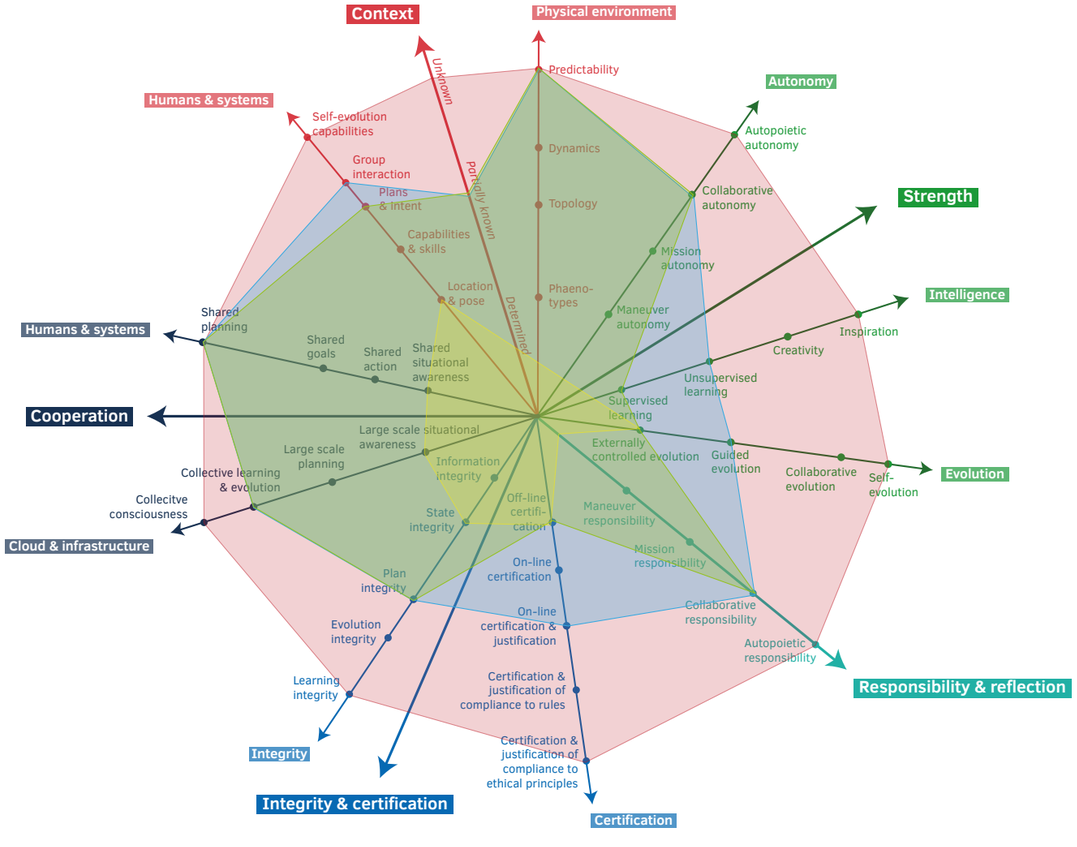


Abb. 3: Zeitliche Abschätzung zum Erreichen der einzelnen Skalenwerte

Legende:

- Langfristig: 2035 ff
- Mittelfristig: 2027 bis 2035
- Mit komplexitätsreduzierenden Einschränkungen zeitnah: heute bis 2027
- Zeitnah: heute bis 2027

„Ein Bewusstsein schaffen, wie verschiedene Branchen auf derselben Basis aufsetzen und Synergien entstehen können.“

Welchen Herausforderungen begegnet der größte europäische Luftfahrtkonzern bei Forschung und Entwicklung zukünftiger Cyber-Physical Systems und welche Visionen verbindet er mit diesen Systemen? Götz Anspach von Broecker, AIRBUS, dazu im Gespräch.

Moderner Flugzeugbau, Weltraumrobotik, Sicherheitstechnik: Hochtechnologie basiert auf vernetzten Cyber-Physical Systems (CPS), welche die physische und virtuelle Welt miteinander verbinden. Bei Europas größtem Luft- und Raumfahrtkonzern AIRBUS werden diese Systeme in Fertigung, Test und im Endprodukt eingesetzt. Damit einher gehen neue Herausforderungen in Forschung, Entwicklung und im gesamten Konzerngeschäft. Wie AIRBUS mit zukünftigen, lernenden CPS, vor allem bei sicherheitsrelevanten Anwendungen umgeht, welche Änderungen die neuen Systeme mit sich bringen und warum gute Roadmapping-Arbeit besonders wichtig ist, erklärt Götz Anspach von Brorcker von AIRBUS Defence and Space, Bremen.

Herr von Broecker, Sie sind bei AIRBUS für Forschung im Bereich Aerospace & Defence sowie ESA Technologieprogramme verantwortlich. Was genau umfasst Ihre Tätigkeit?

Goetz Anspach von Broecker: Ich bin im Bereich Forschungs- und Entwicklungsprogramme im Team für FuE-Kofinanzierung und Partnerschaften tätig. Das umfasst die Akquise von externen FuE-Budgets, die Anbahnung von FuE-Partnerschaften und in viel früheren Stadien, die Interessensvertretung der Branche und der Firma in Technologiefragen (staatliche Programme, Regularien, Synergiesuche mit ähnlichen Branchen), sprich Fragen der Technologiepolitik. Darüber hinaus unterstütze ich FuE-Partner, wie KMU oder Forschungseinrichtungen und Universitäten, in solche Programme zu kommen und deren frühzeitige Zusammenarbeit im Rahmen von FuE-Projekten (frühzeitig im Sinne von: schon bei niederen Technologiereifegraden, sog. TRL= Technical Readiness Leveln).
Ziel dabei ist immer, die Forschungs- und Entwicklungstätigkeiten so zu gestalten, dass technische Risiken bei den späteren Produkten, Services und Projekten minimiert werden und beherrschbar bleiben. Das frühe Vertrautmachen mit neuen Technologien, sowohl intern als auch auf Kunden- und Zuliefererseite, steht dabei im Vordergrund.

Die Zeitspanne eines Roadmapping-Prozesses, sprich der Evaluierung von FuE-Themen, der Verankerung in Förderprogrammen und der Projektakquise, ist stark domänenabhängig. Welche Erfahrungen haben Sie mit den konzernrelevanten Themen gemacht?

In der Luftfahrt, Raumfahrt oder Verteidigung ist das sehr unterschiedlich und innerhalb der Domänen sind diese Zeiträume abhängig von den Inhalten. Es kann sehr schnell gehen, sodass innerhalb von drei Monaten die Idee über die Beauftragung bis zur Umsetzung realisiert werden kann. Bei strategisch langfristigen Themen, wie z. B. dem CO_2-neutralen Fliegen oder Mondexpeditionen, sind Zeithorizonte von zehn bis 15 Jahren durchaus möglich. Es gibt in den Domänen kurz-, mittel- und langfristige Herausforderungen und je nach Bedarf werden entsprechende Programme genutzt oder Projekte initiiert. Um die Themen zu platzieren, Partner und Programme zu finden, ist gutes Roadmapping mit entsprechender Kommunikation ganz entscheidend. Wir erörtern in Workshops mit Kunden, Zulieferern und Forschungseinrichtungen unter Berücksichtigung der aktuellen Industrietechnik und Trends, was wir uns heute für morgen wünschen können. Daher ist eine Roadmap, die Zeitachsen aufspannt, wie das aktuelle Papier zu Human-Machine Systems[1], sehr hilfreich, um z. B. sicher zu stellen, dass funktionierende Entwicklungen durch entsprechende Regularien unterstützt werden oder Prozesse angestoßen werden.

Die von Ihnen erwähnte Roadmap zu „Safety, Security, and Certifiability of Future Man-Machine Systems“, an der AIRBUS mitarbeitet, befasst sich mit zukünftigen hochkomplexen, vernetzten CPS, mit vorrangig sicherheitskritischer Funktionalität. Wo stehen wir aktuell bzgl. der Absicherung vernetzter sicherheitskritischer CPS?

Meiner Einschätzung nach noch recht am Anfang. Es fehlt eine Art „technologische Guideline“, die festlegt, wie wir mit zukünftigen CPS umgehen wollen und auf deren Basis unsere Konzepte der Absicherung aufsetzen. Die technische Absicherung ist bereits möglich. Wir sind in Europa diesbezüglich gut aufgestellt, aber es fehlen die juristischen, föderalistischen, gesellschaftlichen Grundlagen.
Schaut man in andere Länder und Regionen, gibt es verschiede Kulturen und Herangehensweisen: Mit der sehr liberalen, aber mitunter auch für uns Europäer oft unmoralisch anmutenden „Just-Do-It“- oder „Trial-and-Error“-Mentalität haben die USA einen gewissen Vorsprung. Auch das massive Beschaffungswesen (gerade im geschützten Sicherheitssektor) der USA lassen die US-Wirtschaft hier im Vorteil erscheinen. Dagegen steht die Volksrepublik China, mit ihren staatlichen Großprojekten. In Europa, insbesondere in Deutschland, sind die Wege durch Regularien und Entscheidungsprozesse etwas länger. Auch der Glaube an die Technologie als Problemlöserin ist hier weniger ausgeprägt als in USA oder China. In Deutschland und Europa gibt es deutlich mehr Technologiekritik und Regulierung. Das hat zum einen Nachteile, wenn sie eine technische Idee nicht umsetzen können, weil es noch

[1] [Anm. d. Red.]: Safety, Security and Certifiability of Future Man-Machine Systems. Roadmap/Positionspapier. SafeTRANS e.V. (Hrsg.). Draft-Version 2019

kein Regelwerk dazu gibt. Zum anderen, kann diese Vorsicht aber auch sehr schützend sein – für die Menschenrechte, die Persönlichkeitsrechte und damit auch für die Freiheit der Gesellschaft.
Das Knowhow, die Fähigkeiten, die analytische und systemische Stärke haben wir in Deutschland im Bereich der CPS allemal. Die breite, freie Forschungslandschaft, der starke innovative Mittelstand und die moderat agierenden Großfirmen sind, solange Lehre und Ausbildung auf hohem Niveau gehalten werden können, ein hervorragender Nährboden. Wir müssen nur angesichts der massiven Umbrüche mit automatisierten Prozessen, KI-basierten Entscheidungen, transversalen Vernetzungen, neuen Projektmethoden mit agilen Projektprozessen etc. auch anfangen, unsere formalen Prozesse anzupassen. Heute bauen Internetunternehmer Raketen, Suchmaschinenbetreiber und Handelsplattformen werden zu Wirtschaftsgiganten. Daraus lernen wir, dass die Hardware zwar immer noch ein entscheidender Faktor ist, die Daten aber einen eigenen Wert als Handelsware bekommen. Wir müssen zu neuen Regeln kommen, die uns handlungsfähig halten und unsere Ethik und Werte schützen. Die alte Kameralistik oder Zuständigkeitsrangeleien helfen uns da gar nicht. Wenn wir Industrie, Privatleben, Gesundheitswirtschaft und öffentliche Bereiche miteinander in Kontakt bringen und es schaffen, dass sich Forschung, Industrie und öffentlicher Bedarf gegenseitig befruchten und sich Erprobungsräume für Technologie und angewandte Regeln schaffen, dann können wir die technologischen „Assets“ auch voll nutzen. Wir werden agil … und Agilität und Flexibilität ist die Voraussetzung für geschickte Anpassung – es werden dann auch Prinzipien wie der Föderalismus wieder zu wertvollen Errungenschaften und verlieren den Gôut des Bremsschuhs. Und hier setzt die neue SafeTRANS-Roadmap ein – ein Bewusstsein zu schaffen, wie verschiedene Branchen auf derselben Basis aufsetzen und wie Synergien entstehen können. Sie zeigt auf, welcher Player welche Rolle einnehmen kann, wie verschiedene Branchen gegenseitig voneinander lernen können und wo auch politisch und förderpolitisch die besten Hebel sitzen … und natürlich regulatorisch.

Für welche (Geschäfts-)Bereiche von AIRBUS ist die erwähnte Roadmap nach Ihrer Einschätzung relevant?
Für alle Bereiche: AIRBUS besteht im Wesentlichen aus drei Geschäftsbereichen. (A) Commercial Aircraft: also Entwicklung und Bau von Verkehrsflugzeugen. Diese Branche steckt im Umbruch. Reichte es früher ein Flugzeug zu bauen, das günstig zu kaufen und zu betreiben war, kommen jetzt immer komplexere Nutzen zusammen. Kein Flugzeug fliegt mehr alleine. Die Flugzeuge werden über die gesamte Lebensspanne zu vernetzten Elementen. Sie senden Daten zu Zustand und Betrieb der Maschine selbst und der Nutzlast (Passagiere) in ein komplexes Netzwerk. Der optimale Betrieb einer Flotte, das Managen von Flugmobilität, das Zusammenspiel mit Wartung, Bodensegment, Service, Hygiene etc. wird immer komplexer. Der Flottenverbrauch muss über viele Parameter gesteuert werden (Flugrouten, Flugzeugart, Wetterprognosen, politische Geschehnisse etc.). Das sind neue Herausforderungen an einen Flugzeugbauer. Er wird ggf. ein Stück weit zum Mobilitätsanbieter werden müssen.
Dann haben wir (B) AIRBUS Helicopter: Genau genommen ist das kein Hubschrauberbau im eigentlichen Sinne mehr. Hier gilt das Gleiche wie in der kommerziellen Luftfahrtbranche. Bei den VTOL (Vertical Take-Off and Landing = Senkrechtstartern) kommen nun Drohnen und Lufttaxis sowie Services bemannter und unbemannter Systeme dazu. Als Urban Air Mobility Anbieter werden sie zu einem System-of-Systems-Betreiber. Da liegt die Relevanz der erwähnten Roadmap zu Future Man-Machine Systems auf der Hand.
Drittens haben wir dann (C) AIRBUS Defence and Space: Bau von Raumfahrzeugen, Satelliten, Betreiber von Erdbeobachtungs- und Kommunikationssatelliten, Betreiber von Raumstationseinrichtungen, Grenzüberwachungssysteme, Küstenschutzsysteme, militärische Flugzeuge, Transport- und Logistikflugzeuge, GEO-Datenhändler und GEO-Datenservice Anbieter, Navigationssystem u. v. m. Und alles im Portfolio trägt massiv derzeit die Zeichen des Wandels vom Geräte-/Systementwickler zum System-of-System-Haus.
Ebenso der Bereich maritime Sicherheit – hier werden unterschiedlichste behördliche Bereiche (Bundespolizei See, Küstenschutz, DGzRS, Havariekommando, Zoll etc.) miteinander vernetzt werden müssen. Dazu dann noch die Vernetzung im europäischen Rahmen. Regeln, Datenschutz, Infrastrukturschutz und Eigenständigkeit der Beteiligten müssen dabei erhalten bleiben. Ein Paradebeispiel für die Roadmap.

Die Roadmap über Future Man-Machine Systems stellt eine umfassende Klassifikation von Komplexitätsdimensionen mit Unterkategorien auf (Cooperation, Context, Strength, Responsibility & Reflection, Integrity & Certification). Welche Komplexitätsdimension(en) sehen Sie als die wichtigste(n) an und warum?
Das möchte ich nicht unbedingt gewichten. Das ist eine Kette, die kein schwaches Glied haben darf, das sind Kategorien, die sich auch bedingen. Derzeit halte ich aber das Thema „Integrity & Certification“ für am dringlichsten. Denn hier wird die Basis gelegt um komplexe Systeme zukünftig in Leistung und Sicherheit überhaupt beschreibbar zu machen. Das wäre derzeit für mich sozusagen eine „Basis-Dimension“.

Aktuell ist im Zuge der Corona-Pandemie der politische Zugang und die Sensibilisierung für zukünftige CPS etwas in den Hintergrund getreten. Wie könnte ein weiteres Vorgehen aussehen?
Der Spannungsbogen muss gehalten werden, um die Roadmap über Future Man-Machine Systems politisch zu verankern und weiter bekannt zu machen, gerade auch bei Verbänden. Dabei wird die Bedeutung der Themen durch die aktuellen Herausforderungen unterstützt. Wenn die Themen der Roadmap heute schon umgesetzt wären, könnten wir u. a. auf digitale Daten zur Verbreitung des Virus zurückgreifen, einschließlich einer ethischen Zertifizierung und erklärbaren KI, die bei der Auswertung großer Datenmengen unterstützt. Daher ist die Klassifizierung der Komplexitätsdimensionen aktueller denn je, denn mithilfe der Abstufungen der einzelnen Komplexitätsdimensionen können wir zeitliche Abfolgen der benötigten technologischen Fähigkeiten und Fertigkeiten unter Berücksichtigung des regulatorischen Rahmens aufstellen.

Stichwort Absicherung und Beherrschung digitaler Systeme: Machen wir uns zu abhängig von diesen technischen Systemen?
Wir sind schon abhängig. Die verflochtenen weltweiten Systeme sind bereits so komplex, dass es eine unserer wichtigsten Aufgaben ist, die Abhängigkeit beherrschbar zu machen. Dafür müssen die Systeme transparent sein. Die erklärbare KI muss verpflichtend sein.

Wie könnte eine technische Rückfallebene für ein eingeschränktes, aber in jedem Fall sicheres Verhalten aussehen?
Aus der Luft- und Raumfahrt und dem Automotive-Bereich sind wir gewohnt in Redundanzen zu denken: Fällt ein System aus, hat man noch ein zweites. Das geht aber nicht immer. Wir müssen darauf achten, dass unsere Systeme, da sie nicht total ausfallsicher gemacht werden können, Resilienz aufweisen, also fehlertolerant sind. Dies sollte ein Grundsatz sein. Jeder Prozess sollte so angelegt sein, dass das Gesamtsystem - vielleicht unter Aufgabe von etwas Performanz - weiterlaufen kann.

AIRBUS ist ein europäischer Konzern, der weltweit aktiv ist. Inwieweit ist die Komplexitätsbeherrschung vernetzter CPS auf EU-Ebene zu bewältigen und welche Themen sollten eher nationale oder gar weltweite Priorität haben?
Wenn wir es geschickt anstellen, können wir uns in Europa, wie bereits erwähnt, über die Schnittstellen agil vernetzen. Gemeinsam angehen, was die gemeinsame „kritische Masse“ benötigt, individuell lösen, was individuell benötigt wird. Standards nicht zementieren, sondern möglichst offen miteinander vereinbaren. Dann kann ein CPS deutsche, französische oder andere Elemente enthalten und mit nichteuropäischen Systemen zusammenarbeiten, ohne die Sicherheit einzubüßen.

Wie viel Kooperation ist in diesen Bereichen von AIRBUS mit externen Partnern angestrebt bzw. welche Kompetenzen im Bereich CPS werden konzernintern gehalten?
Meines Erachtens bricht gerade das Zeitalter der Kooperation an. Wenn wir uns nicht zu mehr Kooperation zwingen, werden wir scheitern. Die Make-Or-Buy-/Make-Or-Partner-Entscheidungen werden immer wichtiger. Welche Kompetenzen dann „inhouse“ gesichert werden oder doppelt aufgestellt (intern und extern, also disseminativ) oder welche man nur extern pflegen und einbringen lässt, wird im Wesentlichen vom jeweiligen Geschäftsmodell abhängen. Also wenn feststeht, welche Rolle Airbus einnehmen möchte und welche Kompetenz dazu notwendig ist, nachhaltig diese Rolle auszufüllen. Um ein gutes Kaffeehaus zu führen, muss ich nicht selber Kaffee anpflanzen, aber den Aufbrühprozess, den sollte ich beherrschen.

Welche FuE-Bereiche und Themen bedürfen politischer Unterstützung, also z.B. finanzieller Unterstützung in der Grundlagenforschung, regulatorische Unterstützung oder Unterstützung in der Standardisierung?
Im Grunde alle. Nur wie im einzelnen Fall die Unter-

AIRBUS SE (europäische Aktiengesellschaft) im Überblick

Beteiligte Länder	Frankreich, Deutschland, Spanien
Produktpalette	Kommerzielle Flugzeugflotten; Helikopter; Weltraumrobotik, Raumfahrt-Module sowie Satelliten; Transport-, Missions- und Kampfflugzeuge
Hauptsitz	Toulouse, Frankreich
Standorte	Tochtergesellschaften weltweit in USA, China, Japan, Indien, im Nahen Osten
Mitarbeiter	133.700 (135 Nationalitäten)
Netzwerk	rund 7.700 Zulieferer weltweit

stützung aussieht, das variiert enorm. Manchmal reicht es, wenn die politische Seite sich nur für die Rechtssicherheit einsetzt (siehe Drohnen-Regeln), denn die Verfügbarkeit von praxisnahen Regeln schafft Raum für die Umsetzung innovativer Ideen im Geschäft. Manche Unterstützung könnte mit Abnahmegarantien erfolgen, insbesondere durch Reallabore eingeleitet (wie bei Elon Musk und seinem Space X; er hat traumhafte Abnahmegarantien von NASA und Militär). Solch ein Instrumentarium oder die Freigabe öffentlicher Beschaffungsprozesse mit einem solchen Hintergrund könnte noch einmal mehr Start-Up Geist und Venture Capital freisetzen.
Eine zeitgemäße Ausstattung von Forschungseinrichtungen und Universitäten sowie die Überprüfung der Sinnhaftigkeit von Fördermaßnahmen und Förderregularien gehört dazu. Manchmal gibt der Staat mehr Geld in die Förderung, als die Industrie, insbesondere der Mittelstand, abrufen kann. Warum nicht öfter mal vollbezahlte Technologiedemonstrationen wagen?
Und es sollte Wettbewerbsfreiheit zwischen Forschungseinrichtungen und industrieller Dienstleistung bestehen. Sehr oft wird es gerade für Mittelständler schwierig, sich gegen staatliche und halbstaatliche Großforschungseinrichtungen zu behaupten. Diese brechen oft mit ihrer Querfinanzierung in die Wertschöpfungsketten des Mittelstandes ein. Ein Konzern wie AIRBUS braucht einen stabilen, innovativen und gesunden Mittelstand. Das ist ein Standortvorteil, um den uns viele Nationen beneiden und der sehr agil sein kann.
Förderung sollte nicht pauschal erfolgen, sondern immer mit Blick auf das Ziel mit entsprechenden Instrumenten unterstützen. Eine feingliedrige Roadmap bietet dafür ein ideales Grundlagenpapier, um das Regulative, das technisch Machbare und die Verwertung der Ergebnisse in Einklang zu bringen.

Inwieweit können Netzwerke wie SafeTRANS bei der politischen Sichtbarkeit der Themen und (domänenübergreifenden) Kooperationen unterstützen?
Sehr gut. Denn der Domänenübergriff ermöglicht gemeinsames Lernen, Technologie- und Wissenstransfer und sorgt für die Bildung von Interessensgemeinschaften. Die einen haben das Knowhow, die anderen den Marktzugriff und der nächste die erforderliche Stärke, um z. B. politisches Gehör zu bekommen.

Stichwort Zukunft: Wie werden CPS im Jahr 2030 unser Leben beeinflussen? Welche Einsatzgebiete und Anwendungen würden Sie sich persönlich wünschen?
In 2030 denke ich, werden CPS noch massiver unser Leben beeinflussen. Gerade vor dem Hintergrund der aktuellen Sars-COV-2-Pandemie, werden Vernetzungen im Gesundheitswesen und zwischen den Behörden zunehmen. Der Grad an Digitalisierung wird steigen. Mobilität wird anders gesteuert werden.
Wenn ich mir etwas wünschen könnte: ein CPS-Medizinsystem, das alle Sparten so gut vernetzt, dass Krankheitsbilder schneller erfasst und analysiert werden können (mittels KI-unterstützender Anamnese), um das Altern und Leiden besser zu lindern. Und autonomer ÖPNV, flächendeckend bis zu jeder Milchkanne, sodass Mobilität und Reisen ökologisch werden, ökonomisch bleiben und wieder Spaß machen: für die Jungen erschwinglich und die Alten erträglich.

Vielen Dank für das Gespräch!

Götz Anspach von Broecker

Götz Anspach von Broecker hat 1993 sein Studium als Diplomingenieur Hochfrequenz- und Optische Nachrichtentechnik an der TU Braunschweig abgeschlossen. Seine berufliche Laufbahn begann in der Satelliten-Nachrichtentechnik und führte ihn über Stationen beim DLR und (ehemals) Bosch Telecom zu EADS in den heutigen AIRBUS-Konzern. Hier arbeitet er im Forschungs- und Entwicklungsbereich der AIRBUS Defence and Space Gruppe im Bereich AeroSpace & Defence Research Institutions and ESA Technology Programs/Research & Technology.
Neben seinen beruflichen Tätigkeiten ist Götz Anspach von Broecker Mitglied in der Expertengruppe des INNOspace Master Programms, einem vom DLR-Raumfahrtmanagement im Jahr 2015 initiierten jährlichen Ideenwettbewerb, und engagiert sich in Forschung und Lehre an Universitäten und Schulen zum Thema Weltraumtechnologie. Darüber hinaus ist er Beiratsmitglied im NFL (Niedersächsischen Forschungsprogramm Luft- und Raumfahrt).

Neues DLR-Institut „Systems Engineering für zukünftige Mobilität“

Nach der Bewilligung vom Bund in 2019 gab im Juni dieses Jahres der Senat des DLR grünes Licht für das neue Institut.

Der Verbund des Deutschen Zentrums für Luft- und Raumfahrt (DLR) bekommt Zuwachs: Ein neues Forschungsinstitut mit dem Themenschwerpunkt „Systems Engineering für zukünftige Mobilität“ wird in diesem Jahr in Oldenburg entstehen. Dafür werden der Bund und das Land Niedersachsen pro Jahr 8 Mio. Euro in den Standort Oldenburg investieren. Zudem stellt das Land 20 Mio. Euro für den Aufbau bereit. Das Institut soll aus dem heutigen Forschungsbereich Verkehr des Informatikinstituts OFFIS aufgebaut werden. Die zunächst geplanten gut 60 Wissenschaftler*innen werden primär Forschungsarbeiten zu effizienten und sicheren Systemen in der Bereichen Automobil, Schifffahrt und Bahn durchführen. Automatisierte und autonome Verkehrssysteme haben das Potenzial, einen wichtigen Beitrag zum Klimaschutz und zur Bewältigung gesellschaftlicher Herausforderungen im Bereich der Mobilität zu leisten. Themenschwerpunkte des neuen DLR-Instituts werden sein:

- Grundlagen, Methoden, Verfahren und Werkzeuge zur Steigerung und Gewährleistung der technischen Vertrauenswürdigkeit von automatisierten und autonomen Transportsystemen, inkl. Bewertungs- und Zertifizierungsmethoden für deren Zulassung sowie die Förderung von Standards
- Implementierung der Methoden in virtuellen und physischen Testfeldern
- Unterstützung der neuen Leitdisziplin „Autonomik“

Speziell die Leitdisziplin Autonomik soll helfen, das Potenzial, das die Integration von immer mehr Entscheidungskompetenz in Maschinen mit Hilfe neuer Ansätze der künstlichen Intelligenz mit sich bringt, bestmöglich zu nutzen. Die Ziele der Autonomik sind vielseitig: Neben der global angestrebten Nachhaltigkeit spielen hierbei die Vertrauenswürdigkeit, Lebensqualität und Wirtschaftlichkeit eine große Rolle. Umweltbelastungen sollen reduziert werden, indem beispielsweise die vorhandenen Verkehrssysteme effizienter genutzt werden. Es sollen Unfälle vermieden werden (Vertrauenswürdigkeit), es soll ein höherer Komfort während der Reisezeit geschaffen werden (Lebensqualität), und es sollen darüber hinaus Ressourcen geschont sowie Kosten- und Zeitaufwand reduziert werden (Wirtschaftlichkeit). Die Wissenschaft kann hier einen entscheidenden Beitrag leisten, indem sie gemeinsam mit Wirtschaft und Politik verschiedene Fachdisziplinen wie Gesellschaftswissenschaften, Psychologie, Philosophie, Human-, Natur- und Technikwissenschaften wie Physik, Mathematik und Informatik zusammenbringt. Das neue Institut wird sich gemeinsam mit Institutionen und Unternehmen aus Wissenschaft, Wirtschaft und Politik um den Aufbau entsprechender Kompetenzen im Teilgebiet der Verkehrsautonomik befassen, wodurch ein entscheidender Beitrag zur Erforschung und Entwicklung vertrauenswürdiger hochautomatisierter und autonomer Verkehrssysteme der Zukunft geleistet wird. Bis 2024 soll das Institut auf rund 80 Mitarbeiter*innen anwachsen.
„Wir arbeiten im Bereich Verkehr seit sehr vielen Jahren in diversen Forschungsprojekten eng mit dem DLR zusammen“, so Prof. Dr.-Ing. Axel Hahn, OFFIS-Vorstand. „Mit dieser nun vorgesehenen Institutionalisierung der Zusammenarbeit durch die geplante Überführung unseres OFFIS-Bereichs Verkehr in das neue DLR-Institut ‚Systems Engineering für zukünftige Mobilität‘ entsteht ein großer Mehrwert für den Wirtschafts- und Wissenschaftsstandort Deutschland.“
Das Konzept zum neuen DLR-Institut in Oldenburg wurde bereits positiv wissenschaftlich evaluiert. Der operative Start erfolgte mit dem Senatsbescheid am 23. Juni 2020. Derzeit laufen die Prozesse des Transfers des OFFIS-Verkehrsbereich in das neue Institut, sodass eine Überführung für 2021 angestrebt wird. Gemeinsam werden Prof. Dr.-Ing. Axel Hahn als Gründungsdirektor und Prof. Dr. Martin Fränzle (Carl von Ossietzky Universität Oldenburg) den weiteren Prozess verantworten.

Prof. Dr.-Ing. Axel Hahn, Gründungsdirektor des DLR-Instituts „Systems Engineering für zukünftige Mobilität“
Prof. Dr. Martin Fränzle

www.dlr.de/se

CPS on-line sicher updaten

Das nationale Projekt StepUP!CPS entwirft ein domänenübergreifendes Verfahren zur Nachweisbarkeit funktionaler Sicherheit von Systemen, die im Feld on-line aktualisiert werden.

Als ein zentrales Merkmal für die Sicherheit, Leistungsfähigkeit, Effizienz und Akzeptanz zukünftiger Cyber-Physical Systems (CPS) gehört eine modulare Updatefähigkeit - d. h., die Aktualisierung einzelner, auch sicherheitskritischer Funktionen, mit nachweislicher Erhaltung der Betriebssicherheit des Gesamtsystems. Trotz relevanter Vorarbeiten (z. B. Update-Mechanismen für nicht-sicherheitskritische Funktionen), sind bisher keine tragfähigen Konzepte für die durchgehende Absicherung von modularen Updates sicherheitskritischer Funktionen in CPS verfügbar. Daher werden im Projekt domänenübergreifende Software-Methoden und Technologien (TRL 3-4) erforscht und entwickelt, die alle Schritte zukünftiger, sicherer, modularer CPS-Update-Zyklen umfassen. Als proof-of-concept werden diese realisiert und in drei Anwendungsbereichen (Automotive, Industrie 4.0, Maritime) anhand von Use Cases evaluiert und demonstriert. .

Maritimes Fallbeispiel

Erste Ergebnisse lassen sich so am Beispiel des maritimen Anwendungsfalls aufzeigen, in dem das hochautomatisierte Assistenzsystem MTCAS (Maritime Traffic Alert and Collision Avoidance System) für die Navigation in dicht befahrenen Seegebieten an die im Projekt entwickelten Methoden und Konzepte angepasst und erweitert wird. Dabei wird untersucht, wie ein solches Assistenzsystem nach der Inbetriebnahme auf dem Schiff, z. B. zur Fehlerbehebung, aktualisiert werden kann, ohne dass eine vollständige Typprüfung des Brückensystems oder gar des entsprechenden Schiffs erneut durchgeführt werden muss. Zu diesem Zweck wird die bestehende monolithische Systemarchitektur von MTCAS funktional unterteilt und in logisch voneinander getrennte Module überführt. Die dadurch herbeigeführte Entkopplung der funktionalen Einheiten von MTCAS ermöglicht es, die in StepUP!CPS entwickelten service- und vertragsbasierten Modulkonzepte auf den maritimen Use-Case zu überführen und somit den sicheren Austausch ausgewählter Systemkomponenten zu ermöglichen. Durch die Integration von MTCAS in die maritime Technologieentwicklungsplattform eMIR (eMaritime Integrated Reference Platform) wird darüber hinaus eine vollständige Abbildung der in StepUP!CPS entwickelten Update-Mechanismen angepasst an die Anforderungen des maritimen Bereichs ermöglicht und die entwickelten Konzepte und Methoden anhand eines simulativen Fallbeispiels demonstriert.

Der Forschungsverbund besteht aus führenden Universitäten und Forschungsinstituten im Bereich der CPS-Forschung. Insgesamt sind 13 Forschungsgruppen und Lehrstühle beteiligt. Um die Sicht der Industrie aufzunehmen, ist ein Industrial Advisory Board mit Anwendern und Technologie-Providern eng ins Projekt eingebunden. Im Industrial Advisory Board agieren die Industriepartner als „Ideen-Geber“, „Konzept-Prüfer“ und zukünftige Nutzer der Projektergebnisse (mehr zu Industrial Advisory Boards siehe Seite 5). 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 liefert einen wichtigen ersten Baustein für modulare Updates von (sicherheitskritischen) CPS - einer Schlüsseltechnologie mit hoher strategischer Bedeutung für die Wettbewerbsfähigkeit und Innovationsdynamik des Hochtechnologiestandorts Deutschland.

https://stepup-cps.de/

StepUP!CPS - Übersicht

Laufzeit	10/2018 - 9/2021
Koordinator	OFFIS Institut für Informatik
Förderung	BMBF
Volumen	4.081.925 €
Fördervolumen	3.983.766 €
Partner	Carl von Ossietzky Universität Oldenburg, DLR, KIT, FZI, SafeTRANS
Anwendungen	Automotive, Maritime, Industrie 4.0

Neue Validierungsmethodik für automatisierte Fahrzeuge

Das europäische Projekt ArchitectECA2030 erforscht neuen Entwurfsrahmen für sicherheitskritische, elektronische, vernetzte Komponenten und Systeme.

Die europäischen Partner, die sich im Verbundprojekt ArchitectECA2030 (Trustable architectures with acceptable residual risk for the electric, connected and automated cars) zusammengeschlossen haben, planen einen harmonisierten europaweiten Validierungsrahmen für elektronische Komponenten und Systeme zu entwickeln, um sichere vernetzte und automatisierte Fahrzeuge zu ermöglichen (SAE L3 bis L5). Der neue Validierungsansatz soll die Zuverlässigkeit, Robustheit und Sicherheit von Systemen sowie die Rückverfolgbarkeit der Auswirkungen von Design-Entscheidungen verbessern. Schwerpunkte von ArchitectECA2030 sind ein nachvollziehbares und auf Missionen basiertes Design elektronischer Komponenten und Systeme (ECS) sowie die Quantifizierung eines akzeptierten Restrisikos von ECS, um die Typgenehmigung zu erleichtern und die Akzeptanz der Endnutzer zu erhöhen. Die Methoden umfassen automatische integrierte Sicherheitsmaßnahmen beim Entwurf elektronischer Schaltkreise, beschleunigte Tests, Restrisikoquantifizierung, virtuelle Validierung sowie multiphysikalische und stochastische Simulationen. Das Projekt wird am 1. Juli 2020 starten.

Eine unabhängige Validierung ist von grundlegender Bedeutung, um die Leistungsfähigkeit und Sicherheit moderner, vernetzter und automatisierter Fahrzeuge zu gewährleisten. Da die Software- und Hardwarekomponenten von verschiedenen Anbietern stammen und auf vielfältige Weise integriert werden, müssen die verschiedenen erforderlichen Validierungsebenen vollständig verstanden und die Integration mit Primär- und Sekundärteilen berücksichtigt werden. ArchitectECA2030 plant ein neuartiges fahrzeuginternes Überwachungsgerät zu implementieren, mit dem die Elektronik kontrolliert werden kann, um modellbasierte Sicherheitsprognosen, Fehlerdiagnosen und Anomalieerkennungen zu ermöglichen. Dafür wird ein Validierungsrahmen bereitgestellt, der harmonisierte Methoden und Werkzeuge umfasst, mit denen die Quantifizierung von Restrisiken mithilfe von Daten unterschiedlicher Quellen (z. B. Überwachungsgeräte, Sensoren/Aktuatoren, Flottenbeobachtungen) verwaltet werden kann. Ziel ist eine möglichst hohe Sicherheit und Zuverlässigkeit auf allen ECS-Entwurfsebenen. Die Berechnung des Restrisikos ermöglicht die Homologation und Typgenehmigung von ECA-Fahrzeugen (electric, connected and automated vehicles).

Dafür bringt das Projekt Interessensgruppen aus der ECS-Industrie, Normungs- und Zertifizierungsstellen (z. B. ISO, NIST, TÜV), Testfeldbetreiber, Versicherungsunternehmen und Hochschulen zusammen und kooperiert mit der ECSEL-Leuchtturminitiative Mobility.E. So können neu entstehende Normen und Validierungsverfahren für ECA-Fahrzeuge abgestimmt und mitgeprägt werden. Das Projekt wird ergänzt durch ein External Advisory Board, welches von SafeTRANS und dem Konsortialführer Infineon Technologies geleitet wird (mehr zu Advisory Boards siehe Seite 4).

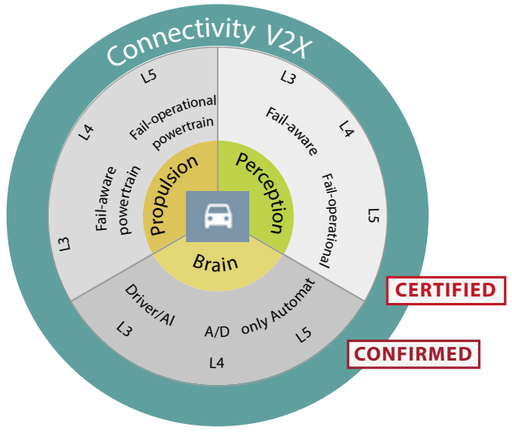


Abb. 1: Die drei Hauptkomponenten vernetzter, hochautomatisierter Fahrzeuge: Antrieb und Lenkung (Propulsion), Wahrnehmung (Perception) und Entscheidungskomponente (Brain).

ArchitectECA2030- Übersicht

Laufzeit	7/2020 - 6/2023
Koordinator	Infineon Technologies AG
Förderung	H2020-ECSEL-2019-2-RIA
Volumen	ca. 13,69 Mio €
Fördervolumen	3,9 Mio €
Partner	23 europäische Partner
Anwendungen	Automotive

„Künftige sicherheitskritische Infrastrukturen mit Elementen, die die Komplexität biologischer Systeme annehmen.“

Die SafeTRANS ACPS Days im Dezember 2019 in Berlin bildeten Plattform für den Expertenaustausch rund um die Absicherung zukünftiger CPS.

Cyber-Physical Systems entwickeln sich zu komplexen, vernetzten, digitalen Systemen, die immer häufiger auf lernender Software basieren. Vor allem branchenübergreifende Lösungen für angriffssichere (Security) und funktional sichere Systeme (Safety) werden benötigt, um die Herausforderungen der Zukunft bewältigen zu können. Daher stießen die SafeTRANS ACPS Days, die vom 11. bis 13. Dezember 2019 in Berlin stattfanden, auf großes Interesse bei Experten aus Wirtschaft, Forschung und Politik. Drei im Format unterschiedliche, sich aber thematisch auf zukünftige Autonomous Cyber-Physical Systems, kurz: ACPS, fokussierende Veranstaltungen boten einen regen Austausch und vertiefende Gespräche zu strategischen und fachlichen Themen.

Strategisches Symposium: Safety, Security, and Certifiability of Future Man-Machine Systems

Am Mittwoch, 11.12.2019, startete das Symposium “Safety, Security, and Certifiability of Future Man-Machine Systems“ in der Niedersächsischen Landesvertretung in Berlin. Hier präsentierte der von Professor Werner Damm (SafeTRANS Vorstand) und Peter Heidl (Robert Bosch GmbH) geleitete Arbeitskreis „Resiliente, lernende und evolutionäre CPS“ seine erarbeitete strategische Roadmap sowie das zugehörige Positionspapier[1] Vertretern aus Wirtschaft und Forschung sowie von einschlägigen Verbänden, um einen Prozess zur weiteren Abstimmung der Inhalte zu starten. Die Dokumente skizzieren die Entwicklung von CPS hin zu hochgradig komplexen Mensch-Maschine-Systemen und erarbeiten eine Technologie-Roadmap sowie Handlungsempfehlungen zur Absicherung des Qualitätsmerkmals „Quality Made in Germany“, damit die Sicherheit und Verfügbarkeit solcher Systeme gewährleistet werden kann und deren gesellschaftliche Akzeptanz steigt (siehe Leitartikel ab Seite 12).

Der Eröffnungsvortrag von Dr. Johannes Helbig, Managing Director Business Transformation Institute, zeigte welche weitreichenden und disruptiven Veränderungen und Möglichkeiten die digitalen Systeme hervorrufen (werden). Neben der technischen Komplexitätsbeherrschung ging der Vortrag auf ökonomische Herausforderungen ein und thematisierte die Beherrschbarkeit dieser Systeme, die zunehmend die Komplexität biologischer Systeme annehmen. Denn „[...] die Frage nach der Qualitätssicherung, ob in Tests und/oder Theorie, wird entscheidend sein für die nationale und europäische Wettbewerbsfähigkeit. Die Erforschung der zunehmend unbekannten Wirkzusammenhänge kann die Lücke schließen zwischen Können (technisch machbar), Wollen (ethisch vertretbar) und Dürfen (beherrschbar, verstanden, zertifizierbar) [...]“ so Johannes Helbig weiter. Die Grundlage für anregende Diskussionen war auch durch die weiteren Vorträge von Prof. Werner Damm, Peter Heidl und Bernhard Evers (Siemens) gelegt.

Professor Peter Liggesmeyer (Insitutsleiter Fraunhofer IESE) stellte Verfahren und Vorgehensweisen für ein digitales Risk-Mangement vor und Frau Professorin Katharina Seifert (Direktorin Institut für Verkehrssystemtechnik, DLR) legte den Schwerpunkt ihrer Ausführungen auf den Straßenverkehr der Zukunft und gab Einblicke in Forschungsarbeiten des DLR zum autonomen Straßenverkehr.

Prof. Dr. Werner Damm (SafeTRANS) führt in der Begrüßung in das Thema ein (oben). Dr. Johannes Helbig gibt Einblicke aus wirtschaftlicher Sicht zum Einsatz zukünftiger CPS.

In der abschließenden Podiumsdiskussion mit allen Referenten sowie Vertretern von den Verbänden BITKOM und ZVEI wurde die Notwendigkeit einer intensiven nationalen und europäischen Forschung deutlich, um Deutschland und die EU als Wirtschaftsstandort für CPS der Zukunft auszubauen, da die Beherrschbarkeit großer, komplexer, vernetzter und vor allem sicherheitsrelevanter Systeme, noch nicht von außereuropäischen Unternehmen besetzt ist und sich die einmalige Chance bietet, das Label „Quality Made in Germany/Europe“ in die digitale Ökonomie zu übertragen.

Fachsymposium: 26. Industrial Day zu KI

Am 12.12.2019 schloss sich der 26. SafeTRANS Industrial Day in Kooperation mit der IAV GmbH an. Der thematische Schwerpunkt des Fachsymposiums lag auf „Künstliche Intelligenz in Cyber-Physical Systems: Einsatzmöglichkeiten, Skalierbarkeit, Erklärbarkeit, Sicherheitsnachweis“.

Damit knüpfte der Industrial Day an die Ergebnisse des Symposiums zu zukünftigen Mensch-Maschine-Systemen am Vortag an und stellte den Praxisbezug durch aktuelle Fragestellungen und Forschungseinblicke her.

Die Fachvorträge des Industrial Days thematisierten Anwendungsmöglichkeiten für KI in CPS als auch im Entwicklungsprozess, Standardisierungsaktivitäten für zertifizierbare KI und beleuchten Möglichkeiten und Grenzen von KI-Algorithmen in sicherheitskritischen CPS.

Prof. Dr. Philipp Slusallek (DFKI) im Podiumsgespräch, u. a. mit Prof. Dr. Martin Fränzle (Universität Oldenburg) (oben). Blick in den ausgebuchten Vortragsraum (unten).

Professor Philipp Slusallek (DFKI) hob die Vorteile von KI heraus und verdeutlichte an Beispielen, inwiefern KI hilft, KI zu trainieren. Dabei solle KI in der Lage sein, eine eigene Risikobewertung vorzunehmen, was u. a. die systeminterne Bewertung aufgenommener Daten einschließt.

Weitere Themen während des Industrial Days bezogen sich auf trainierte und selbstlernende SW (Prof. Dr. Martin Fränzle), Machine Learning Frameworks (Sara Bertram), Sicherheitsnachweise (Dr. Daniel Schneider), selbstverifizierende CPS (Prof. Christoph Lüth), einen trainierten Software-Agenten zur autonomen Navigation hinsichtlich Kollisionsvermeidung und Pfadverfolgung (Florian Thaler) sowie User Monitoring beim autonomen Fahren (Prof. Dr. Achim Rettberg). Eine Demonstration individueller Anpassung im Automobil durch die IAV GmbH rundete die Veranstaltung ab.

Workshop des Arbeitskreises PMT4S&S

Der Arbeitskreises „Branchenübergreifende Prozesse, Methoden und Technologien für Safety und Security hochautomatisierter Systeme“, kurz: PMT4S&S, traf sich zum Abschluss der SafeTRANS ACPS Days am 13.12.2019 zu seinem dritten Workshop.

Der von Martin Rothfelder (Siemens) und Dirk Geyer (AVL Software and Functions) geleitete Arbeitskreis beschreibt Forschungsfelder für Prozesse und Methoden zu Entwicklung, Test und Absicherung zukünftiger, hochkomplexer ACPS unter Einhaltung höchster Qualitätsstandards. Damit konkretisiert der Arbeitskreis die in der Roadmap „Safety, Security, and Certifiability of Future Man-Machine Systems“ dargestellte Komplexitätsdimension „Integrity and Certification“ hinsichtlich benötigter Technologien (siehe Leitartikel ab Seite 12).

Informationen zum AK PMT4S&S sind auf folgender Webseite zu finden:
www.safetrans-de.org/de/Aktivitaeten/Roadmapping_AKs_2018.php

[1] Safety, Security, and Certifiability of Future Man-Machine Systems. SafeTRANS (Hrsg.) Roadmap/Positionspapier. 2019

Sicherheit für automatisiertes und vernetztes Fahren

TÜV NORD Mobilität - IFM bietet ganzheitliche Beratungs- und Prüfdienstleistungen zu neuen Sicherheitsstandards der Automobilindustrie und künftigen Vorschriften zur Fahrzeugtypgenehmigung.

Innovationen im Umfeld zukünftiger Mobilität, wie das elektrifizierte, automatisierte und vernetzte Fahren, haben maßgeblichen Einfluss auf die im Fahrzeug eingesetzten Technologien und die E/E-Architektur. Darüber hinaus ergeben sich neue Herausforderungen an die Fahrzeugsicherheit. Neben der Entwicklung technischer Innovationen steht die Automobilindustrie daher vor der Aufgabe, die bestehende Prozesslandschaft um ein ganzheitliches Sicherheitsmanagement zu erweitern. Künftige Vorschriften zur Typgenehmigung werden neben der Prüfung durch die Hersteller, eine unabhängige Bewertung des Sicherheitsmanagements und der Wirksamkeit der umgesetzten Sicherheitsmaßnahmen erforderlich machen.

Functional Safety

Mit dem mittlerweile etablierten Sicherheitsstandard ISO 26262 zur Funktionalen Sicherheit hat die Automobilindustrie einen Prozess und Methoden eingeführt, mit denen das Management von Sicherheitsrisiken in der Entwicklung, Produktion, Betrieb und Wartung adressiert wird. Dabei befasst sich die ISO 26262 in erster Linie mit potenziellen Gefährdungen, die aufgrund von systematischen Fehlern in der Entwicklung von E/E-Systemen und zufälligen Hardware-Ausfällen im Betrieb auftreten können.
Durch Implementierung eines funktionalen und technischen Sicherheitskonzepts müssen Systemausfälle beherrscht werden und Gefährdungen, wie beispielsweise eine ungewollte Fahrzeugbeschleunigung beim elektronischen Gaspedal, verhindert werden.

Safety Of The Intented Functionality

Neben den in der ISO 26262 adressierten Ursachen für Fehlfunktionen im Fahrzeug können weitere Ereignisse zu einem Fehlverhalten der Fahrzeugsysteme führen.
Insbesondere bei automatisierten Fahrfunktionen, die auf komplexen Systemen zur Umfelderkennung und Algorithmen zur Fahrplanung basieren, können externe Ereignisse zu einem Fehlverhalten des Fahrzeugs führen, ohne dass ein systematischer Fehler oder Ausfall im E/E-System auftritt. Ein einfaches Beispiel ist die Detektion von Hindernissen mittels einer Kamera und der darauf basierende Eingriff des Systems in die Fahrdynamik. So können Gefährdungen beispielsweise auftreten, wenn Hindernisse aufgrund der Umgebungsbedingungen nicht rechtzeitig erkannt oder fehlerhaft klassifiziert werden. Die Auswirkung könnte ein ungewünschtes Notbremsen oder Ausweichen des Fahrzeugs sein, ohne dass hierfür eine situativ bedingte Ursache vorliegt. Das System muss daher mit hinreichender Performanz konzipiert werden, um ein sicheres Verhalten in der großen Menge möglicher Ereignisse und Situationen aufzuweisen.
Mit dem Sicherheitsstandard ISO 21448 wird aktuell ein prozessualer Leitfaden entwickelt, um die beabsichtige Systemfunktion, realisiert durch den Einsatz komplexer Fahrzeugsysteme zur Objekterkennung und Fahrsteuerung sicherzustellen. Neben der Identifikation von Sicherheitsrisiken und den auslösenden Ereignissen, ist eine geeignete V&V-Strategie zentraler Bestandteil für die Systemabsicherung und die Argumentation eines validen Sicherheitsnachweises.

Cyber Security

Durch die zunehmende Vernetzung der Fahrzeugsysteme untereinander und die Vernetzung der Fahrzeuge mit der Umwelt, besteht zusätzliches Gefährdungspotenzial durch eine Kompromittierung der Informationssicherheit. Durch unberechtigte Manipulationen an Fahrzeugsystemen können zum Beispiel die Betriebssicherheit oder auch die Privatsphäre von Personen beeinträchtigt werden.
Mit der ISO/SAE 21434 wird aktuell ein prozessualer Leitfaden entwickelt, um Cyber Security im Fahrzeug in geeigneter Form zu adressieren. Auf Basis eines risikobasierten Ansatzes sind Gefährdungspotenziale zu identifizieren und hinreichende Maßnahmen in der Entwicklung und im Betrieb von Fahrzeugen umzusetzen.
Mit dem aktuellen UN ECE Regelungsentwurf zur Prüfung der Cyber Security im Rahmen künftiger Fahrzeugtypgenehmigungen, bestehen Anforderungen an die Prüfung der herstellerseitig implementierten Cyber Security Management Systeme und der Anwendung der Maßnahmen in der Fahrzeugentwicklung.

Software Updates

Komplexe, software-basierte Fahrzeugfunktionen sind ohne Software Updates nur schwer denkbar. Somit muss das Management von Software Updates den kompletten Lebenszyklus von der Entwicklung über die Produktion, bis zur Außerbetriebnahme von Fahrzeugtypen abdecken. Funktionale Korrekturen aufgrund von Kundenbeanstandungen oder identifizierten Safety- oder Security-Risiken können dann über Software Updates in die Fahrzeuge im Feld ausgerollt werden.
Mit dem aktuell in Entwicklung befindlichen Standard ISO/AWI 24089 soll ein Leitfaden für das Software Engineering in Fahrzeugen entstehen. Mit dem UN ECE Regelungsentwurf zu Software Updates in Fahrzeugen werden zudem Genehmigungsanforderungen für die Software Update Management Systeme der Hersteller und zum Umgang mit Software Updates für Fahrzeuge entwickelt.

Kompetente Beratung und maßgeschneiderte Dienstleistungen

Das Fachgebiet Automotive Electronics von TÜV NORD Mobilität - IFM richtet seine Tätigkeitsschwerpunkte und Dienstleistungen an den Sicherheitsstandards für komplexe E/E-Systeme und den Typgenehmigungsvorschriften für das automatisierte und vernetzte Fahren aus.
Die Mitarbeiter engagieren sich daher sowohl in der Entwicklung von Sicherheitsstandards, als auch in der Entwicklung der UN ECE Regelung. Durch Forschungsaktivitäten und Kundenprojekte der vergangenen Jahre bestehen bereits heute praxisorientierte Erfahrungen und validierte Lösungen zur Implementierung und Anwendung der Standards und Vorschriften.
Somit sieht sich das IFM mit kundenspezifischen Trainings, Beratungs- und Prüfdienstleistungen zu den Themen Funktionale Sicherheit und SOTIF, Cyber Security und Software Updates als Wegbereiter und kompetenter Partner für die Einführung innovativer Fahrzeugtechnologien und Funktionen des automatisierten und vernetzten Fahrens.
www.tuev-nord.de

TÜV NORD Mobilität

SHORTCUTS: TÜV NORD Mobilität - IFM

Unternehmen:	TÜV Nord Group
Sitz:	Hannover
Geschäftsfelder:	Mobilität, Industrie Service, Engineering und Rohstoffe, Bildung, Aerospace, IT
Gründungsjahr:	1869
Mitarbeiter:	12.235 (2019)
Niederlassungen:	In mehr als 70 Ländern

Heiko Ehrich, Head of Department Automotive Electronics, zu neuen Standards:

Aus Sicht des Prüfdienstleisters TÜV NORD, wie bewerten Sie den Aufbau der neuen Standards im Bereich SOTIF und Cyber Security: Vereinfachen diese das Vorgehen für Hersteller und Zulieferer oder gehen damit teilweise auch Einschränkungen bei der Entwicklung einher?
Hersteller müssen das erforderliche Maß an Sicherheit ihrer Produkte gewährleisten. Hierzu sind sämtliche Ursachen möglicher Sicherheitsgefährdungen zu identifizieren und mit der notwendigen Angemessenheit zu behandeln. Durch die Automatisierung und Vernetzung von Fahrzeugen besteht eine zwingende Notwendigkeit die bestehende Prozesslandschaft für das Sicherheitsmanagement zu erweitern. Mit den neuen Sicherheitsstandards zu SOTIF und Cybersecurity entstehen aktuell Regelwerke, die eine solide Grundlage hierzu bilden können. Die Normen stellen somit keine Einschränkung für die Hersteller dar, vielmehr schaffen diese Möglichkeiten für die Entwicklung und Einführung von automatisierten und vernetzten Fahrzeugen.

Welche Herausforderungen sehen Sie als Mobilitätsdienstleister bei der Zulassung aufgrund des immensen Einsatzes von IT- und SW-Lösungen?
Durch den Einsatz von Software-basierten Lösungen in die Fahrzeugtechnik, speziell in den Innovationsbereichen automatisiertes und vernetztes Fahren, werden die Entwicklungsprozesse zunehmend agiler und iterativer. Zudem werden die eingesetzten Softwarefunktionen im Lebenszyklus eines Fahrzeugs an die veränderlichen Umweltbedingungen anzupassen sein. Künftige Genehmigungsprozesse müssen daher angepasst werden, um eine fortlaufende Produktveränderung im Betrieb zu ermöglichen.

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 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.ics-gmbh.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