In den vergangenen Phasen der Entwicklung von E/E-Systemen in den Branchen des Transportwesens hat sich zunehmend die Frage nach den Auswirkungen und der Behandlung von möglichen Fehlfunktionen gestellt, welche durch Lösungen nach jeweiligem Stand der Technik beantwortet wurde. Die Industrie der verschiedenen Bereiche hat reagiert und durch die Einführung und Umsetzung von Sicherheitsstandards, wie beispielsweise DO178, EN5012x und ISO26262, die normative Basis der anzuwendenden Prozesse, Methoden und Technologien geschaffen. Die Herausforderung in der Entwicklung von hochautomatisierten bis autonomen Systemen wird es sein, mit der notwendigen Absicherung immer stärker verteilter und vernetzter Systeme und Komponenten Schritt zu halten. Dabei ist auch die Gewährleistung der Datensicherheit immer wichtiger. Parallel dazu werden die zugrundeliegenden Algorithmen vielschichtiger und dynamischer. So werden in künftigen Systemen nicht nur die Zykluszeiten der Entwicklungsabläufe vor SOP immer kürzer, sondern Funktionen werden durch lernende Systeme sogar zur Laufzeit adaptiert. Daher fokussiert sich der SafeTRANS-Arbeitskreis „Branchenübergreifende Prozesse, Methoden und Technologien für Safety und Security hochautomatisierter Systeme“ darauf, Handlungsempfehlungen zur Berücksichtigung und Bewältigung der oben genannten Herausforderungen zu erarbeiten.

Dirk Geyer
Head of Product Segment Safety & Security
AVL Software and Functions GmbH

SafeTRANS
SAFETY IN TRANSPORTATION SYSTEMS

NEWS

SafeTRANS News 1/2018

Herausforderungen in Test und Zertifizierung zukünftiger E/E-Systeme und CPS

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
Dr. Lothar Borrmann, 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:
AVL Software and Functions GmbH, AVL LIST GmbH, DLR, Fotolia, INGenX Technologies GmbH, SafeTRANS, TTTech

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

Ausgabe:
SafeTRANS News 1/2018 werden im August 2018 veröffentlicht und kostenlos abgegeben.

SafeTRANS News 1/2018

Autonome und lernende CPS 4
Ein Überblick über nationale und europäische Forschungs- und Entwicklungsaktivitäten gibt den Status-quo wider und beschreibt zukünftige FuE-Themen.

Interview: „Schon sehr früh im Projekt erste Demonstratoren aufzusetzen hat sich als wirklich positiv erwiesen.“ 9
Dr. Andrea Leitner, AVL List, über Testmethodiken hochautomatisierter Systeme, den Praxisbezug von Forschung und das Management eines großen europäischen FuE-Projektes.

H2020 project SEPHY implements innovative technologies to realize ITAR-free physical layer transceiver 12
Über das EU-Forschungsprojekt SEPHY

***Safety of the intented Function* und eine gemeinsame Sprache für Safety und Security im Entwicklungsprozess** 16
Rückblick: 24. SafeTRANS Industrial Day und Gründung des Arbeitskreises „Prozesse, Methoden und Technologien für Safety und Security hochautomatisierter Systeme“

Autonomes Fahren erfordert neue, angemessene Entwicklungsmethoden für komplexe Systeme und Funktionen 18
SafeTRANS-Mitglied: INGenX Technologies GmbH

Autonome und lernende Cyber-Physical Systems (ACPS): Herausforderungen in Entwicklung, Test und Zertifizierung

Der folgende Überblick über nationale und europäische Forschungs- und Entwicklungsaktivitäten gibt den Status-quo wider und greift zukünftige Themen auf.

Die Automatisierung nimmt Fahrt auf! Industrielle und alltägliche Produkte werden zunehmend intelligent (Stichwort: „lernende“ Systeme), passen sich dynamisch an ihre Umwelt an und sind untereinander und/oder mit der physischen Welt vernetzt. Bereits heute führen hochautomatisierte und autonome Cyber-Physical Systems (ACPS) eine Vielzahl von sicherheitskritischen Steuerungsfunktionen in nahezu allen Industriezweigen aus und werden stetig weiterentwickelt. Um nur drei Beispiele zu nennen: Biomediziner erarbeiten, wie Sensoren, Mikro- und Messsysteme verbessert werden können für die automatisierte Erfassung und Verarbeitung von Messdaten, um die Effizienz und Qualität von Diagnose- und Behandlungsprozessen deutlich zu steigern.
In der Energiewirtschaft sind Stromeffizienz und Netzsicherheit wichtige Kriterien für einen Netzausbau, der auf unterschiedlichen Energiequellen basiert. Elektrizität soll so verlustfrei wie möglich erzeugt, transportiert und variabel ins Netz eingespeist und abgenommen werden. Heute gibt es kaum noch Kraftwerke und Netzanlagen ohne Prozessautomatisierungs- und Informationstechnologie. Auch im automobilen Verkehr sind Fahrerassistenzsysteme (FAS) nicht mehr wegzudenken. Derzeit in Serie sind FAS in stark regulierten Bereichen, wie auf Autobahnen, doch der Einsatz von unterstützenden Systemen und Funktionen in komplexeren Situationen steht vor der Einführung. Die FAS ebnen den Weg zum automatisierten bzw. autonomen Fahren.

In den genannten Bereichen verspricht die Automatisierung Abläufe sicherer, effizienter, wirtschaftlicher und komfortabler zu machen - und damit „die Welt ein bisschen besser“.

ACPS - technologische Grundlage

Für die (Hoch-)Automatisierung sind ACPS, welche die digitale mit der physikalischen Welt verbinden, unersetzlich. Die Herausforderungen im Bereich zukünftiger, vor allem sicherheitskritischer ACPS liegen u. a. in einer effizienten und effektiven Entwicklung und stellen Forscher und Entwickler derzeit vor viele Fragen. Die Zusammenführung verschiedenster Daten aus unterschiedlichen Quellen und Werkzeugen sowie das Testen und die Zertifizierung benötigen weitere Anstrengungen. Am Beispiel der Absicherung von hochautomatisierten Fahrfunktionen soll der Stand der Wissenschaft nationaler und europäischer Verbundprojekte für Testen und Zertifizierung von ACPS dargelegt werden.

Wege zu autonomen, lernenden Systemen

Die Automatisierung von Fahrfunktionen erfolgt in Ausbaustufen, die sich an dem sogenannten SAE Levels of Driving Automation orientieren (siehe Abb. 1). Dabei gilt: je höher der Automatisierungsgrad, umso mehr ACPS-Technologie kommt zum Einsatz.

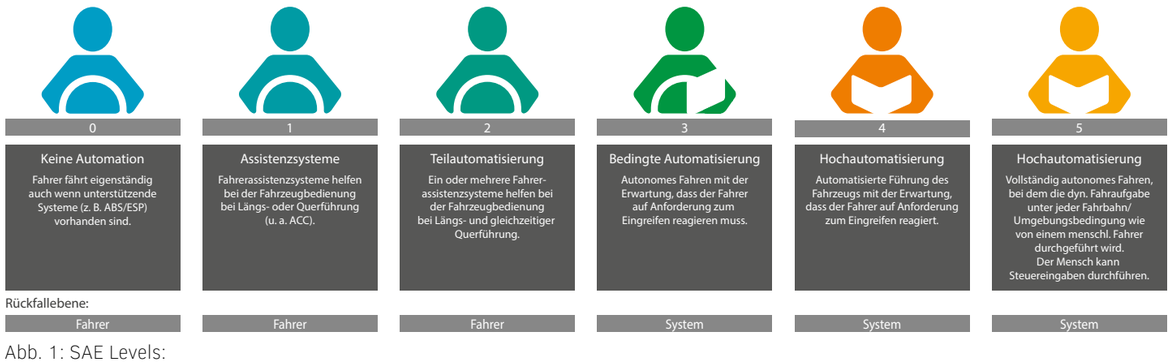

Abb. 1: SAE Levels:
Klassifizierung für Kraftfahrzeuge mit Systemen zum autonomen Fahren

Damit Nutzer ein gerechtfertigtes Vertrauen in die Systeme entwickeln, muss die Sicherheit gewährleistet sein. Dabei sind sowohl die Funktions- als auch die Datensicherheit zwei entscheidende Kriterien. Doch wie können die Systeme in sicherer Umgebung umfassend getestet und geprüft werden und das mit vertretbarem Aufwand? Die vielfältigen Situationen, in denen automatisierte Systeme passende Entscheidungen treffen sollen, sind oft extrem komplex und nicht explizit vorhersagbar.
Es müssen neue und möglichst einheitliche Qualitätsstandards und Methoden entwickelt werden, damit hochautomatisierte Funktionen rechtlich zugelassen werden können, das Nutzervertrauen erlangen und in Serien Anwendung finden. Es gilt nachzuweisen, dass das automatisierte Fahrzeug wenig bis keine Unfälle verursacht – zumindest weniger als ein Mensch – und dennoch effektiv fährt.
Dazu entwickeln Forscher aus Industrie und Wissenschaft in verschiedenen Projekten eine integrierte Betrachtung der Entwicklungs-, Test- und Betriebsphasen von ACPS entlang ihres gesamten Lebenszykluses. Dieser sogenannte DevOps-Ansatz für sicherheitskritische Funktionen umfasst die ACPS-Entwicklung (Development) und die Überwachung im laufenden Betrieb (Operations) (siehe Abb. 2). Ursprünglich stammt dieser Ansatz aus dem Software-Engineering und dient dazu, Erfahrungen aus dem Betrieb zurück in die (Weiter-)Entwicklung des Systems zu integrieren. Genau das ist ein Vorteil des DevOps-Zyklus für ACPS: die Einbindung des Systemverhaltens im Feld (einschließlich etwaiger Fehlverhalten und kritischer Situationen) in den Entwicklungs- und Verbesserungsprozess. Er erlaubt eine Rückkopplung von Entwicklung, Test und Anpassung/Updates der Systeme, um letztlich die Entwicklungszyklen zu verkürzen, die Häufigkeit von Aktualisierungen zu erhöhen und zuverlässigere Releases zu erreichen - unter Berücksichtigung von Sicherheit, Variantenmanagement, V&V-Automatisierung, Zertifizierung, Einsatz sowie Überwachung und Diagnose vor Ort.
Verschiedene nationale und europäische FuE-Verbundprojekte widmen sich Entwicklung und Test entlang der DevOps-Methodik. Die Forschungsschwerpunkte der Projekte bauen teilweise aufeinander auf und/oder ergänzen sich. Im Folgenden werden gezielt Schwerpunkte wichtiger Projekte kurz erklärt und in den übergeordneten DevOps-Zyklus eingeordnet.

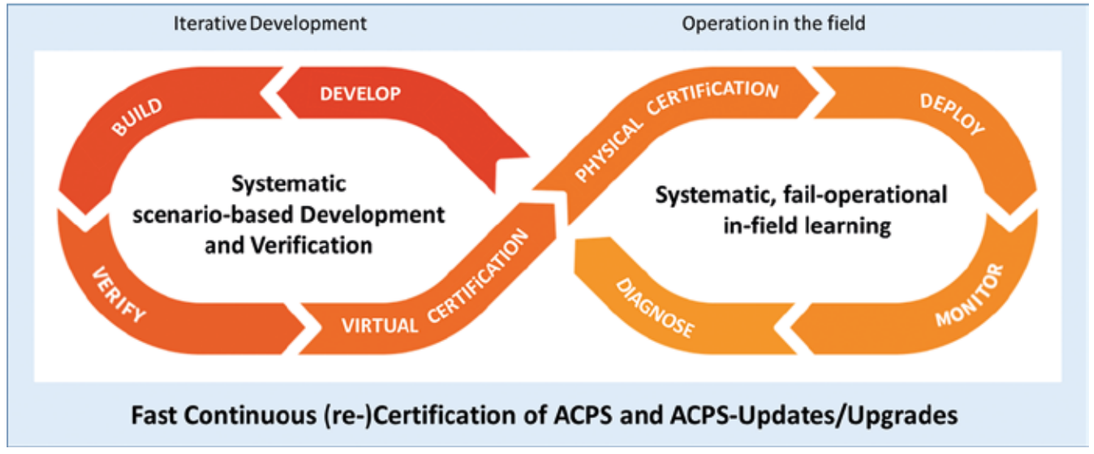

Abb. 2: DevOps-Entwicklungszyklus

Virtuelle Simulation

Teile des gesamten aus acht Phasen bestehenden DevOps-Zyklus (siehe Abb. 2) umfassen die Verifikation und Validierung von ACPS-Funktionen, einschließlich Testen. Klassische Testansätze im Bereich des autonomen Fahrens sind aufgrund der enormen Komplexität von Verkehrssituationen nicht praktikabel, teuer und teilweise gefährlich. Es müssten Milliarden von realen Testkilometern bei jedem Freigabezyklus absolviert werden, sodass es erklärtes Ziel ist, so viele physikalische Tests wie möglich von der realen in die virtuelle Welt der Simulation zu verlagern. Bei der virtuellen Simulation wird die Funktion in eine möglichst realistische, rechnergestützte Simulationsumgebung eingebaut, in der das System die riesige Anzahl von Testkilometern „abfährt“ (Model-, Software-, Hardware-, Vehicle-in-the-Loop). So können die erforderlichen Sicherheitsniveaus durch den Einsatz von szenarienbasierten, virtuellen V&V-Methoden und -Tools nachgewiesen werden. Die Überführung von Verkehrsszenarien und Tests in eine virtuelle Simulation (inkl. V & V) ist u. a. ein Bestandteil des EU-Verbundprojektes ENABLE-S3 (www.enable-s3.eu, siehe auch Interview mit Dr. Andrea Leitner, Projektkoordinatorin ENABLE-S3, ab Seite 9).

In ENABLE-S3 arbeiten 68 europäische Partner aus Industrie und Wissenschaft daran, die heutige kostenintensive Verifizierung und Validierung (V&V) durch fortschrittliche und effiziente Methoden zu ersetzen, um den Weg für die Kommerzialisierung von ACPS zu ebnen. Reine Simulation kann die Physik aufgrund ihrer Einschränkungen bei der Modellierung und Berechnung nicht im Detail abdecken. ENABLE-S3 zielt darauf ab, die beiden Welten optimal miteinander zu verbinden.

Ein besonders interessanter Teilbereich des Projektes ist die Validierung des Systems in eher kritischen Verkehrsszenarien. Dafür müssen die Validierungsplattform und die genutzten Modelle selbst validiert sein. Die Projektpartner erarbeiten eine erste Validierung der Simulationsplattform für das autonome Linksabbiegen. Als Grundlage für die rechnergestützte Simulation werden verschiedene Modelle virtuell erstellt:

- ein Fahrzeugmodell
- ein Modell des optischen Abstands und der Geschwindigkeit (Lidar)
- ein Fahrzeug-Umgebungsmodell
- ein GPS Modell
- ein Sensoren-Modell
- ein Lenkungsmodell
- ein 3D-Umgebungsmodell

Liegt eine rechnergestützte Simulation des Szenarios vor, vergleichen die Forscher die V&V-Ergebnisse des „Systems under Test“ (SuT) im Simulator und in realen Feldversuchen anhand definierter „Key Performance Indicators“ (KPIs):

Human KPIs	Description
Comfort_driver	How comfortable did the test divers feel when turning?
Feel_safe	Did the driver feel safe?
Time_to_confirm	Meantime between action request until button for release is pressed.
... and more	

System KPIs	Description
stops	Number of times the car stopped on intersection
travel_time	Time spent on intersection
v_at_entry	Velocity when entering the intersection
v_at_exit	Velocity when exiting the intersection
α_at_exit	Distance to lane center at exiting intersection
... and more	

Mit Hilfe der virtuellen Modelle und KPIs werden die in der Realität abgefahren verschiedenen Szenarien anschließend rechnergestützt simuliert. Den Aufbau eines Feldversuchs und der Simulation zeigt beispielhaft Abb. 3 [1].

Ist die Validierungsplattform validiert, können durch virtuelles Testen schon im Entwurfsstadium Funktionen von ACPS effizient, schnell und sicher überprüft und angepasst werden.

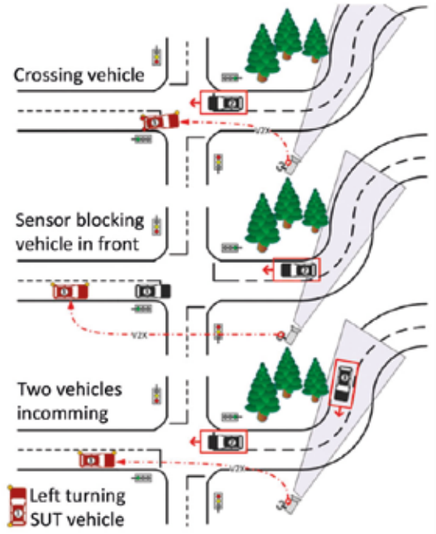

Abb. 3: Adressierte Szenarien nach ENABLE-S3

Entwicklung von Testszenarien

Beim virtuellen Testen werden die Systeme/Funktionen gegen sogenannte Szenarien getestet. Die Entwicklung von Szenarienkatalogen ist u. a. ein Schwerpunkt im nationalen Verbundprojekt PEGASUS (*www.pegasus-projekt.info*). Übergeordnetes Ziel von PEGASUS ist es, ein Vorgehen für das Testen automatisierter Fahrfunktionen zu entwickeln, um so die rasche Einführung des automatisierten Fahrens in der Praxis zu ermöglichen. Für den szenarienbasierten Ansatz entwickeln die Projektpartner relevante verkehrliche Situationen bzw. Szenarien, die einerseits diskrete Abläufe beschreiben, z. B. die einzelnen Zustände bei einem Überholmanöver, und andererseits diskrete und kontinuierliche Parameter mit Angabe von Auftrittswahrscheinlichkeiten enthalten. Die Szenarienkataloge dienen als Grundlage für eine Menge von konkreten Testabläufen und bestehen aus

- funktionalen Verifikationsprozessen (z. B. ISO 26262 für Automotive),
- Sicherheits- und Sicherheitsprozesse (z. B. ISO PAS 21448 / SOTIF (Automobil), ISO 21434 (Automobil)) und
- real aufgezeichneten Szenarien .

Die Absicherung von Fahrfunktionen wird im Projekt am Beispiel eines automatisierten Autobahnchauffeurs betrachtet (Automation des SAE-Levels 3). Das automatisierte System wird in einem Ego-Fahrzeug untersucht, das in eine potenziell kritische Situation gebracht wird, auf die das System entsprechend reagieren soll. Anhand der diversen Szenarienkataloge, die sich in verschiedene Kategorien einordnen lassen, werden Risikointegrale erstellt. Die Testspezifikation für die Fahrfunktion erfolgt verzahnt mit dem Testprozess, um die Systemauswirkungen möglichst variabel und realitätsnah zu gestalten. Aufgrund der Vielzahl der notwendigen Tests wird in PEGASUS weitgehend auf eine rechnergestützte Simulation gesetzt, d. h., die Fahrfunktion wird in einer virtuellen Umgebung getestet (siehe Erläuterungen zur Virtuellen Simulation). Regiert das System zeitlich wie auch situativ korrekt? Wie hoch ist die Wahrscheinlichkeit, dass Fehler auftreten? Diese Fragen werden mit dem PEGASUS-Ansatz beantwortet. Allerdings ist es derzeit nicht möglich, die Risikoermittlung durch szenarienbasiertes Testen automatisiert durchzuführen, da zum einen keine vollständige Spezifikation für alle möglichen in der Realität auftretenden Situationen vorliegt und zum anderen für eine Risikoermittlung Informationen über die Häufigkeiten und Szenarienausprägungen in der Realität fehlen. Daher wird die Auftrittshäufigkeit für die Fälle ermittelt, in denen die Funktion die Sicherheit in genau diesem Szenario nicht gewährleisten kann. Dies deckt aber nur eine kleine Anzahl an Situationen ab [2].

Ein Vorteil des in PEGASUS verfolgten szenarienbasierten Ansatzes ist, dass er auf andere Anwendungsfälle übertragen und erweitert werden kann und damit einen Weg aufzeigt, um drängende Probleme in der Absicherung automatisierter Fahrfunktionen anzugehen.

Entwicklung und Verbesserung von Testmethoden in Testzentren

Um die beschriebenen virtuellen, simulationsbasierten Testmethoden entwickeln zu können, ist die Übertragung der gegenständlichen Welt mit ihren physikalischen Bedingungen in die virtuelle Welt nötig. Dies geschieht vorrangig oder in Kooperation mit speziellen Testzentren. Häufig sind die Areale als Großforschungsanlagen angelegt, die neben realen Teststrecken - sie bestehen zum Teil aus öffentlichen und privaten Teststrecken - ein weites Spektrum der Verkehrsforschung abdecken, z B. mit entsprechenden Testfahrzeugen, Datensammel-, Auswertungs- bzw. Interpretationswerkzeugen, Simulationsanlagen, geschultem Personal, etc. In Deutschland ist u. a. die Großforschungsanlage „Anwendungsplattform Intelligente Mobilität“, kurz: AIM, sowie in Erweiterung des Braunschweiger Umfelds das Testfeld Niedersachsen mit Unterstützung des Bundes, des Landes Niedersachsen und der Stadt Braunschweig entstanden (siehe z. B. SafeTRANS News 2/2017, Seiten 6 und 10). In Österreich wird im ALP.Lab in der Steiermark automatisiertes Fahren er-

probt (siehe SafeTRANS News 2/2017, Seite 20). Die Testzentren ermöglichen neue Testmethoden zu entwickeln, zu prüfen und letztlich auch ACPS-Funktionalitäten zu testen. Sie schaffen einmalige Bedingungen, um Funktionen im realen Verkehr sowie in der Simulation zu prüfen und Know-how an einem Standpunkt zu bündeln. Oft sind die Testzentren in nationale und europäische FuE-Projekte eingebunden.

The way forwad: Themen zukünftiger Projekte

Die beschriebenen Entwicklungen bedingen sich gegenseitig: Testszenarien sind eine wichtige Grundlage für das virtuelle Testen basierend auf Simulationen und Testzentren helfen die Entwicklungs- und Testprozesse kontinuierlich weiterzuentwickeln durch ihre hochkarätige Ausstattung.
Aus den verschiedenen und ineinandergreifenden Ansätzen sowie der Komplexität des Themenfeldes ergeben sich weitere Forschungsfragen und Schwerpunkte im DevOps-Zyklus. In der Roadmap „Hochautomatisierte Systeme: Testen, Safety und Entwicklungsprozesse“ (Hrsg. SafeTRANS, 2017) wurde u. a. die Update-Fähigkeit im Betrieb von ACPS als Forschungsschwerpunkt identifiziert. Ein nationales Projekt, das sich aktuell in der Antragsphase befindet, greift dieses Thema auf. Andere Schwerpunkte in geplanten europäischen Projekten betreffen die Funktions- und Datensicherheit sowie den Datenschutz speziell im Automobilbereich bzw. das Testen, Validieren und Zertifizieren von ACPS in verschiedenen Anwendungsdomänen unter besonderer Berücksichtigung von künstlicher Intelligenz.
Mit Hilfe koordinierter Roadmapping-Prozesse werden Themen und Projekte auf nationaler und europäischer Ebene abgestimmt, angestoßen und initiiert. Für weitere FuE-Themen erarbeitet SafeTRANS aktuell in zwei Arbeitskreisen Forschungsroadmaps zu den Themen „Branchenübergreifende Prozesse, Methoden und Technologien für Safety und Security hochautomatisierter Systeme“ (kurz: AK PMT4S&SS) sowie „Resiliente, evolutionäre und lernende CPS“ (kurz: AK REL-CPS, mehr zu den SafeTRANS Arbeitskreisen unter: *www.safetrans-de.org*). Ziele der Arbeitskreise umfassen die Entwicklung von forschungsstrategischen Leitlinien an der sich Wissenschaft, Industrie und Politik bei Weiterentwicklungen von ACPS orientieren können sowie die Überführung der erarbeiteten Ergebnisse in Normungsgremien und Weiterführung der Handlungsempfehlungen.
Neben Unterstützung in den genannten Forschungsbereichen engagiert sich SafeTRANS auf methodischer Ebene für die Interoperabilität von Entwicklungswerkzeugen für ACPS. Dafür ist SafeTRANS u. a. im ICF, dem IOS Cooperation Forum innerhalb von ARTEMIS-IA, aktiv (mehr zur IOS und dem ICF siehe SafeTRANS News 1/2017), denn leistungsfähige Simulationswerkzeuge und -methoden sind Voraussetzung für die Senkung von Entwicklungskosten, Verkürzung von Entwicklungszeiten und Gewährleistung von Sicherheit. Mit Hilfe abgestimmter FuE-Verbundaktivitäten gehen die strategische, methodische und technologische Entwicklung für zukünftige ACPS Hand in Hand.

Abb. 4: Roadmap Hochautomatisierte Systeme: Testen, Safety und Entwicklungsprozesse. Hrsg: SafeTRANS. 2017. Abrufbar unter:
www.safetrans-de.org/de/Aktivitaeten/Roadmapping.php

[1] Gerald Temme, Fabian Utesch, DLR, Validation & Verification by Simulation. AAET-Ausstellung, März 2018

[2] Hardi Hungar, Frank Köster, DLR. Formalisierung von Szenario-Klassen zur Absicherung automatisierter Fahrfunktionen. AAET, März 2018

„Schon sehr früh im Projekt erste Demonstratoren aufzusetzen hat sich als wirklich positiv erwiesen.“

Dr. Andrea Leitner, Projektleiterin bei AVL List, über Testmethodiken hochautomatisierter Systeme, den Praxisbezug von Forschung und das Management eines großen europäischen Forschungs- und Entwicklungsprojektes

Große europäische Forschungs- und Entwicklungsprojekte sind eine Herausforderung, inhaltlich als auch koordinativ: von der Antragsstellung, Förderung über die laufende Arbeit und vor allem die Gewährleistung der weiteren Nutzung der Projektergebnisse (Stichwort: Nachhaltigkeit). Im Bereich Absicherung hochautomatisierter, vor allem sicherheitskritischer Systeme ist länderübergreifender Austausch extrem wichtig, um sich neben dem Know-how-Austausch zu einer einheitlichen Vorgehensweise und in Richtung Standardisierung abstimmen zu können. Dr. Andrea Leitner, AVL List GmbH und Koordinatorin des EU-Projektes ENABLE-S3, berichtet über den Stand der Forschung nach zwei Jahren Projektlaufzeit und die Arbeit als Managerin internationaler, großer FuE-Projekte.

Frau Leitner, Sie koordinieren das EU-Forschungsprojekt ENABLE-S3 mit 68 Partnern aus 16 Ländern. Womit beschäftigt sich das Projekt konkret? Was möchte das Projekt erreichen?
Andrea Leitner: Das Projekt beschäftigt sich mit Testmethodik und Testumgebungen zur Absicherung von hochautomatisierten Systemen in unterschiedlichen Anwendungsdomänen. Ein höherer Automatisierungsgrad hat das Potenzial sich positiv auf unterschiedliche gesellschaftliche Aspekte auszuwirken. Zum Beispiel können automatisierte Fahrzeuge die Sicherheit und Effizienz im Straßenverkehr erheblich zu erhöhen. Ähnliches gilt auch für andere Bereiche wie Schifffahrt oder Luftfahrt.
Aktuell wird die Markteinführung allerdings durch das Fehlen einer wirklichen Lösung für die Absicherung dieser hochautomatisierten Systeme verhindert. ENABLE-S3 versucht einen erheblichen Schritt in diese Richtung zu machen.

Im Projekt geht es u. a. um die Anwendung von Simulation zum Testen hochautomatisierter Systeme/Funktionen in verschiedenen Anwendungsdomänen (Automobil, Luft- und Raumfahrt, Bahn, Seefahrt Gesundheit, Landwirtschaft). Was sind typische konkrete Anwendungen?
Wir beschäftigen uns im Projekt nicht nur mit reiner Simulation, sondern auch mit unterschiedlichen Kombinationen aus Simulation und realen Komponenten, um sicherzustellen, dass wirklich alle Fehler gefunden werden können.
Typische Anwendungen lassen sich am besten durch die Applikationen im Projekt darstellen. ENABLE-S3 ist so aufgesetzt, dass Industriepartner ein konkretes zu testendes System beschreiben. Daraus werden die Anforderungen an das Testsystem abgeleitet und am Ende werden die Lösungen in diesem Kontext evaluiert. Beispiele für solche Anwendungen sind unter anderem Valet Parking Systeme (Anm. d. Red.: siehe auch SafeTRANS News 2/2017 unter: *http://news.safetrans-de.org/ausgabe-2017-02/EU-Projekt_ENABLE-S3.html*). Beim Valet Parking wird das Auto an einer Parkgarage abgegeben und sucht sich selbstständig einen Parkplatz. Andere Anwendungen sind unter anderem ein Highway Pilot, der selbstständig auf der Autobahn fährt, oder automatisierte Erntesysteme in der Landwirtschaft.

ENABLE-S3 bereitet im Moment das EU-Reporting über das zweite Jahr vor. Wurden die gesetzten Zwischenziele erreicht?
Ja. Die Entscheidung schon sehr früh im Projekt erste Demonstratoren aufzusetzen hat sich als wirklich positiv erwiesen. Dadurch erhält man sehr schnell Feedback, ob die entwickelten Lösungen die erhofften Vorteile bringen bzw. wo noch Verbesserungsbedarf besteht. Dadurch können wir nun schon am Ende des zweiten Projektjahres eine Vielzahl an Demonstratoren vorweisen, die bei einer öffentlichen Ausstellung Anfang Juli in Dublin gezeigt wurden.

Wie bewerten Sie die bisher erreichten Ziele? Lässt sich bereits absehen, wo ein Durchbruch erreicht werden kann und welche Verfahren eventuell nicht zielführend sind? Tauchen bereits neue Weg auf?
Die Projektergebnisse wecken großes Interesse. Das zeigt uns, dass wir auf dem richtigen Weg sind. Virtuelle Validierung wird mittlerweile in allen Anwendungsdomänen als einzig mögliche Lösung zur Handhabung der hohen Testkomplexität gesehen. Nichtsdestotrotz haben wir mittlerweile erkannt, dass das Problem am Ende des Projekts nicht komplett gelöst sein wird. Allerdings konnten einige wichtige Erkenntnisse gewonnen werden, die gleichzeitig die Anforderungen an zukünftige Projekte stellen. Wir sind stark bestrebt, das aufgebaute Wissen auch mit anderen Projekten zu teilen, um schneller voranzukommen.

Und was bedeuten diese Ergebnisse für die praktische Anwendung?
Ich denke, dass uns die Projektergebnisse einen großen Schritt weiter in Richtung Absicherung und damit auch Homologation oder Zertifizierung, d. h. zur tatsächlichen Zulassung der Systeme, bringen. Wie gesagt, gibt es noch einige offene Fragestellungen, die aber vermutlich nur in einem größeren, globaleren Kontext gelöst werden können.

Kann man die Erkenntnisse der im Projekt entwickelten Use-Cases für jede Domäne in die Praxis übertragen? Falls nein, was fehlt noch?
Erste Teilergebnisse werden schon im Produktivbetrieb bei einzelnen Projektpartnern eingesetzt. Was jedoch noch fehlt, ist ein ganzheitlicher methodischer Ansatz. Das Projekt kann dazu wichtige Bausteine liefern. Allerdings bedarf es dafür die Zusammenarbeit unterschiedlichster Interessensgruppen, wie z.B. auch der Gesetzgebung, Versicherungen, Zertifizierungsstellen, usw.

Welche Vorhaben stehen im Rahmen von ENABLE-S3 konkret in nächster Zeit an?
Nach dem 2nd Year Review im Juli wird das Feedback entsprechend umgesetzt. Außerdem werden die Erkenntnisse aus dem Aufbau der Demonstratoren zur Verbesserung der technischen Lösungen genutzt. Im dritten Projektjahr geht es hauptsächlich darum, letzte Umsetzungen abzuschließen und die gewonnenen Erkenntnisse zusammenzufassen. Das klingt zwar schon eher nach Projektabschluss, beinhaltet aber auch wichtiges Feedback in Spezifikations- und Standardisierungsarbeitsgruppen. Damit sind dies wichtige Schritte, um die Nachhaltigkeit der Projektergebnisse zu sichern.

Sie sind Expertin für Software-Entwicklung. Bei ENABLE-S3 übernehmen Sie die Projekt-Koordination. Was gefällt Ihnen besser: die Forschungsarbeit oder das Forschungsmanagement?
Das ist nicht leicht zu beantworten: bei der reinen Forschungsarbeit kann man sich mit Problemstellungen eher im Detail beschäftigen. Allerdings ist es auch spannend, eine Gesamtübersicht zu haben und gewisse strategische Entscheidungen ableiten zu können.

Welche Lehren ziehen Sie - aus Management-Sicht - aus einem so großen europäischen FuE-Projekt?
Ein Projekt dieser Größe hat sowohl Vor- als auch Nachteile und stellt vor allem eine große Herausforderung dar. Für mich haben sich die folgende Dinge als wesentlich erwiesen:

- Mit motiviertem Projektteam und engagierten Arbeitspaketleitern funktioniert das Management eines solchen Projekts sehr gut.
- Ein Projekt dieser Größe bringt zwar einen höheren Koordinationsaufwand, allerdings ist der Austausch mit anderen Projektpartnern, speziell auch aus anderen Domänen sehr wertvoll. Es ist wichtig, dass man dafür den notwendigen Rahmen schafft.
- Durch die Größe des Projekts, bekommt man auch eine gewisse Sichtbarkeit nach außen. Da viele Partner in dem Projekt involviert sind, werden die Ergebnisse auch für externe Partner interessant.

Vielen Dank für das Interview!

Mehr Informationen: *http://enable-s3.eu/*

ENABLE-S3 im Überblick

Laufzeit	Mai 2016 bis April 2019
Koordinator	AVL List GmbH
Förderung	ECSEL Joint Undertaking
Volumen	64,8 Mio. Euro
Fördervolumen	33 Mio. Euro
Partner	68 aus 16 Ländern (davon 9 SafeTRANS-Mitglieder)
Anwendungen	Automobil, Luft- und Raumfahrt, Bahn, Seefahrt, Gesundheit, Landwirtschaft

Dr. Andrea Leitner

Andrea Leitner hat 2009 ihren Master-Abschluss in Software Engineering und Wirtschaft und 2012 ihren Doktor der technischen Wissenschaften (Dr. techn.) in Informations- und Kommunikationstechnik an der TU Graz erhalten. Nach einigen Jahren am Virtual Vehicle Research Center in Graz arbeitet sie derzeit als Research Project Manager Automated Driving bei der AVL List GmbH in der Grazer Konzernzentrale im Geschäftsbereich „Instrumentation and Test Systems (ITS)“, im Bereich Testmethoden und -umgebungen für ADAS und Automated Driving. In diesem Zusammenhang leitet sie das große europäische Forschungsprojekt ENABLE-S3, das verschiedene Aspekte automatisierter Systemtests abdeckt, und verantwortet die Aktivitäten zur Szenariengenerierung und Testplanung innerhalb von AVL.

Radiation-hardened Ethernet transceiver:

H2020 project SEPHY implements innovative technologies to realize ITAR-free physical layer transceiver

SEPHY is strengthening the competitiveness of the European space sector.

The growing complexity of space systems is creating the need for high-speed data networking technologies interconnecting different elements of a spacecraft to address increasingly demanding missions. This has spurred initiatives by both the European Space Agency (ESA) and the National Aeronautics and Space Administration (NASA) to define the next generation networking technologies for space. In both cases, Ethernet has been identified as the preferred choice due to its wide adoption in terrestrial applications and because it is fully standardized, thus ensuring interoperability. Deterministic versions of Ethernet are often used for safety-critical command and control functions onboard spacecraft. For example, the NASA advanced multi-purpose crew vehicle (supported by the European Space Agency) and the upcoming European launcher family, Ariane 6, are both employing Time-Triggered Ethernet (TTEthernet) [1] to realize their avionics needs [2].
The requirements for integrated circuits that must operate in space are very different from those that are used in terrestrial applications. In particular, the radiation is much more intense and causes several types of effects on the devices that compromise their reliability [3]. Therefore, special "rad-hard" design and manufacturing techniques are needed for devices that will operate in space. In SEPHY project novel techniques are elaborated and applied to design and manufacture a rad-hard Ethernet PHY (Physical Layer) for space applications [4].

Being executed by 6 recognized industrial and academic partners with clear non-overlapping responsibilities from 4 European countries, SEPHY targets the development of a first-class 10/100Mbps Ethernet PHY for the space market to enable Ethernet-based technologies to become an international space networking standard. This device will enable the use of Ethernet in space systems and also provide the starting point for the long-term objective of implementing a Gigabit Ethernet PHY for space. To implement the Ethernet PHYs efficiently, the consortium has significant analogue (Arquimea) and digital (IHP) design capabilities. In addition, it has also partners experienced in application of the Ethernet upper layers in space systems (TTTech) and in the design and implementation of Ethernet PHYs and Ethernet standards (Universidad Antonio de Nebrija). Finally, the electronic technology and manufacturing capabilities (Microchip Technology Nantes) allow for the production of samples of a future product for testing (Thales Alenia Space Spain).

Technical Approach

Ethernet is, as most communication protocols, structured in layers with the most relevant ones being the Medium Access Control (MAC) and the Physical (PHY) layer. The PHY layer interacts with the transmission media and ensures that data is transmitted with a low bit error rate. To that end the PHY devices implement advanced signal processing techniques. In fact, high speed Ethernet PHYs are complex mixed signal devices that pose significant implementation challenges because the physical layer transceiver is by nature a mixed-signal device processing analog signals from cables and transform the signals into digital signals at MAC. There are several Ethernet PHY standards supporting different types of transmission media and speeds, however, they need to be upgraded addressing radiation effects to enable widespread adoption of Ethernet in space.
The general idea of SEPHY is to use a radiation hardened FPGA that can withstand radiation and can serve as platform on which the system is implemented that reduces costs significantly. There has been some effort to implement programmable devices for mixed-signal circuits, but none of them are capable to withstand radiation to the best of our knowledge. SEPHY proposes a novel solution implemented as follows.
The SEPHY Ethernet transceiver is a mixed-signal device developed in Europe and is free from restrictions imposed by the International Traffic in Arms Regulations (ITAR). The physical layer transceiver deals with the transmission and reception of data over the physical medium ensuring reliable communication. Since the PHY interacts directly with the physical signals on the cable, it must contain an analogue front end capable of transmitting and receiving analogue signals. As the PHY connects to the digital MAC layer, it needs to perform complex digital signal processing and data controlling. Therefore, the physical implementation occurs by means of a mixed-signal ASIC – a complex semiconductor device that embeds in the same substrate analogue and digital functions.
The SEPHY device is compatible with 10BASE-T and 100BASE-TX Ethernet standards and it integrates all the physical-layer functions needed to transmit and receive data. The PHY supports the standard and reduced Media Independent Interface (MII/RMII) for direct connection to MAC (see Figure 1) and uses mixed-signal processing to perform equalization, data recovery, and error correction to achieve robust operation over CAT 5 twisted-pair wiring.

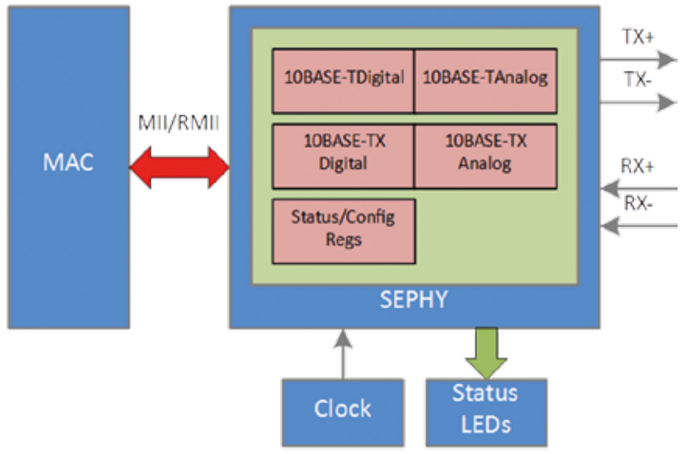

Figure 1: SEPHY Block Diagram

SEPHY implements two-fold radiation hardening approach: by design and by manufacturing process. The former is based on special circuit design techniques that can be applied at the system, architectural or layout level, e.g.: EDAC, TMR. The latter is accomplished by modifications during fabrication processes when the chip is being built to reduce the impact of radiation on integrated circuits, e.g.: use of specific insulator materials or the modification of doping profiles. Results are being tested in a radiation environment measuring the various radiation effects on the chip - single event upsets (SEU), latch-up (SEL) and total ionizing dose (TID), see [4] for more details.
The PHY behavior is and will be tested with regards to standard Ethernet and Time-Triggered Ethernet functionality. Figure 2 shows an Ethernet network setup and Figure 4 a testing setup used for the first successful validation of chip functionality. All test activities executed and planned in the project guarantee that the SEPHY device achieves a high maturity level such that it will be ready for qualification at the end of the project.

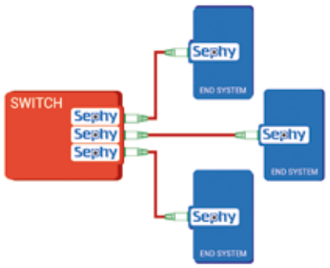

Figure 2: Ethernet Network Setup

Figure 3: SEPHY chip

SEPHY impact and potential

The ambition of the SEPHY project is to put Europe at the forefront of the adoption of Ethernet PHYs in space systems. This is rather challenging as

a. the Ethernet commercial and industrial integrated circuit market is dominated by non-European companies (Intel, Broadcom, Marvell, etc.) and
b. Ethernet PHYs are complex mixed signal devices and there are no Ethernet PHYs qualified for space.

Since the PHYs are a key component in Ethernet, the success of SEPHY would not only ensure non-dependence but possibly a globally leading role in the future. Therefore, the goals are ambitious both technically and in terms of the long term strategic impact of the project.

The SEPHY project also targets to reuse the developed PHYs for other mission critical or safety-critical applications. These include automotive, aeronautics and industrial systems in which Ethernet is already or is likely to become the dominant data networking technology. This extends the ambition of the project beyond space systems. Enabling the use of the SEPHY physical layer transceivers for terrestrial applications could help in positioning Europe as a player in the Ethernet integrated circuit market (which is a large market with more than one hundred million devices sold every year).

Thus, the project results allow for a number of applications in cyber-physical systems especially those working in harsh environments. Such systems usually comprise a number of interconnected components, such as sensors, computing units, various types of actuators, etc., which must reliably communicate one with each other. Furthermore, for instance, in industrial applications multiple cyber-physical systems must exchange information about their internal states to ensure safe and correct execution of production processes. Being exposed to magnetic fields or various sources of radiation cyber-physical systems cannot use Ethernet controllers developed for common applications such as office or public networks. Since SEPHY uses rad-hard design and manufacturing approaches, its products guarantee reliable communication also in situations when common products fail. SEPHY can be used in a wide range of applications reaching from industrial to aerospace. However, the radiation tolerant design of the analog and digital blocks within the chip supports high-reliability in harsh radiation environments (aeronautics and space applications including launch vehicles and satellites) which is enabled by the wide operational temperature range.

The Ethernet PHY developed within SEPHY will be a mixed-signal device packaged and tested within Europe. On the standardization side, the project consortium focuses on standards to drive adoption of Ethernet in Space and the project partners actively participate in the ECSS-TTE and CCSDS-SOIS working groups as well as in the EtherSpace Alliance meetings. Additionally, three NDAs have been signed with leading European space companies Airbus Defence and Space SAS and ArianeGroup as well as with the well-known Geneva-based research organization CERN showing the interest and proving the importance of the results to be achieved in SEPHY at the end of 2018. At the time of writing of this article sample SEPHY chips (Figure 3) are being manufactured based on the integrated circuit design shown in Figure 5.

The SEPHY chip will be available in space-grade packaging to support different customer requests, see *http://sephy.eu/flyer/* for more details.

SEPHY overview

Project	SEPHY (Space Ethernet Physical Layer Transceiver)
Duration	01.05.2015 - 31.12.2018
Coordinator	Arquimea
Programm	H2020-LEIT-Space-Competitiveness of the European Space Sector-2014
Grant Agreement	no. 640243
Total project costs	3.115.222,50 Mio. Euro
EC Funding	100 %
Partners	IHP, Thales Alenia Space España, Universidad Antonio de Nebrija, Microchip Technology Nantes, TTTech

Sephy

www.sephy.eu

References

[1] Steiner, W., Bauer, G., Hall B., and Paulitsch, M. Time-triggered Ethernet: TTEthernet. In Time-Triggered Communication, R. Obermaisser, Ed. CRC Press, 2011.

[2] Loveless, A. TTEthernet for integrated spacecraft networks. In Proceedings of the AIAA Space and Astronautics Forum and Exposition (SPACE 2015), 2015.

[3] Schrimpf, R. D., and Fleetwood, D. M. Radiation effects and soft errors in integrated circuits and electronic devices. World Scientific, 2004.

[4] P. Reviriego, J. López, M. Sánchez-Renedo, V. Petrovic, J. F. Dufour and J. S. Weil, „The space Ethernet physical layer transceiver (Sephy) project: a step towards reliable Ethernet in space," in IEEE Aerospace and Electronic Systems Magazine, vol. 32, no. 1, pp. 24-28, 2017.

Authors: Anna Ryabokon and Matthias Mäke-Kail, TTTech

Acknowledgement: We would like to thank the European Commission for the funding and all project partners for their valuable contributions to the project that allowed us to write this paper.

Figure 4: SEPHY Testing Setup showed at TASE Technodays in 2017, Spain. TTEthernet demonstration with three elements: FPGA with LEON 3 and TTEthernet controller, TTEthernet switch and PC with TTEthernet controller

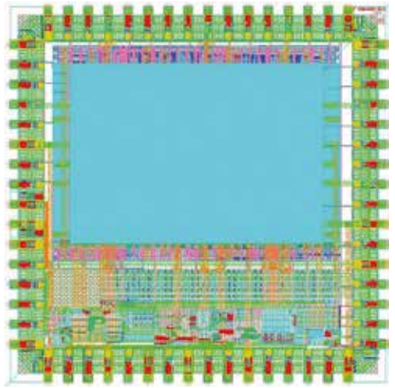

Figure 5: SEPHY layout

Figure 6: The last SEPHY consortium meeting took place on December 14th, 2017 at the TTTech Computertechnik AG Headquarters in Vienna (Austria).

Safety of the intented Function und eine gemeinsame Sprache für Safety und Security im Entwicklungsprozess

Spannende Vorträge und Diskussionen beim 24. SafeTRANS Industrial Day schaffen neue Erkenntnisse für Entwicklungs- und Testprozesse zukünftiger CPS.

Am 13. Juni 2018 fand in der Münchner Konzernzentrale bei Siemens das Fachsymposium des 24. SafeTRANS Industrial Days statt, der sich den Thema branchenübergreifende Prozesse, Methode und Technologien für Safety und Security hochautomatisierter Systeme widmete. Experten aus Industrie und Wissenschaft beleuchteten in ihren Fachvorträgen jeweils unterschiedliche Aspekte derzeitiger und zukünftiger Herausforderungen im Entwicklungs- und Testprozess autonomer Embedded und Cyber-physical Systems (CPS). Im Anschluss an das Fachsymposium wurde der Arbeitskreis *Prozesse, Methoden und Technologien für Safety und Security hochautomatisierter Systeme* (AK PMT4S&S) gegründet, der von Martin Rothfelder (Siemens) und Dirk Geyer (AVL Software and Functions) mit Unterstützung von SafeTRANS geleitet wird.

Die Verbindung von Safety und Security bei Entwicklung und Test

Warum sollte neben Safety auch Security bereits im Entwicklungsprozess sicherheitskritischer Funktionen stärker berücksichtigt werden und wie kann das geschehen, trotz unterschiedlicher Engineering-Ansätze? Die verschiedenen Anforderungen und Sichtweisen sind letztlich zwei Seiten einer Medaille: funktionaler und gegen äußere Angriffe geschützter Funktionen in autonomen oder hochautomatisierten Systemen. Die Optimierung der Test- und Entwicklungsprozesse zukünftiger CPS stand im Mittelpunkt der Tagung, vorrangig am Beispiel der Automobilindustrie wurden konkrete Ansätze vorgestellt und diskutiert. Im Eingangsvortrag griff Dirk Geyer Sicherheitsfunktionen für Functional Safety im Automobilbau auf. Darin wurde deutlich, dass Security-Gefährdungen die funktionale Safety-Entwicklung beeinflussen und Security-Mechanismen Safety-Anforderungen erfüllen müssen.

Das Verbindende und Trennende von Safety und Security verdeutlichte der Security-Fachmann Professor Hans-Joachim Hof von der TH Ingolstadt. Er hob die Bedeutung von Security für Safety hervor und welche Vor- und Nachteile unterschiedliche Security-Testmethoden in der Safety-Entwicklung haben. Auch die Experten im Publikum meldeten sich zahlreich zu Wort und das Thema wurde von Vertretern von OEMs, Zulieferern und Werkzeugherstellern sowie der Wissenschaft kontrovers diskutiert. Vor allem die Unterschiede zwischen Safety- und Security-Engineeringansätzen zeigen, dass sich beide Gebiete trotz unmittelbarer Beeinflussung derzeit schwer im gleichen Ansatz umsetzen lassen. Von den Experten wurde eine Unternehmenskultur, die beide Aspekte berücksichtigt, gefordert, indem Safety- und Security-Entwicklungsteams mit Überschneidungen arbeiten und eine einheitliche Sprache nutzen. Die Umsetzung von Safety und Security Aspekten durch das gleiche Entwicklungsteam wurde im Allgemeinen für nicht zweckdienlich erachtet. Zu verschieden sind die Ansätze, Werkzeuge und Denkweisen, die für entsprechende Nachweise genutzt werden, als das sie durch die gleichen Personen umgesetzt werden könnten. Wichtig sei aber ein gegenseitiges Verständnis der Anforderungen und ihrer Umsetzung.

SOTIF, szenarienbasiertes Testen und der AK PMT4S&S

Ein weiterer gesprächsintensiver Punkt betraf die Erweiterung eines neuen Standards SOTIF, *Safety of the intended functionality,* der im Bereich Testen von hochautomatisierten Systemen bestehende Standards, wie z.B. die ISO 26262, ergänzen soll. Was genau adressiert der Standard? Dr. Bert Boedekker (DENSO International Europe) referierte zum Thema und gab Auskunft zu Fragen und Anmerkungen. So wurde klar, dass die intendierte Funktion im Straßenverkehr mit autonomen Systemen viel stärker fokussiert werden muss. Es reicht nicht mehr aus, Systeme nur gegen Fehler bezüglich ihrer Spezifikation zu testen, da die Sollfunktion (Intented Function = gewünschtes Verhalten) oft gar nicht vollumfänglich formal spezifiziert werden kann. Somit stellt sich die Frage, wie die Sollfunktion zu spezifizieren bzw. zu entwickeln ist, sodass sie als hinreichend sicher angesehen werden kann. Dies wird als „Safety of the Intended Function“ (SOTIF) bezeichnet. Dass dabei die Anzal und Komplexität der zu testenden Fälle enorm ansteigt, stellt die Systementwickler und -tester vor enorme Herausforderungen. Ein Ansatz ist das szenarienbasierte Testen in virtueller Umgebung (siehe ab Seite 4), das von Dr. Hardi Hungar (DLR) vorgestellt und in der Anwendung von Dr. Tino Teige (BTC Embedded Systems) erläutert wurde.

Dass Szenarienkataloge eine Grundlage für technische Methoden und Prozesse zukünftiger CPS liefern, zeigte Dr. Jürgen Holzinger (AVL LIST), indem er die DevOps-Methodik für sicherheitskritische Systeme vorstellte. DevOps, kurz für die Verknüpfung von *Development* und *Operations*, verbindet u. a. das virtuelle Testen von hochautomatisierten Fahrfunktionen im Labor mit Ansätzen für das Lernen im Feld.

Die Gespräche und Diskussionen beim Fachsymposium machten deutlich, wie grundlegend der branchenübergreifende Austausch zwischen OEMs, Zulieferern, Werkzeugherstellern und Forschungsinstituten ist. Die Gründung des Arbeitskreises PMT4S&S ist ein wichtiger Schritt, um die Gespräche themenfokussiert weiterzuführen. Inhalte des 24. SafeTRANS Industrial Days sowie darüber hinaus wurden bestimmt zur weiteren Bearbeitung in einem Folgetreffen. Vom AK unabhängig wird der kommende 25. SafeTRANS Industrial Day im Herbst 2018 sattfinden.

Mehr Informationen zum 24. SafeTRANS Industrial Day unter:
www.safetrans-de.org/de/Veranstaltungen/2018/06/13/24.-safetrans-industrial-day
Auskünfte zum AK PMT4S&S auf folgender Webseite:
www.safetrans-de.org/de/Aktivitaeten/Roadmapping_AKs_2018.php

Eindrücke vom 24. SafeTRANS Industrial Day am 13. Juni 2018 in der Münchner Konzernzentrale von Siemens (v.l.n.r.): Blick in den Sitzungssaal; Martin Rothfelder (Siemens AG) eröffnet das Fachsymposium; anregende Diskussionen zwischen Publikum und Referenten

Autonomes Fahren erfordert neue, angemessene Entwicklungsmethoden für komplexe Systeme und Funktionen

INGenX Technologies berät Entwicklungsunternehmen bei der Umsetzung von Hochtechnologien.

Autonom fahrende Kraftfahrzeuge, Pkw wie Lkw, werden in wenigen Jahren das Bild auf unseren Straßen radikal verändern und Teil unseres gesellschaftlichen Lebens und unserer individuellen Mobilität sein. Die dafür benötigten technischen Lösungen werden durch Echtzeitverhalten, Fail-Operational Funktionsredundanzkonzepte, hochverfügbare Systeme, Sensorfusion und andere technologische Herausforderungen bestimmt und schnell die Grenzen der bisherigen Methoden der Systementwicklung im Automobilbau aufzeigen.

Robustes und nachverfolgbares Design für komplexes Systemverhalten

Neue, komplexe Technologien verlangen angemessene Analyse- und Synthesemethoden sowie beherrschbare Entwicklungsprozesse mit hohen Reifegraden. Die funktionale Sicherheit technologisch anspruchsvoller Entwicklungen zur Realisierung des autonomen Fahrens muss während der komplexen Produktentstehungsphasen und danach im Umfeld des Verkehrsbetriebs durch klar strukturierte, transparente und jederzeit reproduzierbare Prozesselemente und Arbeitsprodukte gewährleistet werden. Klare und nachweisbare Anforderungen an Produkte und Prozesse bilden die Kernelemente für sichere, robuste und nachverfolgbare Design-Lösungen. Ziel muss daher sein, komplexes Systemverhalten über einfach zu erfassende Prozesslösungen abzusichern, nachhaltig und zuverlässig.

INGenX Technologies GmbH berät unter anderem Kunden aus der Automobil- und Nutzfahrzeugindustrie und unterstützt bei der Implementierung, um diese Herausforderungen zusammen mit den Kunden zu bewältigen und damit zu nachhaltig sicherer Entwicklung beizutragen. Jahrzehntelange Erfahrung aus der Luftfahrtindustrie und ein sehr anwendungsorientiertes Verständnis komplexer Systeme und Funktionen bilden das Fundament für eine solide und sehr hohe Qualität der Technologie- und Prozessberatung. Dieses tiefe Verständnis eingebetteter Systeme und deren Funktions- und Nutzungsumgebung wurde bereits vor 15 Jahren durch erste modellbasierte Entwicklungsansätze aufgebaut, die ihrer Zeit weit voraus waren. Diese sehr früh erarbeiteten Kompetenzen und Erfahrungen sind nun die Grundlage für die Beratung der Automobilhersteller und Systemzulieferer.

Funktionale Sicherheit dank schlanker Anforderungsdefinitionen

Einen besonderen fachlichen Beratungsschwerpunkt bildet bei INGenX Technologies die Funktionale Sicherheit als integrales Produktmerkmal in Verbindung mit einer signifikanten Reduzierung der erforderlichen System- und Subsystemanforderungen in der Produktentwicklung. Die Definition und Verwaltung von mehreren tausend funktionalen Anforderungen ist leider für heutige Steuergeräte (ECUs) zur Regel geworden, anscheinend im Glauben, mehr Dokumentation schaffe auch mehr Sicherheit und mehrfaches Wiederholen mache Dinge richtiger. All diese unzähligen textuellen Anforderungen müssen einerseits durch passende Design-Lösungen realisiert und andererseits einwandfrei und lückenlos getestet werden. Dieses Anforderungsphänomen bindet in den betroffenen Unternehmen unzählige Ressourcen und verursacht sehr hohe Kosten, wird in den seltensten Fällen souverän beherrscht und hat damit eher zweifelhaften Mehrwert.

Meistens findet die Definition der Anforderungen ohnehin erst im Reverse Engineering statt, nachdem die Lösung festgelegt ist. Dass dabei meist nicht die ideale Lösung gefunden wird, sondern nur bekannte Lösungen nach altbewährten Vorgehensweisen und Kalkulationen implementiert werden, wird nicht hinterfragt. Auch agile Vorgehensweisen zeigen wenig Wirkung, wenn sie nur auf das Althergebrachte aufgesetzt oder - soweit das überhaupt möglich ist - zusätzlich angewendet werden.

INGenX Technologies zeigt zum Beispiel mit modernen Entwurfsmethoden neue Wege und Ansätze und bricht mit den alten Verhaltensschemata, die sich durch die evolutionäre Annäherung der Automobilindustrie an eingebettete, komplexe Systeme über Jahrzehnte halten konnten, ohne wirklich schlank und zielführend zu sein. Die Anwendung neuer Methoden erfordert aber auch ein Umdenken der prozessbeteiligen Menschen. Um diese für die Veränderungen zu befähigen, unterstützt INGenX Technologies die Kunden mit fachlichem, aber auch Soft Skill Coaching in ihrer täglichen Entwicklungsarbeit.

Gemäß dem Unternehmens-Claim INNOVATION.PROCESS.SOLUTION erfassen die Beratungsmethoden von INGenX Technologies die Veränderungsprozesse als „ganzheitliche Systeme“. Somit werden von Anfang an die veränderungsrelevanten Entscheidungsprozesse identifiziert und Maßnahmen initiiert, mit den Zielen, die damit verbundenen Risiken zu minimieren, um in der Lösungsumsetzung überdurchschnittlich erfolgreich zu sein.

„Denken ist die schwerste Arbeit die es gibt. Das ist wahrscheinlich der Grund, warum so wenig Leute sich damit beschäftigen.“ *Henry Ford*

INGENX TECHNOLOGIES GmbH

http://www.ingenx-technologies.com/

SHORTCUTS: INGenX Technologies

Unternehmen:	INGenX Technologies GmbH
Sitz:	Stade
Geschäftsfelder:	Technologieberatung mit dem Schwerpunkt Systems Engineering
Gründungsjahr:	2014

Fragen an Jörg Krüger, Geschäftsführer:

INGenX hat seine Ursprünge in der Luftfahrtindustrie und wächst derzeit stark im Automotive Bereich. Worin liegen die Unterschiede beider Ingenieursansätze?

In der Luftfahrt ist das stringente Entwicklungsvorgehen nach dem V-Modell (Systems Engineering) seit Jahrzehnten der Industriestandard. Für Entwicklungsingenieure von Flugzeugsystemen muss die System Safety seit jeher an oberster Stelle stehen, um die strengen Zulassungsvorschriften erfüllen zu können. Die Systemsicherheit ist quasi inhärenter Teil einer jeden Systementwicklung und bei den Ingenieuren in Fleisch und Blut übergegangen. Diese Ausprägung ist in der Automobilindustrie noch nicht annähernd erreicht, aber unabdingbar, wenn es um komplexe Systementwicklung geht.

Was glauben Sie ist in Zusammenhang mit (hoch-) automatisierten Fahrzeugen die größere Herausforderung: Die Umsetzung der Systemanforderungen oder der Zertifizierungsprozess und die (kontinuierliche) Erbringung von Sicherheitsnachweisen?

Die gesamte Prozesskette stellt eine große Herausforderung dar. Wichtig ist, dass der gesamte Entwicklungsprozess konsequent umgesetzt und gelebt wird und meines Erachtens mittels einer formalen Prozesssicherstellung (Process Assurance) - die über Automotive SPICE hinausgeht - lückenlos überwacht werden sollte.

INGenX ist ein junges, agiles Unternehmen. Sehen Sie bereits Anpassungen aufgrund veränderter Kundenwünsche?

Ganz klar, nein. Wir sind als Technologieberatung für Systems Engineering gestartet und haben in der Gründungsphase unseren Zielmarkt intensiv analysiert und bewertet. Die Erfahrungen der ersten vier Jahre haben die damaligen Annahmen mehr als bestätigt.

SafeTRANS Mitglieder

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

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

ICS AG
www.ics-ag.de

INGenX Technologies GmbH
www.ingenx-technologies.com

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

TU Braunschweig
www.tu-braunschweig.de

Universität Bremen
www.uni-bremen.de

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

Verified Systems
International GmbH
www.verified.de