Hochautomatisierte Systeme: Testen, Safety und Entwicklungsprozesse

Forschungsherausforderungen und Handlungsempfehlungen

Positionspapier

Herausgeber

Peter Heidl, Robert Bosch GmbH

Werner Damm, OFFIS

Dieses Dokument fasst die wichtigsten Ergebnisse und Empfehlungen des SafeTRANS-Arbeitskreises "Hochautomatisierte Systeme" zu Herausforderungen in Forschung und Regulierung für einen kosteneffektiven und sicheren Einsatz von hochautomatisierten Systemen zusammen. Dabei konzentrieren wir uns auf die technischen Herausforderungen und regulatorischen Anforderungen, die den gesamten Entwicklungsprozess betreffen, einschließlich Architektur und Sicherheitsaspekten sowie Verifikation und Validierung (V&V). Der Arbeitskreis bestand aus Experten aus vier Anwendungsbereichen – Automobil, Luft- und Raumfahrt, Bahn und Schiffsverkehr (siehe Anhang 1 zu „Organisationen und Mitwirkende“) – um Gemeinsamkeiten und Synergiepotenziale der Domänen auszunutzen. Das Dokument baut auf bestehenden nationalen und europäischen Roadmaps für hochautomatisierte Systeme auf (siehe Anhang 2). Das vollständige Dokument wird als SafeTRANS-Roadmap „Hochautomatisierte Systeme“ im Sommer 2017 veröffentlicht werden und enthält insbesondere eine ausführliche Herleitung und Priorisierung der Forschungsthemen. Das Positionspapier sowie die Roadmap richten sich an öffentliche Institutionen – für regulatorische Belange sowie zur Gestaltung des Rahmens für Forschung und Entwicklung – und an die Industrie – zur Abstimmung von Forschungs- und Entwicklungsvorhaben sowie hinsichtlich Normung und Standardisierung.

1 Ziele des Dokuments

Damit die nationale und europäische Verkehrsindustrie ihre führende Marktposition halten und ausbauen kann, müssen nachhaltige Lösungen für eine sichere und umweltschonende Mobilität in allen Verkehrsbereichen (Automobil, Luftfahrt, Bahn, Schiffsverkehr) vorhanden sein. Der aktuelle Wettbewerbsvorteil basiert auf einer profunden Expertise in der Entwicklung von komplexen *Embedded Systems*. Um von einer ständig steigenden Automatisierung und von neuen Fähigkeiten der Systeme angemessen profitieren zu können (Kapitel 2), müssen derzeit und zukünftig verstärkt enorme Herausforderungen bezüglich Komplexität, Sicherheit, Verfügbarkeit, Steuerbarkeit, Wirtschaftlichkeit und Komfort bewältigt werden. Diese Anstrengungen im Bereich der Forschung, Entwicklung, Validierung und Infrastruktur sind so hoch,

dass keine einzelne Organisation in der Lage sein wird, diese alleine zu tragen. *Um in einer führenden Marktposition zu bleiben und diese weiter auszubauen ist es notwendig, die Zusammenarbeit in und zwischen den Industriesektoren auf- und auszubauen*, einen auf Beobachtungen im Feld basierenden Lernprozess zu etablieren (Kapitel 3), die technischen Herausforderungen zu adressieren (Kapitel 4) und gemeinsam die strategischen Maßnahmen umzusetzen (Kapitel 5). Basierend auf einer Vision *Sicherheit für hochautomatisierte Verkehrssysteme* hat der Arbeitskreis die folgenden Ziele für eine sektorübergreifende Forschungs- und Entwicklungs-(F&E)-Strategie abgeleitet:

Ziele

1. Etablierung kontinuierlicher, branchenübergreifender, auf Analyse von Flottendaten basierender Lernprozesse für die Entwicklung von hochautomatisierten Verkehrssystemen, um eine schnelle Übernahme neuer Features und Funktionen unter Beibehaltung und Verbesserung der Sicherheit und Leistung der Systeme zu ermöglichen.

2. Standardisierung einer gemeinsamen, erweiterbaren, fehlertoleranten Systemarchitektur, die Onboard-Systeme und Infrastruktur umfasst, und welche die notwendige Innovationsgeschwindigkeit und einen effektiven Validierungsaufwand erlaubt.

3. Bewältigung der in Kapitel 4 identifizierten Forschungsherausforderungen sowie die Entwicklung und Erweiterung von Methoden zur Unterstützung der V&V, des Engineerings sowie der Modellierung für sichere Open-World-Systeme, mit denen ein modellzentrierter Ansatz für Verifikation und Validierung erfolgen kann. Darüber hinaus die Etablierung einer offenen Entwicklungsumgebung und eines von Herstellern, Zulassungs-und Zertifizierungsbehörden sowie der Gesellschaft gemeinsam anerkannten Entwicklungs- und Validierungsprozesses.

4. Kombination etablierter, deterministischer, modellzentrierter Entwicklungsansätze mit Verfahren zur kognitiven Automatisierung und zu semantischen Algorithmen, um den sicheren Betrieb dynamischer Open-World-Systeme und deren Validierung zu ermöglichen.

5. Minimierung des durch hochautomatisierte Verkehrssysteme erzeugten Risikos durch selbst-bewusste Systeme.

6. Mensch-Maschine-Interaktion und -Kooperation werden auf einer intentionalen Ebene möglich. Kognitive Automatisierung wird die Sicherheit des Systems durch Reduktion der Unberechenbarkeit des Menschen erheblich erhöhen.

7. Verkehrs- und Cloud-basierte-Infrastrukturen werden in die Lage versetzt, automatisierten Verkehrssystemen validierte Umgebungsinformationen zur Verfügung zu stellen, wodurch ein sicherer automatisierter Betrieb ermöglicht sowie die Komplexität des Fahrzeugs selbst reduziert wird.

2 Ausbaustufen der Hochautomatisierung

Der aktuelle Stand der industriellen Praxis in den drei Verkehrsdomänen Bahn, Luft- und Raumfahrt und Seefahrt umfasst bereits *Remote Operating Vehicles* (ROV), ferngesteuerte Systeme, die für eine begrenzte Zeit und für eingeschränkte Ziele autonom agieren, falls z.B. die Datenverbindung verloren geht (z.B. Remotely Piloted Air Systems), sowie vollständig autonome Systeme, wie z.B. autonome Unterwasserfahrzeuge (AUV) im maritimen Bereich und automatisierte Metros in kontrollierten städtischen Umgebungen. Dennoch befinden wir uns erst am Anfang dieser Entwicklung von automatisierten und autonom agierenden Maschinen. Diese Entwicklung ist gekennzeichnet durch die Zunahme des autonomen Verhaltens

- in zunehmend komplexen Umgebungen
- für zunehmend komplexere Aufgaben
- mit zunehmender Fähigkeit des Systems, mit anderen Maschinen und Menschen zu kooperieren und
- mit zunehmender Fähigkeit, von Erfahrungen zu lernen und das entsprechende Verhalten anzuwenden

Aus heutiger Sicht gehen wir von vier Ausbaustufen für hochautomatisierte Systeme aus. Jede dieser Stufen ist durch neue konzeptionelle Eigenschaften gekennzeichnet, die neue Herausforderungen der Systemtheorie und -architektur mit sich bringen. Die Ausbaustufen werden sich mit einer Phasenverschiebung von etwa einer Dekade parallel entwickeln und nicht sequenziell, sondern überlappend am Markt verfügbar sein.

Stufe	Merkmale
1	*Funktionale automatisierte Systeme* können begrenzte, klar definierte Aufgaben autonom erfüllen, wie z.B. automatisches Einparken, automatisches Landen oder die automatische Abarbeitung einer durch einen Operator im Vorfeld geplanten Mission. Diese Systeme können während des Betriebs nicht lernen; die Kooperation mit anderen Systemen ist auf den Austausch von Kontextinformationen beschränkt.
2	*Missionsorientierte Systeme* haben die Aufgabe, situationsabhängig eine ungeplante Kette beherrschbarer und bekannter Situationen zu durchlaufen. Dabei können verschiedene Optimierungskriterien wie die Minimierung des Zeit- oder Ressourcenbedarfs eine Rolle spielen. Planungs- und Optimierungsberechnungen werden zur Laufzeit durchgeführt. Diese Systeme können während des Betriebs nicht lernen; die Kooperation mit anderen Systemen ist auf den Austausch von Informationen über den Kontext und über das System selbst beschränkt. Beispiele hierzu sind der Highway-Pilot oder die Durchführung von Gebietserkundungen.
3	*Kollaborative Systeme* sind Systeme wie Roboter, Fahrzeuge, Schwärme, die z.B. einfädeln lassen oder die zur Unfallvermeidung miteinander kooperieren. Solche Systeme sind zur Erfüllung ihrer Mission in der Lage, mit anderen Systemen und Menschen zu kooperieren und ihre Wahrnehmungen, Interpretationen, Ziele, Pläne und Aktionen miteinander abzustimmen. Die Systeme tauschen mit ihren Kooperationspartnern relevante Kontextinformationen aus, sind jedoch nicht lernfähig.

4	*Autopoietische Systeme*[1] sind Systeme, die ihre Perzeption, ihre Interpretationen, ihre Aktionen und ihre Kooperationsmöglichkeiten selbstständig erweitern und sich mit anderen Systemen darüber austauschen können (inklusive der Weitergabe von erlerntem Verhalten). Diese Systeme zeigen somit menschenähnliches Verhalten. Die Fähigkeit des nicht-überwachten Lernens ist das wesentliche Charakteristikum dieser Systemklasse.

Wir erwarten, dass diese Ausbaustufen in den nächsten Dekaden im Markt eingeführt und etabliert werden. Jede Stufe hat eine eigene Wertschöpfung und schafft wirtschaftlichen Nutzen. Die meisten aktuellen Systeme sind funktionale automatisierte Systeme; wir befinden uns an der Schwelle zur Einführung von missionsorientierten Systemen und auch erste Systeme mit einfachen Kollaborationsmöglichkeiten existieren bereits. Unüberwachtes Lernen im laufenden Betrieb ist derzeit nicht möglich und wird es auch in naher Zukunft nicht sein. Die möglichen Fortschritte in dieser Entwicklung basieren auf konzeptionellen Fortschritten in Forschung und Engineering zu den unten dargestellten Herausforderungen.

3 Notwendigkeit des Lernen aus Feldbeobachtungen

Für jede der im vorangegangenen Abschnitt genannten Ausbaustufen müssen für jedes neue System Antworten auf die folgenden Fragen präzise festgelegt werden:

1. Welche Umweltsituationen müssen mit welcher Genauigkeit und mit welcher Zuverlässigkeit erkannt und interpretiert werden, um das gewünschte autonome Verhalten zu ermöglichen?
2. Welche Nachweise für Sicherheit und Zuverlässigkeit müssen für die (Typ-)Zulassung geführt werden?
3. Welche Methoden, Prozesse und regulatorische Rahmenbedingungen müssen für die Markteinführung solcher Systeme vorhanden sein?

[1] "An autopoietic machine is a machine organized (defined as a unity) as a network of processes of production (transformation and destruction) of components which: (i) through their interactions and transformations continuously regenerate and realize the network of processes (relations) that produced them; and (ii) constitute it (the machine) as a concrete unity in space in which they (the components) exist by specifying the topological domain of its realization as such a network" [17]

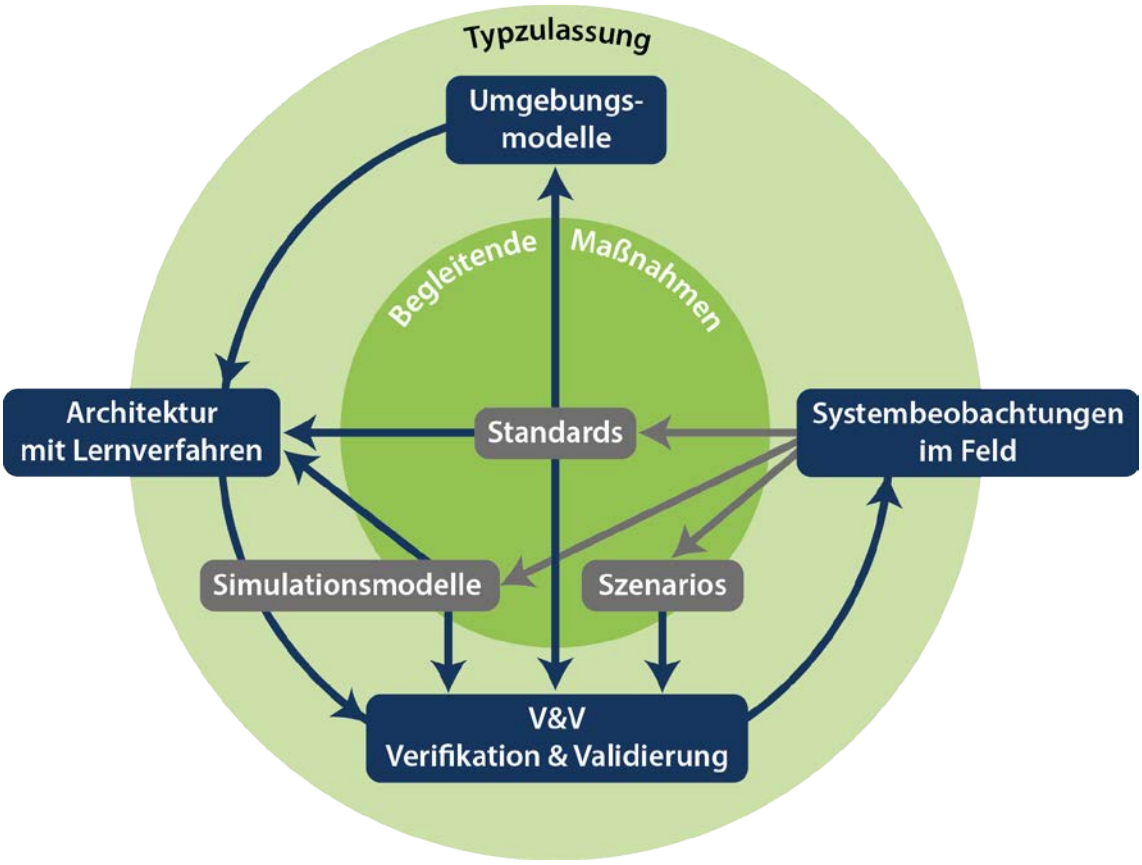

Abbildung 1: Wesentliche Elemente eines Systems der kontinuierlichen Überwachung und des Lernens aus Feldbeobachtungen für hochautomatisierte Systeme

Die hohe Komplexität der Umwelt macht die Durchführung einer für eine Zulassung ausreichend großen Anzahl von Feldtests für hochautonome Systeme impraktikabel. Daher empfehlen wir dringend ein System der kontinuierlichen Überwachung solcher Systeme zu implementieren sowie von Daten aus Feldbeobachtungen zu lernen. Dadurch können die obigen Fragen 1 und 2 beantwortet werden und es ergeben sich erste Empfehlungen zu Frage 3 mit Schlüsselelementen, die in Abbildung 1 dargestellt sind.

Abbildung 1 zeigt eine Meta-Ebene des Lernprozesses, bei dem die Systeme im Feld beobachtet und diese Felddaten nach Beurteilung durch eine unabhängige Stelle die Basis für den Lernprozess sind. Diese Beurteilung liefert Richtlinien oder Empfehlungen für neue Features und/oder neue Funktionalitäten für den Entwicklungs- und Validierungsprozess mit dem zweifachen Ziel (1) der Verbesserung der Wahrnehmungsfähigkeiten des Systems und (2) der Sicherstellung von situationsangepasstem und sicheren Verhalten der Systeme. Ein solcher Lernprozess ermöglicht eine kontinuierliche Evolution autonomer Systeme auch dank der Möglichkeit der virtuellen Freigabe neuer Features und Funktionen im Rahmen eines modellzentrierten Entwicklungsprozesses. Zentrale Bausteine dieses Prozesses sind die Systemarchitektur und Algorithmen, Umweltmodelle, Verfahren der Verifikation und Validierung- sowie die systematische Erfassung von Betriebsdaten aus dem Feld. Diese grundlegenden Elemente müssen entsprechend standardisiert sein, benötigen eine gemeinsame offene Simulationsumgebung und konkrete, akzeptierte (Test-)Szenarien für die Freigabe.

4 Herausforderungen in der Forschung

In der ausführlichen Roadmap „Hochautomatisierte Systeme“ werden zur Erreichung der wichtigsten Ziele des Meta-Ebenen-Lernprozesses aus Kapitel 3 die folgenden Forschungsbereiche hergeleitet (siehe Abbildung 2):

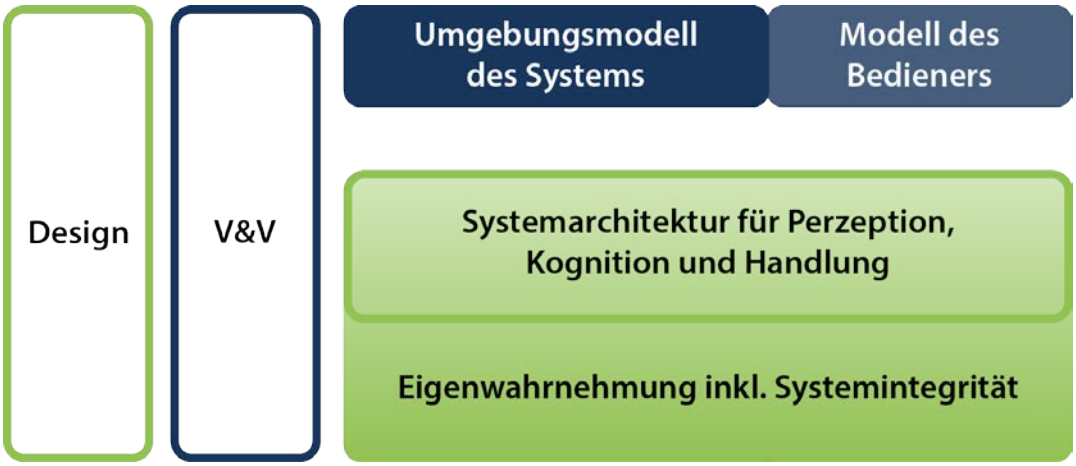

Abbildung 2: Forschungsbereiche

1. Der Forschungsbereich *Umgebungsmodell des Systems* befasst sich mit einer präzisen und umfassenden Spezifikation der operativen Systemumgebung in einer Form, die modellzentrierte, virtuelle Testverfahren unterstützt.
2. Im Forschungsbereich Modell des Bedieners werden Modelle des Verhaltens menschlicher Akteure in der Interaktion und Kooperation mit technischen Systemen entwickelt und untersucht, die eine Voraussage des Verhaltens, der Absichten, des Gesundheitszustands, der Fähigkeiten und weiterer Eigenschaften erlauben.
3. Der Forschungsbereich *Systemarchitektur für Perzeption, Kognition und Handlung* umfasst Grundlagen und Engineering-Methoden für erweiterbare Top-Level-Architekturen für die autonome Wahrnehmung, Entscheidungsfindung und Kontrolle unter Berücksichtigung der jeweiligen technologischen Randbedingungen.
4. Der Forschungsbereich *Design* beinhaltet die Entwicklung von Designmethoden und -prozessen zum Nachweis der Systemintegrität bei Integration von Cloud-basierten Services in sicherheitskritisches Systemverhalten sowie bei der Online-Integration neuer Features und Fähigkeiten.
5. Der Forschungsbereich *Verifikation und Validierung* (*V&V)* umfasst Nachweismethoden und -verfahren, um mithilfe von virtuellen Testumgebungen mit vertretbarem Aufwand die Sicherheit autonomer Systeme in allen möglichen Umgebungen und Zuständen, auch bei Sicherheitsattacken, nachzuweisen.
6. Der Forschungsbereich *Eigenwahrnehmung inkl. Systemintegrität* widmet sich Online-Methoden zur Sicherstellung der Systemintegrität unter allen – auch degradierten – Betriebsbedingungen und -modi, auch bei Security-Angriffen.

Für jeden dieser Forschungsbereiche ist in Anhang 3 eine weitere Detaillierungsebene mit den im jeweiligen Bereich identifizierten Forschungsprioritäten dargestellt.

5 Empfehlungen

Um die dargestellten Ziele zu erreichen, schlagen wir folgende ergänzende Maßnahmen vor, die – parallel zu F&E-Aktivitäten in den oben benannten Forschungsbereichen – von Industrie und öffentlichen Institutionen umgesetzt werden sollten. Diese Maßnahmen konzentrieren sich hier zunächst auf technische Normen und Vorschriften, weitere Maßnahmen in ebenso wichtigen Bereichen sind am Ende dieses Abschnitts zu finden.

Handlungsbereich	Maßnahmen
1. Umweltmodelle	I. Entwicklung eines offenen europäischen durch die Industrie getriebenen Standards für Umweltmodelle in den einzelnen Anwendungsfeldern, angepasst an die einzelnen Ausbaustufen und mit davon abhängigen Komplexitätsgraden. II. Aufbau eines durch die öffentliche Hand getriebenen Prozesses und entsprechender Infrastruktur zur Etablierung virtueller Systemvalidierung. Dazu nötig sind: a. Akkreditierte Einrichtungen b. eine öffentlich zugängliche Validierungsumgebung c. weitere Spezifikationen für Validierungen im Feld III. Erstellung einer durch Zulassungsstellen und Gesellschaft akzeptierten Argumentationskette für den Sicherheitsnachweis hochautomatisierter Systeme bestehend aus einer Kombination aus virtueller Freigabe und Brauchbarkeitstests im Feld
2. Lernende Community	I. Aufbau eines durch die öffentliche Hand getriebenen Prozesses zum Lernen aus Feldbeobachtungen. Dazu sind nötig: a. durch die öffentliche Hand akkreditierte Trust Center b. Selbstverpflichtung der Industrie, die dazu relevanten Daten an durch die Industrie akzeptierte Trust Center anonymisiert zur Verfügung zu stellen c. Rückführung der Analyseergebnisse der Trust Center in den Validierungsprozess
3. Architektur	I. Eine durch die Industrie getriebene Standardisierung der Repräsentation der auszutauschenden Informationen zu Objekten und Situationen, um die Kooperation zwischen Systemen zu ermöglichen. II. Eine durch die Industrie getriebene standardisierte funktionale Systemarchitektur für automatisierte Systeme und ihre Komponenten, die kompositionale Sicherheitsnachweise erlaubt und sichere Mindestfunktionalität in degradierten Modi (nach SAE bzw. analogen Spezifikationen in anderen Domänen) unterstützt. III. Ein öffentlich abgestimmter Entwicklungsprozess für hochautomatisierte Systeme, inklusive sicherer Upgrade-Fähigkeit IV. Ein Industrie getriebener Standard für on-line Zertifizierung/Validierung der Kompatibilität von Upgrades

	mit der existierenden E/E Architektur. V. Sichere, standardisierte Degradationsstufen mit garantierter Mindestfunktionaliät.
4. Absicherung der Interoperabilität autonomer Fahrzeuge	I. International abgestimmte Klassifikation von Ausbaustufen der Architektur von hochautomatisierten Systemen und ihrer Interoperabilität. II. Einführung von Zertifikaten für die Übereinstimmung von Architekturen mit dieser Klassifikation, die von durch die öffentliche Hand benannten Stellen vergeben werden. III. International abgestimmte Release-Prozesse für neue Ausbaustufen
5. Framework	I. Bereitstellung einer Plattform mit Basisdienten für autonomes Fahren für die unterschiedlichen Ausbaustufen II. Etablierung von anwendungsspezifischen Industriestandards für Frameworks, der von durch die öffentliche Hand benannten Stellen zertifiziert ist III. Bereitstellung von Representation Engines zur Aktualisierung der jeweils wahrgenommen Umgebungssituation, der Darstellung möglicher Zukünfte sowie zur Ableitung von daraus resultierenden Handlungen.

Für die Entwicklung und vor allem die Anwendung hochautomatisierter Systeme gibt es eine große Anzahl von Herausforderungen in nicht-technischen Bereichen, die bewältigt werden müssen. Einige von diesen werden in der folgenden Tabelle aufgeführt. Obwohl dieses Positionspapier und die begleitende Roadmap den Fokus auf die technische Umsetzung legt, stufen wir die nicht-technischen Bereiche als ebenso relevant ein und sehen diese mit den aufgezeigten technischen Standards und Regularien einhergehend.

Handlungsbereich	Maßnahmen
Training	I. Training des Fahrers bzw. des Fahrzeugführers hinsichtlich a. Nutzung automatisierter Funktionen und (standardisierten) Degradationsmöglichkeiten b. notwendiger Maßnahmen und Handlungen in degradierten Systemzuständen.
Wettbewerbsfähigkeit	I. Analyse von technischen Lösungen bzgl. Markt- und Geschäftsbeschränkungen; Maßnahmen zur Separation oder zum Ausgleich dieser Aspekte (vor allem für die Schaffung einer geeigneten Infrastruktur, von hochredundanten Systemarchitekturen ohne die Gefährdung der Wettbewerbsfähigkeit)
Gesetzliche Haftung	I. Rechtlicher Rahmen für hochautomatisierte Systeme, einschließlich Vorschriften zum Betrieb und zur Haftung bei Unfällen sowie zur Produkthaftung II. Ein von der öffentlichen Hand gesteuerter Prozess und entsprechende Infrastruktur für die Haftung bei Unfällen

	(zum Beispiel hinsichtlich der Nutzung von Sprach-, Video- oder Daten-Aufzeichnungen).

Anhang 1: Teilnehmende Organisationen und Mitwirkende

Organisation	Mitwirkende
Airbus Defence & Space	Ottmar Bender
	Carsten Böttcher
	Dr. Winfried Lohmiller
	Josef Schalk
Airbus DS Electronics and Border Security GmbH	Prof. Dr. Heinrich Daembkes
	Dr. Uwe Kühne
ASES	Henning Butz
ATLAS Elektronik GmbH	Michael Roske
	Dr. Ramona Stach
AVL LIST GmbH	Steffen Metzner
	Dr. Michael Paulweber
AVL Software and Functions GmbH	Dirk Geyer
BMW AG	Dr. Werner Huber
	Thomas Kühbeck
Daimler AG	Mohamed Elgharbawy
DLR e.V.	Dr. Tobias Hesse
	Prof. Dr. Frank Köster
	Prof. Dr. Karsten Lemmer
fortiss GmbH	Gereon Hinz
	Prof. Dr. Alois Knoll
	Dr. Harald Ruess
Fraunhofer IESE	Prof. Dr. Peter Liggesmeyer
	Dr. Daniel Schneider
	Dr. Mario Trapp
ITK Engineering AG	Bernd Holzmüller
	Christoph Riedl
KIT FAST Institute	Mohamed Elgharbawy
OFFIS e.V.	Prof. Dr. Werner Damm
paluno/University Duisburg-Essen	Dr. Andreas Metzger
	Prof. Dr. Klaus Pohl
	Dr. Thorsten Weyer
Robert Bosch GmbH	Peter Heidl
	Dr. Maria Rimini-Döring

SafeTRANS e.V.	Prof. Dr. Werner Damm
	Jürgen Niehaus
Safran Engineering Services GmbH	Brian Grunert
	Felix Hoffmann
Siemens AG	Prof. Dr. Jens Braband
	Bernhard Evers
	Dr. Cornel Klein
	Karl-Josef Kuhn
	Martin Rothfelder
VIRTUAL VEHICLE Research Center	Dr. Michael Stolz
	Dr. Daniel Watzenig

Anhang 2: Relevante Dokumente und Referenzen

[1] ACARE (Advisory Council for Aviation Research and Innovation in Europe) (Eds). FlightPaht 2050 Goals. Luxembourg. 2011
http://www.acare4europe.com/sria,Letzter Zugriff am 30.04.2016

[2] ACARE (Advisory Council for Aviation Research and Innovation in Europe) (Eds.). Strategic Research and Innovation Agenda, Volume 1 and Volume 2.
http://www.acare4europe.com/sria, Letzter Zugriff am 30.04.2016

[3] acatech (Eds.). Neue autoMobilität. Automatisierter Straßenverkehr der Zukunft (acatech POSITION). München. 2015

[4] Bayerisches Staatsministerium für Wirtschaft und Medien, Energie und Technologie (Eds.). Bayerische Luftfahrtstrategie 2030. Munich. 2015

[5] C.E. Billings. Aviation Automation-the search for a human centered approach. Erlbaum, Mahwah, NJ, 1997

[6] Bundesministerium für Verkehr und digitale Infrastruktur (Eds.). Strategie automatisiertes und vernetztes Fahren. Leitanbieter bleiben, Leitmarkt werden, Regelbetrieb einleiten. Berlin. 2015

[7] Bundesministerium für Wirtschaft und Energie (Eds.). Die Luftfahrtstrategie der Bundesregierung. Berlin. 2014

[8] Bundesministerium für Wirtschaft und Technologie (BMWi) (Eds.). Nationaler Masterplan Maritime Technologien (NMMT). Deutschland, Hochtechnologie-Standort für maritime Technologien zur nachhaltigen Nutzung der Meere. Berlin. 2011

[9] ECSS Secretariat: Space engineering: space segment operability. Technical report, ESAESTEC, Requirements and Standards Division, ECSS-E-ST-70-11C, Noordwijk, The Netherlands. 2008

[10] Ericsson AB (Eds.), Ericsson Mobility Report, 2015

[11] ERRAC (The European Rail Research Advisory Council) (Eds). Research and Innovation – Advancing the European Railway. Future of Surface Transport Research Rail. Technology and Innovation Roadmaps. Belgien. 2015

[12] ERTRAC (Eds.). Automated Driving Roadmap. Version 5.0. Status: final for publication. Brüsssel. 2015

[13] Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO (Eds.): Hochautomatisiertes Fahren auf Autobahnen – Industriepolitische Schlussfolgerungen. 2015

[14] Tom M. Gasser, Eike A. Schmidt (Eds.). Bericht zum Forschungsbedarf. Runder Tisch Automatisiertes Fahren. AG Forschung
http://www.bmvi.de/DE/VerkehrUndMobilitaet/DigitalUndMobil/AutomatisiertesFahren/automatisiertes-fahren_node.html, Letzter Zugriff am 30.04.2016

[15] IfM Education and Consultancy Services Limited, University of Cambridge (Eds). UK Marine Industries Technology Roadmap 2015. Cambridge. 2015

[16] MAROS Konsortium. MAROS 2015 – Roadmap-Entwicklung für die Maritime Robotik und Sensorik Auswertung der Workshops und Einarbeitung des Feedbacks der Teilnehmer. Im Erscheinen (Status 2015)

[17] H.R. Maturana, F.J. Varela (1980). "The cognitive process". Autopoiesis and cognition: The realization of the living. Springer Science & Business Media. -S. 13. ISBN 978-9-027-71016-1.

[18] McKinsey&Company (Eds.). Competing for the connected customer – perspectives on the opportunities created by car connectivity and automation. 2015

[19] Nationaler Masterplan Maritime Technologien (NMMT) http://www.nmmt.de. Letzter Zugriff am 30.04.2016

[20] SafeTRANS, Gesellschaft für Informatik, and Verband der Automobilindustrie (Eds.), Eingebettete Systeme in der Automobilindustrie – Roadmap 2015-2030. 2015

[21] P. Scharre and M. C. Horowitz. An Introduction to AUTONOMY in WEAPON SYSTEMS. CNAS WORKING PAPERS (Hrsg.). 2015

[22] VDA (Verband der Automobilindustrie e.V.) (Hrsg.). Automatisierung. Von Fahrassistenzsystemen zum automatisierten Fahren. Berlin. 2015

[23] VDI/VDE-IT (Eds.) EPoSS: European Roadmap. Smart Systems for Automated Driving. Version 1.2. 2015

[24] E. L. Wiener & D. C. Nagel, D.C. Human Factors in Aviation. Academic Press. San Diego, CA. 1988

Anhang 3: Forschungsherausforderungen

Die folgende englisch sprachige Tabelle gibt einen detaillierten Überblick über die Herausforderungen in der Forschung (vergleiche Abbildung 2 in Kapitel 4). Sie enthält den Forschungsbereich samt Forschungsthema mit einer kurzen Erläuterung sowie einer Einordnung zu

- Priorität hinsichtlich der Bedeutung für hochautomatisierte Systeme (**L**ow, **M**edium, **H**igh) und
- zeitlicher Dringlichkeit hinsichtlich des Bedarfs der Resultate, mit folgenden Abstufungen: **S**hort Term (innerhalb von 5 Jahren), **M**edium Term (innerhalb von 10 Jahren), **L**ong Term (nach mehr als 10 Jahren)

Priority List of Research Challenges				
Nr.	**Topic**	**Explanation**	**Priority** (**L**ow, **M**edium,**H**igh)	**Urgency** (**S**hort, **M**edium **L**ong term needed)
1 System Context Models				
1.1	System context modelling	To propose a description method for all aspects of the system context (comprises representations for all possible relevant real world situations in which the vehicle will be acting) meeting the following criteria: • covering all relevant environmental factors • compliance to industry standards on the space of all artefacts in traffic situations (including identification of types of artefacts, physical characteristics of artefacts, behaviour prediction models of such artefacts) and quality attributes (confidence, accuracy) of such information • supporting compositional specification methods for required system reactions in a given set of traffic scenarios • supporting model based V&V methods for type certification of autonomous vehicles	H	S
1.2	Object identification	Define relevant objects, localization and their static and dynamic properties with defined accuracy, calculation complexity, and confidence.	H	S
1.3	Scenario specification	Languages and Methods to specify scenarios as normative behaviour as a basis for homologation purposes, including support for • modular, parametrized specifications • expressing dependencies between scenarios and environmental conditions, such as "this scenario can only be performed if a given set of environmental conditions persist during the execution of this scenario" • consistency checking of scenarios.	H	S – M

1.4	Fault behaviour for exceptional situations	Methods to define fault (and/or degraded) behaviour for exceptional situations in environment perception.	H	S – M
1.5	Test specification	Test specification for autonomous systems and approaches to reduce the exponential growing test complexity in the space of all environment context models	H	S
2 Operator Models				
2.1	Handover scenarios	Methods to guarantee safe handover of vehicle control from technical system to human and vice versa	H	S
2.2	Human health state prediction / human state prediction	Methods to predict human health state (behaviour, capabilities, awareness, emotions, …)	M	Domain-specific: S – L
2.3	Human intention prediction	Methods to predict human intentions	M	Domain-specific: S – L
3 System Architecture for Perception, Cognition and Actuation				
3.1	Architectural principles supporting decomposition of scenario verifications	Methods to design the architecture for situational perception, cognition and actuation in such a way that it allows to decompose the V&V processes for the compliance of autonomous vehicles to specifications as given in scenario catalogues into • V&V arguments insuring such compliance under the assumption of perfect and complete observation of surrounding traffic situations • V&V arguments guaranteeing a sufficiently precise observation of all "relevant" artefacts in traffic situations with sufficiently high levels of confidence along the complete sensor chain including sensor fusion and sharing of traffic situations through vehicle to infrastructure or vehicle to vehicle communication	H	S
3.2	Architectural principles enabling model centred type certification through automated verification	Architectural principles supporting highly automated model based verification methods supporting type certification of autonomous vehicles addressing V&V of their perception, cognitive, and actuation capabilities	H	S
3.3	Architecture principles supporting compositional safety and security proofs	What are architectural principles supporting compositional safety and security proofs?	H	S

3.4	Architectural Principles to support Dynamic safety evaluation and assurance (runtime certification)	a) Dynamic reconfiguration of known 'blueprints' (c.f. ASAAC) b) dynamic integration and certification in open systems	a) L b) M	a) S b) M
3.5	Processing/Fusion of semantically enriched data	Knowledge-based processing/fusion of semantically enriched sensor data and representations of the environment (including accuracy, confidence, etc.)	H	S
3.6	Service oriented framework for deterministic execution of automated functions		H	S
3.7	Fault tolerance layer	To provide a consistent fault tolerance service including • health state monitoring and signalling of health state to situation interpretation capability • intrusion protection and identification mechanisms • self healing mechanisms ensuring max. functuality in degraded health states, automatic isolation of infected/ill system components, dynamic reconfiguration, error redundancy, and other fault tolerance mechanisms	H	S
4 Design				
4.1	Guaranteeing sufficient observability of traffic situations	Design principles to guarantee a sufficient precise observation of all "relevant" artefacts in traffic situations with sufficient high levels of confidence along the complete sensor chain including sensor fusion and sharing of traffic situations through vehicle to infrastructure or vehicle to vehicle communication	H	S
4.2	Safe methods for real-time complexity reduction in situation representation and situation prediction	Methods allowing to determining dynamically based on the mission objectives and the anticipated manoeuvers to determining for each object in the situation representation, the level of required accuracy of the key physical attributes of these objects as well as the accuracy required in predicting the evolution of its future states	H	S
4.3	Reasoning Engines	Representation, prediction and reasoning engine mechanisms to handle all environment situations properly: a) provide a prediction engine to forecast probable futures, b) provide an interpretation languages and engine to derive optimal recommendations of action.	M	M
4.4	Value Governance	Appropriate abstractions for specification and online monitoring of constraints on the behaviour of autonomous	M	L

		system representing value governance.		
4.5	Online synthesis of strategies	How can we efficiently compute online strategies implementing mission objectives, including different alternative options?	H	S
4.6	Safe upgrade in operation	Mechanisms for safe upgrade in operation, including methods for dynamic safety evaluation and assurance (runtime certification) a) upgrade with components/features etc. that in principle were known at design time b) open systems	a) L b) M	a) S b) M
4.7	Self-management and -healing	Mechanisms for self-management of complex safety-relevant Embedded Systems - raise robustness by system-driven re-configuration with respect to the capabilities of the available components during failure situations. a) Reconfiguration according to known 'blueprints' b) open systems	a) L b) M	a) S b) M
4.8	Heterogenous functions	Methods to combine heterogeneous classes of functions.	Domain-specific: M – H	S
4.10	Trade-offs between decentralised or centralised situation prediction, cognition and actuation	What are the key trade-offs in allocating capabilities for situation perception, cognition and strategy synthesis of autonomous systems between on-vehicle capabilities and cloud based capabilities?	M	M
4.11	Learning new situation artefacts and their behaviour	• Algorithms for the identification of additional/new relevant artefacts in situational representations • Algorithms for learning models for predicting the behaviour of such newly identified artefacts	M	L
4.12	Open world approach	Methods to cope with the open world problem	H	M
5 Verification and Validation				
5.1	Sensor Models	To provide sufficiently precise models for sensors as basis for model based verification of perception incl. Characterisation of precision and confidence under all relevant environmental conditions (certified)	H	S
5.2	Validated and Standardized Context and Scenarios	Validated and standardized context models and scenario catalogue, incl. statistically validated models of expected levels of incompliance to traffic regulations	H	S
5.3	Validated Operator Models	Validated models of human operators. Statistically validated models about human behaviour in traffic situations (incl. statistically validated data about their risk acceptance.	H	S

5.4	Compositional safety and security	Methods and tools for compositional safety and security proofs	H	S
5.5	Model centred type certification through automated verification	Highly automated Model based verification methods supporting type certification of autonomous vehicles addressing V&V of their perception, cognitive, and actuation capabilities	H – M	M
5.6	Complexity reduction for testing autonomous vehicles (I)	Methods to decompose the overall safety case for type certification to a model based V&V argumentation assuring safety under the assumption of field test based evidence of a systematically derived set of "local" test cases	H	S
5.7	Complexity reduction for testing autonomous vehicles (II)	How can we guarantee that testing of "short" sequences of scenarios under statistically relevant sets of environmental conditions is sufficient to provide a safety case for testing the vehicle under all possible sequences of scenarios and all environmental conditions?	H	S
5.8	Complexity reduction for testing autonomous vehicles (III)	How can we decompose V&V processes for the compliance of autonomous vehicles to specifications as given in scenario catalogues into • V&V arguments insuring such compliance under the assumption of perfect and complete observation of surrounding traffic situations • V&V arguments guaranteeing a sufficiently precise observation of all "relevant" artefacts in traffic situations with sufficiently high levels of confidence along the complete sensor chain including sensor fusion and sharing of traffic situations through vehicle to infrastructure or vehicle to vehicle communication	H	S
5.9	Handling of Unknowns	Validation methods to ensure safe operation in spite of incomplete/non-reliable/wrong information (fail operational)	H	S
5.10	Verification of strategy-synthesis algorithms	How can we verify that the employed synthesis algorithms meet all system requirements including system safety and value governance constraints?	H	S
5.11	Virtual validation	Methods and tools for virtual validation and test; virtual release environment (incl. Criteria for and Measures of Quality, including abstract test functions for re-use in MIL/SIL/HIL/xIL Environments)	H	S – M
5.12	Abstract Scenarios	Stochastic methods to cover the variance of abstract scenarios to real scenarios.	M	L
5.13	Communication and Cooperation	Test methodology for Communication and Cooperation (System-Human, System-System, System-Environment, System-Infrastructure)	H	S

5.14	V&V for online situation interpretation and prediction	What are V&V methods allowing to establish the correctness of algorithms for online situation interpretation and prediction?	H	S – M
5.15	Safe degraded modes	Methods and tools for ensuring safe operation even in degraded mode resp. outside of specification limits (unknown situations, unknown environments).	M	M
5.16	Virtual Integration Testing	Virtual Integration of System functions, monitoring of invalid emergent behaviour and feature interactions, dynamic integration of application software code from different vendors at runtime and dynamic validation of the resulting behaviour, e.g. by running "licensing" scenarios before the new configuration is used for control of the vehicle	H	S
5.17	V&V of imported components	- Methods and processes for creating certification evidence insuring compliance of module implementations against characterisations for such modules which are to be imported from service providers into the existing architecture of autonomous vehicles, where the module characterisation must encapsulate all information required for a consistency and integrity check of that component into the existing EE architecture - Methods for the online certification of compatibility of imported components with existing EE architecture	H	S – M
5.18	V&V methods for learning components	What combination of offline V&V methods for the verification of learning algorithms with runtime verification methods can be used for online certification of the resulting modification of situation, prediction and intension with respect to system safety and value governance requirements?	M	M
5.19	Context learning	Unsupervised Learning of environment context models for autopoietic systems.	L	L
5.20	Autopoietic systems	How can we analyse and guarantee for self-learning systems that on the basis of learned artefacts, objects, and situations a sufficiently precise situation representations can always be constructed with the required level of confidence? Can this analysis be done on-line, in spite of limited resources? Are there parts of this analysis that can be done offline? Can boundary conditions be established or even learned by the system that ensure a sufficiently high confidence? How can we ensure that learned objects, situations, and strategies are consistent with existing strategies and safety goals?	L	L
6 Self Awareness and System Integrity				
6.1	Integrity	Methods and Tools for ensuring functional-, structural- and semantic integrity. Establishing on-line methods guaranteeing System integrity under all operational conditions in the presence of security	H	S – M

		attacks (includes Authentification)		
6.2	Context integrity	Methods to predict the integrity of context constellations including cloud and infrastructure information to harden systems against security attacks.	H	S – M
6.3	Handling of uncertainty	Methods to handle uncertainty, e.g., in the object recognition and situation interpretation including information from backend	H	S
6.4	On-line verification	on-line verification of system health state and exception conditions	H	S
6.5	Runtime verification of availability of demanded system capabilities	Methods for runtime monitoring ensuring compatibility of capabilities assumed in situation interpretation strategy synthesis vs. current health state provided by fault tolerance layer	H – M	M

Impressum

Herausgeber: SafeTRANS e.V.
Escherweg 2
D-26121 Oldenburg
http://www.safetrans-de.org

Datum: August 2017