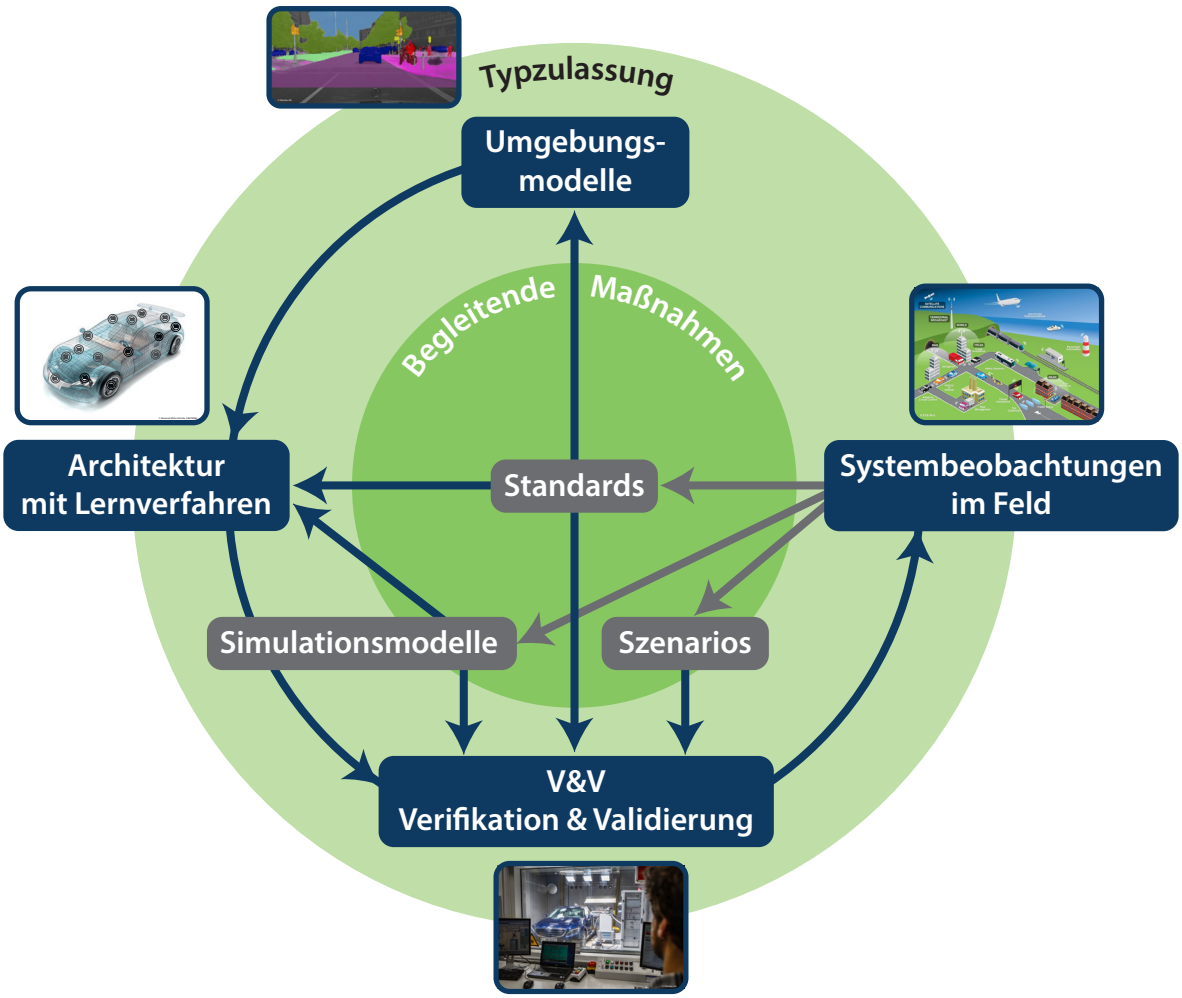
Hochautomatisierte Systeme: Testen, Safety und Entwicklungsprozesse

Roadmap
Forschungsfelder und Handlungsempfehlungen



SafeTRANS
SAFETY IN TRANSPORTATION SYSTEMS

Inhalt

1 Einleitung

1.1 Kontext

Fortschrittliche Assistenz- und Automatisierungsfunktionen, der Informationsaustausch Transportmitteln[1] (Straßenfahrzeugen, Züge, Flugzeuge, ...) wie auch deren Vernetzung mit der Verkehrsinfrastruktur oder mit Hintergrundsystemen entwickeln sich zu unverzichtbaren Bausteinen zukünftiger Transportsysteme und ermöglichen einen immer höheren Automatisierungsgrad der Fahrzeugfunktionen. Neben einer Steigerung des Komforts kann hierüber auch eine weitere Verbesserung in den Sektoren Sicherheit, Effizienz (hier insbesondere Energieeffizienz und die effiziente Nutzung von Wegeinfrastrukturen etc.) und Umwelt (z.B. Reduktion von Schadstoffen und Lärm) in Aussicht gestellt werden. Flankiert wird diese Entwicklung durch einen Trend weg von der ad-hoc Mobilität, hin zur stärker geplanten bzw. organisierten Mobilität, bei der u.a. verschiedene Fahrzeuge (z.B. der individuelle PKW, ein ÖPNV-Angebot und die Bahn bzw. das Flugzeug) in Reiseketten integriert genutzt werden, um Wegstrecken zu bewältigen. Hieraus resultieren hohe Anforderungen an zukünftige Fahrzeuge und Verkehrsinfrastrukturen auf technologischer und struktureller Ebene sowie auf der Ebene der Entwicklungsprozesse.

Die Entwicklung innovativer Fahrzeuge dauert entsprechend lang und ist mit hohen Kosten verbunden. Zudem werden in unterschiedlichen Branchen – z.B. Automotive, Bahn, Luftfahrt und Nautik – teilweise vergleichbare Lösungsansätze unabhängig voneinander entwickelt. Branchenübergreifende Synergien in den Bereichen Entwicklungswerkzeuge, Architekturkonzepte, Soft-/Hardwarebausteine und Testprozeduren sind von daher nach wie vor eine Ausnahme.

Eine wichtige Aufgabe besteht deshalb darin, existierende branchenspezifische Roadmaps (siehe z.B. die im folgenden Abschnitt gelisteten Roadmaps) aufzubereiten und insbesondere hinsichtlich ihrer Anforderungen an

- Entwicklungswerkzeuge und -Prozesse
- Architekturkonzepte und Soft-/Hardwarebausteine
- Testprozeduren
- Nachweise der Funktionalen- und Datensicherheit

zu analysieren. Basierend hierauf können Roadmaps abgeleitet werden, in deren Mittelpunkt nicht Funktionen stehen, sondern die auf Werkzeuge, Architekturen, Komponenten und generische Testmethoden zur Entwicklung und zum Sicherheitsnachweis solcher Funktionen fokussieren. Diese Roadmaps sind neben Fahrzeugherstellern und Herstellern von Verkehrsinfrastruktur insbesondere für die Zulieferindustrie und Dienstleister interessant, welche in die Umsetzung von Produkten und in die Implementierung von Funktionen eingebunden sind. Es entsteht die Möglichkeit domänenübergreifend nutzbare Toolboxen und Kompetenzen aufzubauen, in welche die Erfahrungen aus der gesamten Breite innovativer Fahrzeugentwicklungen und Verkehrsinfrastrukturen einfließen. Diese ermöglichen die zeit- und kostenökonomische Entwicklung von Fahrzeugen und Infrastrukturkomponenten auf hohem Qualitätsniveau.

[1] Im Folgenden wird oft der Begriff „Fahrzeuge“ synonym verwendet.

Entsprechend der oben skizzierten Zielsetzung ist der SafeTRANS Arbeitskreis „Hochautomatisierte Systeme: Testen, Safety und Entwicklungsprozesse“ gestartet, in dem Experten der Branchen Automotive, Bahn, Verkehrsinfrastruktur, Luftfahrt und Nautik zusammenarbeiten. Dieser Personenkreis ist in verschiedenen branchenspezifische Roadmapping-Aktivitäten eingebunden, sodass aufbauend hierauf ideale Ausgangsbedingungen zur Gestaltung einer Roadmap mit Fokus auf branchenübergreifend nutzbare Entwicklungswerkzeuge und -Prozesse, Architekturkonzepte und Soft-/Hardwarebausteine sowie Testprozeduren bestehen. Zudem verfügen die Mitglieder über exzellente Erfahrung in wissenschaftlichen und produktorientierten Projekten.

1.2 Struktur der erstellten Roadmap und Teilziele des Arbeitskreises

Wichtige Ausgangsbasis für die hier erstellte Roadmap ist die Analyse bereits existierender Roadmaps, wie z.B.

- Runder Tisch Automatisiertes Fahren [13, 14]
- VDA – Übersicht zu Automatisierungsfunktionen in PKW [22]
- HOCHAUTOMATISIERTES FAHREN AUF AUTOBAHNEN – INDUSTRIEPOLITISCHE SCHLUSSFOLGERUNGEN [13]
- Smart Systems for Automated Driving [23]
- Ericsson Mobility Report [10]
- Automated Driving Roadmap [12]
- Competing for the Connected Customer [18]
- Positionspapier acatech Neue Automobilität [3]
- Roadmap autonomes Fliegen z.B. von Airbus oder BDLI
- ACARE Strategic Research and Innovation Agenda [2]
- ACARE FlightPath 2050 Goals [1]
- Luftfahrtstrategie der Bundesregierung [18] und Bayerische Luftfahrtstrategie [4]
- Nationaler Masterplan Maritime Technologien (NMMT) [8]
- EPoSS – European Roadmap Smart Systems for Automated Driving [23]
- ERTRAC – Automated Driving Roadmap [12]
- 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. Belgium. 2015 [11]
- UK Marine Industries Technology Roadmap 2015 [15]
- Nationaler Masterplan Maritime Technologien (NMMT). Deutschland, Hochtechnologie-Standort für maritime Technologien zur nachhaltigen Nutzung der Meere. [19]
- MAROS Roadmap [16]

Aus diesen werden die Anforderungen an

- Entwicklungswerkzeuge und -Prozesse
- Architekturkonzepte und Soft-/Hardwarebausteine
- Testprozeduren

extrahiert, zusammengefasst und ergänzt. Wichtige Teilziele der Analysephase sind in diesem Zusammenhang:

1. Etablierung einer branchenübergreifenden Terminologie zur Automatisierung und Vernetzung
   - o für die Automotive-Branche ist z.B. die SAE-Terminologie ein wichtiger Ausgangspunkt:

Summary of Levels of Driving Automation for On-Road Vehicles

This table summarizes SAE International's levels of *driving* automation for on-road vehicles. Information Report J3016 provides full definitions for these levels and for the italicized terms used therein. The levels are descriptive rather than normative and technical rather than legal. Elements indicate minimum rather than maximum capabilities for each level. "System" refers to the driver assistance system, combination of driver assistance systems, or *automated driving system*, as appropriate.

The table also shows how SAE's levels definitively correspond to those developed by the Germany Federal Highway Research Institute (BASt) and approximately correspond to those described by the US National Highway Traffic Safety Administration (NHTSA) in its "Preliminary Statement of Policy Concerning Automated Vehicles" of May 30, 2013.

Level	Name	Narrative definition	Execution of steering and acceleration/ deceleration	Monitoring of driving environment	Fallback performance of *dynamic driving task*	System capability (*driving modes*)	BASt level	NHTSA level
***Human driver* monitors the driving environment**								
0	**No Automation**	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a	Driver only	0
1	**Driver Assistance**	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes	Assisted	1
2	**Partial Automation**	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes	Partially automated	2
***Automated driving system* ("system") monitors the driving environment**								
3	**Conditional Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task* with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes	Highly automated	3
4	**High Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes	Fully automated	3/4
5	**Full Automation**	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**	-	

   - o Weitere Definitionen werden hiermit integriert – z.B. die Darstellung der BASt und des VDA aus der Automotive-Domäne, sowie die unten dargestellten Definitionen der ESA, Autonomie-Level der ESA (European Cooperation for Space Standardisation: Autonomy Levels versus Space Robot Application, nach [9])

Level	Description	Functions
E1	Mission execution under ground control; limited on-board capability for safety issues	Real-Time control from ground for nominal operations Execution of time-tagged commands for safety issues
E2	Execution of pre-planned, ground defined, mission operations on-board	Capability to store time-based commands in an onboard scheduler
E3	Execution of adaptive mission operations on-board	Event-based autonomous operations Execution of on-board operations control procedures
E4	Execution of goal-oriented mission operations on-board	Goal-oriented mission re-planning

- Automatisierungsgrade aus dem Bahnbereich[2]

Basisfunktionen des Fahrbetriebes		Fahren auf Sicht (Sichtfahrbetrieb)	Nicht automatischer Fahrbetrieb	Halbautomatischer Fahrbetrieb	Fahrerloser Fahrbetrieb	Unbegleiteter Fahrbetrieb
		GOA0	GOA1	GOA1	GOA3	GOA4
Sicherstellen sicherer Zug-bewegungen	Sicherstellen einer sicheren Fahrstraße	x (Weichen stellen und überwachen im System)	System	System	System	System
	Sicherstellen der sicheren Abstandhaltung von Zügen	x	System	System	System	System
	Sicherstellen der sicheren Geschwindigkeit	x	x (teilweise überwacht durch System)	System	System	System
Fahren	Steuern und Überwachen von Beschleunigen und Bremsen	x	x	System	System	System
Überwachen des Fahrweges	Verhindern eines Zusammenstoßes mit Hindernissen	x	x	x	System	System
	Verhindern eines Zusammenstoßes mit Personen im Gleis	x	x	x	System	System
Überwachen des Fahrgastwechsels	Steuern und Überwachen der Fahrgastraumtüren	x	x	x	x	System
	Verhindern der Verletzung von Personen zwischen Wagen oder Bahnsteig und Zug	x	x	x	x	System
	Sicherstellen der sicheren Anfahrbedingungen	x	x	x	x	System
Betreiben eines Zuges	Einsetzen/Aussetzen	x	x	x	x	System
	Überwachung des Zugstatus	x	x	x	x	System
Sicherstellen des Erkennens und der Bewältigung von Notfallsituationen	Ausführen der Zugdiagnose, Erkennen von Feuer/Rauch und Entgleisung, Bemerken des Verlustes der Zugintegrität, Behandeln von Notfallsituationen (Ruf/Evakuierung/Überwachung)	x	x	x	x	System und/oder Personal in OCC
ANMERKUNG x = Verantwortlichkeit von Betriebspersonal (kann durch UGTMS-System realisiert werden) System = muss durch UGTMS-System realisiert werden						

GOA: Automatisierungsgrad (en: grade of automation)
UGTMS: Betriebsleit- und Zugsicherungssystem für den städtischen schienengebundenen Personennahverkehr (en: urban guided transport management and command/control system)

- Automatisierungsgrade aus dem maritimen Bereich
  In der maritimen Domäne wird im zivilen Bereich lediglich zwischen ROV (Remotely Operated Vehicle) und AUV (Autonomous Underwater Vehicle) unterschieden. In der Praxis zeigen sich Parallelen zu den oben genannten Stufen der ESA, die sich auch auf den Unterwasser-Sektor übertragen lassen. Der militärische Bereich unterscheidet drei Ausbaustufen (Human “in the loop“, Human “on the loop”, Human “out of the loop”) [21], die sich ebenfalls auf den Betrieb von Unterwasserfahrzeugen anwenden lassen und den Ausbaugrad und die Fähigkeiten eines Vehicles beschreiben.

2. Ableitung einer generischen skalierbaren Gesamtarchitektur und branchenübergreifend nutzbarer Komponenten. Hierzu müssen z.B.
   - die Gesamtarchitektur automatisierter und vernetzter Systeme,
   - funktionale Grundbausteine und deren Schnittstellen,
   - Konzepte zur Selbstbeschreibung und der Beschreibung von Capabilities,
   - Konzepte zur Umgebungsbeschreibung
   - Methoden und Ansätze für die Skalierung der Architekturen

   aufbereitet werden.

3. Identifikation generischer Konzepte in Entwicklungswerkzeugen und –Prozessen.
4. Inhaltliche Präzisierung der Teilstränge der Roadmap.

[2] Nach DIN EN 62290-1 (VDE 0831-290-1): 2015-06 EN 62290-1:2014: Bahnanwendungen – Betriebsleit- und Zugsicherungssysteme für den städtischen schienengebundenen Personennahverkehr – Teil 1: Systemgrundsätze und grundlegende Konzepte

Entsprechend dieser Teilziele des Arbeitskreises gliedert sich die Roadmap wie folgt:
In Kapitel 2 werden zunächst die Motivation für sowie die Herausforderungen bei der Einführung hochautomatisierter Systeme beschrieben. Es schließt sich eine domänenübergreifende Taxonomie der Ausbaugrade hochautomatisierter Systeme an, die die im vorangegangenen Abschnitt dargestellten domänenspezifischen Taxonomien subsumiert. Abschnitt 2.4 beschreibt einen herstellerübergreifenden, aus Beobachtungen im Feld „lernenden" Prozess für die Entwicklung, den Test und die Zertifizierung/Typzulassung hochautonomer Systeme, der zum einen ein zentrales Ergebnis dieser Roadmap-Aktivität darstellt, zum anderen als Hintergrund für die in den folgenden Kapiteln identifizierten Herausforderungen dient.
Kapitel 3 enthält die aus den Herausforderungen abgeleiteten Forschungsthemen, die in sechs Forschungsfelder zusammengefasst werden: Für die Themen „Umgebungsmodelle", „System-Architektur für die Wahrnehmung, Kognition und Aktion" sowie „Verifikation und Validation (V&V)" erfolgt dabei eine detaillierte Analyse der in den jeweiligen Bereichen entstehenden Herausforderungen und daraus abgeleiteten Forschungsfragen und -themen. Hierbei ergeben sich auch Fragestellungen in den Feldern „Design", „Modell des Bedieners" und „Eigenwahrnehmung inkl. Systemintegrität": Kapitel 3.4. enthält eine zusammengefasste Darstellung aller so identifizierten sechs Forschungsfelder. Kapitel 4 schließlich enthält die aus den obigen Betrachtungen abgeleiteten Handlungsempfehlungen, die sowohl die Lösung der technischen Herausforderungen, die Etablierung herstellerübergreifender, gesellschaftlich und politisch akzeptabler Entwicklungs-, Test- und Zulassungsprozesse, als auch die Identifikation weiterer Anforderungen an die Einführung hochautomatisierter Systeme enthält.
Im Anhang der Roadmap findet sich ein Verzeichnis der Referenzen und eine detaillierte, nach Forschungsfeldern und Prioritäten geordnete Auflistung der identifizierten Forschungsthemen.

1.3 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 Institut	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

2 Zielvision

2.1 Motivation, Voraussetzungen und Herausforderungen im Zuge der Realisierung Hochautomatisierter Transportsysteme

2.1.1 Motivation und Effekte der Hochautomation im Transportsektor

Die Nachfrage und der Qualitätsanspruch an Transportkapazitäten für Menschen und Güter – zu Lande, zu Wasser und in der Luft – steigt synchron und stetig mit zunehmender Globalisierung sowie mit der Wohlstandsentwicklung alter und neuer Volkswirtschaften. Insbesondere im Zuge steigender Sozialstandards in Ländern, die eine wachsende Transportlogistik für Menschen und Güter unterhalten, entstehen anspruchsvolle und weitreichende Anforderungen an die Transportmittel in Bezug auf Sicherheit, Zuverlässigkeit, Wirtschaftlichkeit, Verfügbarkeit und Komfort.

Um eine hohe und nachhaltige Qualität der Transportsysteme und Dienste im Sinne der zuvor genannten Anforderungen sicherzustellen, ist eine weitgehende Automatisierung des Transportwesens und der Transportmittel unerlässlich. In [1] wird gezeigt, dass Analysen und Studien zeigen, dass mit steigender Automatisierung von Funktionen im Transportwesen eine proportionale Verbesserung der Sicherheit, des Komforts sowie der Wirtschaftlichkeit des betroffenen Transportsektors einhergehen. Allerdings wirkt diese erfreuliche positive Korrelation zwischen Automatisierungsgrad und Transportqualität nicht über alle Grenzen. Da i.d.R. Menschen an verschiedenen Stellen in die Automatisierungsprozesse eingreifen (Piloten, Fahrer, Lokführer, Steuerleute, Lotsen, Navigatoren, Wartungspersonal sowie auch Entwickler, Designer, Testingenieure, Trainer etc.), kippt der positive Gradient der Qualitätszunahme ab einem bestimmten Automatisierungsgrad ins Negative. Insbesondere die Systemsicherheit nimmt wieder ab [1], [2]. Der Umkehrpunkt befindet sich an jener Stelle, wo die Automation zu viel weitere Komplexität in ein bereits komplexes Bedien- oder Systemumfeld bringt und so beginnt, für die Menschen „im Prozess“ unverständlich oder intransparent zu werden. Ab hier nimmt die Häufigkeit menschlicher Fehler sprunghaft zu. Dabei kann sich der „Prozess“, wo die Fehler auftreten, überall im Lebenszyklus des Produktes befinden: beim Produktentwurf, im Betrieb, bei der Wartung usf. Die Ursachen sind:

- Fehlerhaftes Design (Komplexität)
- Fehlerhafte Integration (funktionale Interoperabilität)
- Lückenhafte Test (State Explosion)
- Integritätsprobleme (unerkannte System-, bzw. Sensorfehler)
- Falsche Prozeduren (Trainingsfehler)
- Bedienungsfehler (Mode Confusion, System Awareness)
- Unklare Mensch-Maschine-Kommunikation (Maschinen-Semantik vs. Humaner Semantik, „Byzantinische Dialoge“, Ablenkung, Mode Confusion)
- Unterforderung (Aufmerksamkeitsdefizite)
- Selbstüberschätzung (erhöhte Risikobereitschaft)
- Konflikte zwischen Systemfunktion und dem operativen Umfeld (Dis-Funktionalität, Validationsmängel)
- Fehlerhafte Wartung (Fehldiagnose, Nichterkennen von Folgefehlern)

Zur Bekämpfung, bzw. Eindämmung der oben aufgeführten Fehlerursachen wurden in den vergangenen Jahrzehnten, seit dem Aufkommen und der Ausweitung komplexer Automatikfunktionen, diverse Methoden und Maßnahmen entwickelt. Im Wesentlichen handelt es sich dabei um:

- Verbesserte Entwicklungsmethoden
    - Requirements Based Engineering (RBE), Model Based Design (MBD), formalisierte Dokumentation, ausführbare Spezifikationen, objektorientierte Programmierung, continous delivery, formale und automatische Testfallgenerierung, etc.
- Fehlertolerante Systemarchitekturen
    - Diversitäre Redundanz, Fehlerdiagnostik, Isolation des Fehlers, Re-Konfiguration im Fehlerfall (inhärente Fehlertoleranz), Sensor-Hybridisierung (Plausibilitätskontrolle von Signalen, Integritätsabsicherung), etc.
- Mensch-Maschine-Interaktion, Human Factor Methoden, Prozeduren
    - Intensivierung des Mensch-Maschine-Trainings, verbesserte Bedien- und Notfallprozeduren, verbesserte Ergonomie, Anzeigen, Ansagen, Bedienelemente etc.
- Wartung
    - Verbesserte Wartungsprozeduren, Prüfmittel und Diagnosesysteme, automatische (Selbst-Tests), fool-proof-design, etc.
- „Smarter" Verkehrsraum, Normierung und Überwachung der Verkehrsräume
    - Verlagerung von Steuer- und Überwachungsfunktionen von Bord der Transportmittel in den Verkehrsraum (Leitstrahlen, Traffic Surveillance, GPS etc.) sowie Schutz der Verkehrsräume gegen „abnorme" Betriebsbedingungen (Einschränkung der Varianz der Betriebsumfeld-Charakteristiken)

Die in der voranstehenden Tabelle genannten Maßnahmen zur Erhaltung hoher Sicherheitsreserven bei weiterhin zunehmende Automation, stoßen in den verschiedenen, hier betrachteten Transportbranchen auf deutlich unterschiedlich hohe Hürden, die ihrer Umsetzung entgegen stehen. Selbst die verwendeten Entwicklungsmethoden und -prozesse differieren zwischen den Branchen erheblich, i.w. hinsichtlich der:

- Standardisierung homogener und kompatibler Entwurfs-Prozesse,
- durchgehenden Verwendung formalisierter (Tool-basierter) Methoden
- der zu erbringenden Nachweise und der Nachweistiefe sowie
- Eindeutigkeit der Entwurfsziele, aufgrund struktureller Unschärfe bei der Definition des Missionsraumes und -profils der Hochautomatisierten Systeme.

Zudem bestehen auch bei der Realisierung und Implementierung fehlertoleranter Systemarchitekturen aufgrund der nahezu entgegengesetzten Kostenmodelle zwischen der Automobilbranche gegenüber der Luftfahrtindustrie erhebliche Unterschiede bei der Umsetzung wirtschaftlich tragfähiger Lösungen. Während bspw. im Flugzeugbau die Entwicklungskosten gegenüber den Gerätekosten die kritischere Größe darstellen, ist es im Automobilbau genau umgekehrt. Deshalb stellt die Realisierung redundanter Systemarchitekturen, mit z.T. 3-facher oder 4-facher Gerätemultiplikation, in Kraftfahrzeugen ein erhebliches Kostenproblem dar. Wesentlicher weiterer Hintergrund ist hier, dass sich in den traditionellen Kfz-Fahrfunktionen ein langjähriger Stand der Technik auf Basis von fail-safe –Sicherheitsfunktionen entwickelt hat, der mit vergleichbar geringer Komplexität implementierbar ist. Die neue Herausforderung für automatisierte Fahrzeugsysteme wird entsprechend ein Paradigmenwechsel im Kostenbewusstsein in Hinsicht auf fehlertolerante bzw. fail-operational-Sicherheitsstrukturen stattfinden müssen, während solche Lösungen bei Luftfahrtsystemen seit Jahrzehnten gängig sind und i.w. nur nach rein technischen Erwägungen entschieden werden. Die Konditionen der Bahnindustrie sowie der Nautik liegen irgendwo dazwischen.

Ein Kostenfaktor, der alle Arten Hochautomatisierter Systeme gleichermaßen betrifft, ist der überproportional steigende Aufwand, der mit der Realisierung zunehmend komplexer Funktionen verbunden ist. Die Funktionskosten wachsen umso stärker, je unklarer die Betriebsbedingungen sind, unter denen das Hochautomatisierte System betrieben wird. Diese hängen sehr wesentlich von den Mechanismen und Vorkehrungen ab, die entweder außerhalb des Transportmittels im Verkehrsraum oder in Wartungszentren getroffen werden oder auf verlässlichen Trainingsabläufen, bzw. auf kontrolliert auszuführenden Bedienprozeduren beruhen. Hier gibt es bedeutende Branchenunterschiede. Während in der Luftfahrt weltweit weitgehend einheitliche Standards für die Luftraumüberwachung, -abgrenzung. -instrumentierung und –steuerung existieren und dort auch die Prozeduren der Verkehrs- und Flugzeugführung am Boden und im Cockpit international vereinheitlicht sind, trifft dies für Bahn und Schifffahrt zumindest noch auf nationaler Ebene zu. Demgegenüber existieren im Bereich des Automobiltransports weder eine ausgeprägte Verkehrsraumüberwachung, -instrumentierung und -abgrenzung, noch abgestimmte internationale Standards hierfür. Ebenso wenig kann sich das automobile Verkehrssystem auf die Einhaltung von normierten Prozeduren bei den Beteiligten des Transportsystems verlassen.

Aus den genannten Gründen sind die Anforderungen an eine hohe Automatisierung im automobilen Transportsektor besonders herausfordernd. Infolge dessen sollen sie hier nachfolgend als richtungsweisend für die Roadmap „Hochautomatisierte Systeme“ betrachtet werden.

2.1.2 Gründe und Arten der Hochautomatisierung im automobilen Transportsektor

Die im vorangehenden Kapitel beschriebenen Umkehr-Effekte der Automation, insbesondere bei der Sicherheit treten beim privaten Automobiltransport wesentlich früher auf, als in anderen Transportbranchen. Die Gründe hierfür sind vielfältig. Im Wesentlichen sind dies:

- Systemarchitekturen, deren Design einer scharfen Konkurrenz zwischen hohen Sicherheitsanforderungen und massiven Kostenbeschränkungen ausgesetzt ist
- Interoperabilitätsprobleme zwischen den Automatiken aufgrund fehlender Kompatibilitätsstandards
- unzählige Verkehrssituationen in einem kaum normierten und unbegrenzten Verkehrsraum, was die Validation der Automatiken und der Sensorik erheblich erschwert
- hohe Vielfalt der automobilen Applikationen, insbesondere im Nutzfahrzeugbereich und off-road
- fehlende normierte Prozeduren der Fahrer sowie eine weite Spanne in deren „skill-level“, was die Validation der Funktionen sowie auch die Verteilung von „Sicherheitsfunktionen“ zwischen dem Fahrer in seinen verschiedenen Rollen (als Fahrer, Halter, Navigator, Passagier etc.) und dem Automaten beim Entwurf der Automatiken erschwert.
- Nahezu ausschließliche Implementierung der Automatikfunktionen und Sensorik an Bord der Fahrzeuge ohne wesentliche Unterstützung durch im Verkehrsraum installierte Sensoren und Funktionen, was die Integritäts- und Verfügbarkeitsanforderungen an die Bordautomatik sowie deren Komplexität in immense Höhen schraubt. Dadurch entstehen weitere massive Konflikte mit allen zuvor genannten Effekten, insbesondere natürlich mit denen der Kostenbeschränkung

Trotz der erkennbaren Gefahr, die Segnungen der Automation durch ihre zunehmende Ausweitung frühzeitig in ihr Gegenteil zu verkehren, wird auch beim automobilen Transport der Automationsgrad in den kommenden Jahren signifikant steigen. Diese Tendenz beruht einerseits auf veränderten Gewohnheiten der Fahrer, die ihre Fahrtzeit mit anderen Aufgaben (bspw. Informationsdienste auswerten) als nur dem Fahren ausfüllen möchten und kommt andererseits zunehmend aus Volkswirtschaften (insbes. BRIC-Staaten), deren automobiler

Transport sich sehr schnell entwickelt, in einem Umfeld äußerst unbestimmter Infrastruktur und wenig geschulter Fahrer. Bei einem Fahrzeugaufkommen wie in entwickelten Volkswirtschaften wären hier (fatale) Unfallraten zu erwarten, die gesellschaftlich nicht akzeptiert würden. Die Bereitschaft dieser Staaten zur Automation für „sichere“ Transportsysteme ist deshalb sehr hoch. Des Weiteren besteht nach wie vor die Tatsache, dass durch Automation sowohl der Komfort (bspw. Stressbelastung), wie auch die Wirtschaftlichkeit (bspw. die Ausnutzung der Infrastruktur) der Transportsysteme deutlich verbessert werden kann. Die Begrenzung der Automation ist deshalb keine Option. Vielmehr geht es darum festzustellen, wie die zuvor genannten Sicherheits- und Integritätsanforderungen an höhere und hohe Automation gemeistert werden können.

Anhand der in diesem Kapitel eingangs angeführten Gründe für das Versagen hoher Automation in klassischen Konfigurationen, lassen sich i.w. fünf Lösungswege beschreiben, in deren Richtung die zukünftige Automation entwickelt werden muss, um die genannten Herausforderungen zuverlässig zu beherrschen.

1. Realisierung hochredundanter, fehlertoleranter Architekturen zur Erhaltung sicherheitskritischer Funktionen im Fehlerfall, die gleichzeitig restriktive Kostenbeschränkungen erfüllen. Hier weist der Vektor zukünftiger Forschungsprogramme eindeutig in die Richtung neuer Methoden der sog. „analytischen Redundanz“, bspw. durch Verwendung Softwarebasierter Schätzverfahren anstelle von redundanten Sensornetzen.
2. Kognitive Automaten, die in der Lage sind, komplexe Situationen selbsttätig zu interpretieren, mit den Sicherheits- und Missionszielen des Transportmittels zu korrelieren und situationsgemäße Automationsregeln adaptiv, spontan zu generieren und auszuführen.
3. Ausstattung der Verkehrsräume mit geeigneten, ggf. noch zu entwickelnden Sensorkonzepten, Überwachungs- und Regelfunktionen sowie mit breitbandiger Kommunikationstechnik (bspw. LTE) zur Übertragung von Verkehrssituations- und Steuerungsinformationen an die Transportmittel. Die hierzu notwendigen Technologien liegen u.a. im Bereich der Forschung zum Thema „Cyber-Physical-Systems“
4. „Sense and Avoid“ Funktionen, um Konflikte mit gering automatisierten Transportmitteln zu vermeiden, die ggf. auch von der Verkehrsraumkommunikation ausgeschlossen sind.
5. Geeignete Methoden und Werkzeuge zur Realisierung, zum Nachweis und zur Unterhaltung der zuvor beschriebenen Automationstypen und -konzepte, die eine Beherrschung der damit verbundenen Komplexität über den gesamten Lebenszyklus der Systeme (Entwicklung, Integration, Produktion, Wartung, Modifikation etc.) sicherstellen.

Aus der Liste sind insbesondere die Maßnahmen 1., 2. und 3. hervorzuheben, da sie im Automobilsektor „Neuland“ bedeuten.

Die kognitive Automation kompensiert die Unzulänglichkeiten und Differenzen in den Fähigkeiten der Transportmittelführer sowie die Unsicherheiten bei der Einhaltung korrekter, normierter Prozeduren auf Seiten der Teilnehmer am Transportsystem. Sie normiert, bzw. ersetzt den heutigen Fahrer in seinen verschiedenen Rollen als Fahrer, Halter, Navigator, Passagier und Überwacher des Transportmittels. Außerdem ist sie lernfähig und kann sich so an Situationen adaptieren, die beim Entwurf der Automatiken nicht bekannt waren und daher nicht validiert werden konnten. Insbesondere ist sie dadurch in der Lage, die Grenzen der Transportsystemautomation mit zunehmender Genauigkeit abzuschätzen, um so rechtzeitig bspw. auf andere Moden umzuschalten oder die Systemführung von der Automation wieder an den Fahrer zurückzugeben, bevor

eine kritische Situation für die Automatik unbeherrschbar wird. Diese Eigenschaften wirken zudem positiv auf die Fehlertoleranz des Gesamtsystems.

Probleme bereiten die kognitiven Automaten dagegen bei der Nachweisführung ihrer Funktionen im Rahmen einer Zulassung des Transportsystems, bzw. seiner kognitiv automatisierten Bestandteile. Verantwortlich ist hierfür die Tatsache, dass die kognitiven Interpretationsmechanismen und Lernfunktionen nicht vollständig deterministisch sind. Diese Aspekte werden im folgenden Kapitel erörtert.

Die Verlagerung von Sensorik sowie damit verbundene Überwachungs- und Steuerungsfunktionen von Bord der Transportmittel in den Verkehrsraum reduzieren den notwendigen Automationsgrad der Fahrzeuge erheblich. Diese Kausalität ist aus der Luftfahrt lange bekannt und wird deshalb dort konsequent angewendet. Außerdem fördert die Automation der Verkehrsräume massiv deren Standardisierung und Harmonisierung, was wiederum die Validation der Bordautomatiken wesentlich vereinfacht.

Demgegenüber erfordert eine solche Maßnahme nicht nur sehr hohe Anfangsinvestitionen in die Infrastruktur, sondern erzeugt auch recht hohe laufende Kosten für die Wartung und Absicherung der Integrität der Verkehrsraumautomation. Für solche Investitionen wird es schwierig, in westlichen Volkswirtschaften geeignete Geschäftsmodelle mit vertretbarem ROI zu definieren. Außerdem werden Prozesse und Regeln benötigt, mit denen die Funktionen des Verkehrsraumes mit jenen der Bordautomatiken und der kognitiven Automaten kontinuierlich (z.B. nach jeder Funktionsmodifikation oder -erweiterung auf jedweder Seite) harmonisiert werden. Auch dieser Aspekt wird im nachfolgenden Kapitel, insbesondere auch im Sinne der Systemnachweisführung und -zulassung erörtert.

2.1.3 Herausforderungen bei der Einführung Hochautomatisierter Transportsysteme

Wie bereits in den voranstehenden Kapiteln erwähnt, stehen insbesondere im Bereich der automobilen Transportsysteme einer hohen und umfangreichen Automation, die den notwendigen Sicherheitsstandard aufrecht erhält, ernstzunehmende Herausforderungen bei deren Implementierung entgegen. Diese sind:

- Die kosten-effiziente Erzielung des erforderlichen Grades an Verlässlichkeit zur autonomen Führung der Systeme durch Verteilung der Aufgaben zwischen System und Infrastruktur
- Die Verifikation komplexer und insbesondere kognitiver Automaten, deren wahrgenommene Information inhärent mit Unsicherheit behaftet ist
- In selbstlernenden Systemen, deren Funktionen aufgrund der mehrschichtigen Vernetzung sowie ihrer autonomen Bewertungs- und Lernfähigkeit nicht deterministisch sind, bleiben wesentliche Verhaltensbestandteile der Automatikfunktionen zur Entwicklungszeit unbekannt und offen, sodass sie nach den heute praktizierten Verfahren weder validiert noch verifiziert werden können.
- Außerdem ist die Zulassungs-, bzw. Zertifizierungsfähigkeit aktuell ungeklärt.
- Die ständige Harmonisierung der Automatikfunktionen an Bord der Transportmittel mit denen, die in ihrem Betriebsumfeld installiert sind. Diese Harmonisierung hat bei jeder Modifikation und Erweiterung einer Funktion innerhalb des Gesamtsystems nach einem festgelegten Prozedere und abgestimmten Regel zu erfolgen, was die Kontrolle durch eine Behörde oder Standardisierungsorganisation nahelegt. Darin enthalten ist auch die Notwendigkeit einer Migrationsstrategie, von dem heutigen Zustand eines weitgehenden Fehlens jeglicher Verkehrsraumüberwachung und Fahrzeugautomation bis hin zu einer Vollausstattung mit Automatiken und Sensoren auf beiden Seiten.

Lösungen für die hier angeführten Herausforderungen, werden ggf. aus Industriebereichen und Volkswirtschaften kommen, die bisher nicht als Protagonisten im Transportsektor aufgetreten sind. Kognitive und semantische Algorithmen, mit denen lernfähige und interpretierende Funktionen realisiert werden, sind heute eher bei Suchmaschinen und Social Network Plattformen im Internet anzutreffen, als in den Entwicklungsabteilungen der Automobilindustrie. Das gleiche gilt für „Big Data“, also der schnellen Isolation von „Bedeutung“ aus massenhaften Daten, die als Roh-Information aus hoch-vernetzten Sensor- und Meldeeinheiten an einer „Bewertungs-„ oder „Verarbeitungsstelle“ zusammenkommen. Dies mag einer der Gründe sein, warum Google gegenwärtig im Bereich des Autonomen Fahrens Aufmerksamkeit erregende Aktivitäten entwickelt.

Die Probleme, einen wirtschaftlich tragfähigen Businesscase für den Aufbau und die Unterhaltung einer Verkehrssystem-Infrastruktur zu finden, stellen sich in staatskapitalistisch orientierten Volkswirtschaften, wie China und Russland, weit weniger kritisch dar, als in marktwirtschaftlich ausgerichteten Staaten. Die Gewinne aus Staatsbetrieben der Transportwirtschaft (in China tragen sie bspw. mit mehr als 40% zur chinesischen Gesamtproduktion bei und gehören zu den profitabelsten Unternehmen der Welt, ZEIT-ONLINE, 19.07.2012) lassen sich quasi per politischem Beschluss eines Zentralkomitees in den Aufbau und die Unterhaltung der Infrastruktur eines Verkehrssystems umlenken. Solchen Maßnahmen stehen in kapitalistischen Volkswirtschaften verständliche Profitinteressen der Privatwirtschaft entgegen. Das gleiche gilt sinngemäß für die notwendige diversitär redundante Geräteausstattung an Bord der Transportmittel, da die Preisgestaltung der Produkte in staatlich organisierten „Supply Chains“ wesentlich willkürlicher gestaltet werden kann, als in marktwirtschaftlich agierenden Unternehmen einer Kunden-Lieferanten Beziehung. Und schließlich fördert und erleichtert das „all-in-one-hand“ Prinzip der hochprofitablen „sozialistisch-staatskapitalistisch“ organisierten Unternehmenskonglomerate ganz erheblich die Adaption und Standardisierung von Bord- und Verkehrsraumsystemen sowie deren permanente Harmonisierung über den Lebenszyklus.

Hinzu kommt, dass in den BRIC Staaten der Druck zu höherer Automation deutlich stärker ist als in entwickelten Staaten, weil sich der Ausbildungsstand der Fahrer zwischen beiden erheblich unterscheidet. Schon heute, bei einem durchaus noch niedrigen Niveau des Individualverkehrs, halten die BRIC Staaten den traurigen Weltrekord bei den Raten fataler Verkehrsunfälle. Um bei weiter anwachsenden Transportkapazitäten – insbesondere im Individualverkehr - zukünftig gesellschaftlich intolerable Unfallzahlen zu vermeiden, ist davon auszugehen, dass die Motivation in den BRIC Staaten sehr hoch sein wird, umfassend in hochautomatisierte Transportsysteme zu investieren. Angesichts der Schäden, bzw. Katastrophen, die es zu vermeiden gilt, wird dabei auch die Bereitschaft, riskantere Lösungen und Technologien für den Verkehr freizugeben sicherlich höher sein, als in entwickelten Volkswirtschaften. Die Lernkurve der Erfahrungen mit hochautomatisierten Transportsystemen wird daher in „Emerging Countries“ vermutlich deutlich schneller durchlaufen werden als in den „Developed Countries“.

Als Schlussfolgerung aus diesen eher volkswirtschaftlichen und gesellschaftspolitischen Betrachtungen resultiert, dass im globalen Wettbewerb den entwickelten Nationen bei der Realisierung Hochautomatisierter (Straßen-)Verkehrssysteme nicht nur technische, sondern auch volkswirtschaftliche und –politische Hindernisse entgegen stehen, die in den „Emerging Countries“ nicht oder zumindest in weit geringerer Ausprägung vorhanden sind.

Zusammenfassend ergeben sich aus den hier angestellten Betrachtungen zu den Voraussetzungen und Hindernissen der Realisierung Hochautomatisierter Transportsysteme die folgenden Handlungsfelder für eine Agenda im Sinne dieser Roadmap:

1. Entwicklung von Konzepten einer verteilten Automationsarchitektur zwischen bordgebundener und ausgelagerter Funktionalität
2. Entwicklung von Methoden der vollständigen Validation Hochautomatisierter Systeme in einem weitgespannten und in Bereichen unbestimmten Betriebsumfeld
3. Definition von Verfahren zur kontinuierlichen Kontrolle, Wartung und Harmonisierung der bordzentrierten und dislozierten Funktionseinheiten zur Aufrechterhaltung der „Transport-Worthiness“ des Transportsystems
4. Analyse der Abhängigkeit technischer Lösungen von marktwirtschaftlichen Gegebenheiten und Definition von Lösungsansätzen zur Trennung, bzw. Kompensation solcher Abhängigkeiten. Dies betrifft insbesondere die Realisierung von im Verkehrsraum verteilter Automation und Sensorik sowie die wirtschaftliche Realisierung hochredundanter Automationsarchitekturen an Bord der Transportmittel und im Transportsystem
5. Entwicklung neuer Automationskonzepte auf der Basis kognitiver / semantischer Verfahren
6. Definition von Methoden zur Validation und Nachweisführung offener, kognitiver Automatiken, deren Funktionen und Verhalten zum Zeitpunkt der Entwicklung und auch während des Lebenszyklus‘ nicht strikt determiniert ist
7. Entwicklung von Methoden, Prozessen und Werkzeugen, die die Beherrschung der Komplexität Hochautomatisierter Transportsysteme sicherstellen, insbesondere auch in Gegenwart von nicht strikt determinierten Kognitionsfunktionen und Betriebsbedingungen
8. Klärung auch der rechtlichen Konsequenzen (Produkthaftung, Unfall-Schuldfrage), die durch die Hochautomation eines Transportsystems mit eingeschränkten Kontroll- und Eingriffsoptionen des Operateurs entstehen.
9. Definition von technischen Einrichtungen, die eine eindeutige Klärung der Haftungs- und Schuldfrage bei Unfällen ermöglichen (bspw. Voice-, Video-, Data-Recorder)

Die notwendigen (technischen und formalen) Lösungen und Schritte für Deutschland zur Lösung, bzw. Beseitigung der oben dargelegten Probleme und Fragestellungen werden in späteren Kapiteln dieser Roadmap ausführlich erörtert werden.

2.2 Ausbaustufen der Automatisierung

2.2.1 Motivation

Die Entwicklung automatisierter bis autonomer Systeme befindet noch am Anfang. Die Annäherung der Reaktionen dieser Systeme an menschliches Verhalten mit entsprechenden kognitiven Fähigkeiten muss noch eine Reihe von Evolutionsschritten durchlaufen. Die Theorien und Technologien, auf denen diese Evolutionsschritte basieren, sind noch nicht vollständig entwickelt.

In der Luftfahrt gibt es heute schon eine Vielzahl von autonomen Flugzeugen, welche RPAS (Remotely Piloted Air Systems) heißen. Hier wurde schon ein sehr hoher Automatisierungsgrad erreicht für den Fall dass der Datenlink verloren geht. Die breite Markteinführung erfordert jedoch eine angemessene Zulassung zum Schutz von Dritten am Boden oder in der Luft. Dies ist die höchste Priorität für Autonomieentwicklungen in der Luftfahrt in den nächsten Jahren.

In der Bahntechnik wurden im Nahverkehr fahrerlos fahrende Züge erstmalig in den 1980er Jahren eingeführt und sind heute Stand der Technik. Aktuelle Bemühungen zielen darauf ab, die Anwendung fahrerloser Systeme auf den Fernverkehr, sowohl im Güter- als auch im Personenverkehr, zu erweitern. Im Vergleich zum Nahverkehr bewegen sich die Züge des Fernverkehrs jedoch nicht in einer geschützten und weitaus komplexeren Umgebung, wodurch zusätzliche Gefährdungen, z.B. Hindernisse auf dem Gleis, zu berücksichtigen sind. Zurzeit übernimmt der auf den Zügen vorgeschriebene Lokführer in diesen Fällen die Sicherungsfunktion. Darüber hinaus sind zusätzliche Funktionen, beispielsweise in Rückfallebenen, vorzusehen, die wiederum mit einem zusätzlichen Gefährdungspotential einhergehen. Die vorrangigen Aufgaben im Bereich des Fernverkehrs liegen daher in der Identifikation der notwendigen Aufgaben des Lokführers in einem sehr komplexen Umfeld, der Bereitstellung einer geeigneten und hinreichend sicheren Sensorik, die Integration der neuen Komponenten in die bestehende Systemlandschaft sowie die Erarbeitung einer geeigneten Sicherheitsnachweis- und Zulassungsstrategie, um einen sicheren Betrieb zu ermöglichen.

Im Rahmen maritimer Einsatzszenarien kommen bereits neben den Remotely Operated Vehicles (ROV) ebenso auch Autonomous Underwater Vehicles (AUV) zum Einsatz. Die Anwendungen sind zum Teil militärisch als auch durch zivile Forschungsvorhaben motiviert. Ein grundlegender Unterschied bei der Missionsdurchführung im Vergleich zu den Air- und Land-Systemen besteht darin, dass speziell die autonomen Fahrzeuge (AUV) in der Regel nicht vollständig überwacht werden können, bzw. ein Eingreifen durch den Operator in der Regel nicht möglich ist. Entsprechend wurden bereits Entscheidungsfunktion und Verhalten auf den Fahrzeugen umgesetzt um dessen Einsatz robuster und zuverlässiger zu gestalten.

Dieser Abschnitt unternimmt den Versuch, die erforderlichen Evolutionsschritte im Sinne von Ausbaustufen skizzenhaft aufzuzeigen. Automatisierte bzw. autonome Systeme werden ihre Fähigkeit zu menschenähnlichem Verhalten entlang der Grundfähigkeiten von Systemen zur Perzeption, Aktion und Kooperation entwickeln.

Perzeption definiert dabei die Fähigkeit der Systeme, den relevanten Kontext wahrzunehmen sowie die aktuelle Situation zu interpretieren, sie zu bewerten und Vorhersagen darüber treffen, wie sie sich entwickeln kann. Unter Aktion verstehen wir die Fähigkeit von Systemen, Missionen zu planen und das Potential ihrer Aktuatoren zu nutzen, um zu handeln. Kooperation ist die Fähigkeit von Systemen, mit Maschinen und Menschen auf verschiedenen Ebenen zweckmäßig zusammenzuarbeiten.

Existierende Definition von Ausbaustufen für automatisierte bzw. autonome Systeme, wie die der SAE oder BAST, beschreiben den Grad der Autonomie anhand der Verantwortlichkeit die der Fahrer in verschiedenen Fahrsituationen noch übernehmen muss und welchen Grad an Verantwortung für Aktionen das Fahrzeug übernimmt. Die hier betrachteten Ausbaustufen gehen von diesen Definitionen aus und beschreiben die technische Weiterentwicklung autonomer Systeme und die Engineering Fragestellungen, die sich daraus ableiten.

Im Bereich der maritimen Forschung, die sich speziell mit AUVs und deren Weiterentwicklung befassen, werden mitunter bereits jetzt schon Themen aus den nächsten Entwicklungsstufen bewegt, vgl. Abschnitt

2.2.2. Ein Thema darunter ist aktuell eines, bei dem abgesetzte Sensoren sich sowohl geeignet je nach zugeteilter Aufgabe formieren, als auch eine aktive Anpassung an schwierige Umgebungsbedingungen (Riff, Felsen, Überhänge mit starken Strukturen) zulassen, damit ein vorgegebenes Gebiet erfasst und kartiert werden kann. An deren Umsetzung sind mehrere Fahrzeuge beteiligt die entsprechend Informationen untereinander austauschen. Die Fahrzeuge sind jeweils mit einer anderen Sensorik ausgestattet um entsprechend ihre Aufgabe innerhalb der kompletten Formation zu übernehmen. So ist zum einen die Kollisionsvermeidung ein Thema, als auch die aktive online Mission-Umplanung innerhalb des zu untersuchenden Gebietes.

Zusätzlich befasst man sich bereits mit Ansätzen, die es erlauben, ohne die Hilfe eines Operators in der Regelschleife, eine Servicing-Mission auf ein Fahrzeug zu bringen, bei der Wartungsarbeiten autonom Unterwasser übernommen werden. Denkbare Einsatzszenarien sind hier die Wartung von Pipelines auf dem Meeresgrund und die Instandhaltung von Offshore Windparks.

Um dem Ziel einer einfachen Missionsplanung näher zu kommen, gibt es mittlerweile Bestrebungen den AUVs idealerweise nur noch einen Auftrag zu geben, sowie ein paar Randbedingungen. Ein mögliches Szenario hierzu ist die komplett Erfassung von einem gegebenen Gebiet, wobei es zeitliche Einschränkungen, Anforderungen an die Genauigkeit und Auflösung der Daten geben kann und ggf. auf weitere Vorkommnisse wie Hindernisse, reagiert werden muss.

Eines der wichtigen Themen für den AUV Bereich ist neben dem Nachweise der Machbarkeit ebenso eine zuverlässige Nachweisführung bei der Verifikation und Validierung und der Verbesserung in der Robustheit solcher Verfahren, besonders bei dem Schritt von einem Forschungsvorhaben hin zur Industrialisierung und Zulassung.

2.2.2 Ausbaustufen

Aus heutiger Sicht gehen wir von vier Ausbaustufen aus, die mit einer Phasenverschiebung von ca. einer Dekade parallel entwickeln werden. Die Ausbaustufen wurden in dieser Weise gewählt, weil sie jeweils ganz neue Merkmale für Systeme erschließen müssen, die sich nicht aus der Verfeinerung oder Permutation der vorhergehenden Ausbaustufe ergeben und deshalb zu originär neuen Herausforderungen an die Systemtheorie führen. Die Entwicklung zu hochautomatisierten Systemen ist gekennzeichnet durch die Zunahme 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

Die folgende Tabelle beschreibt die hier betrachteten vier Ausbaustufen automatisierter Systeme:

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*[3] 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.

Nachfolgend werden die vier Ausbaustufen anhand folgender Merkmale charakterisiert.

- **Perzeption**- Wahrnehmung des relevanten Kontext
- **Aktion –** Fähigkeiten zu Handeln
- **Einordnung** in SEA und BAST
- **Kooperation** – Fähigkeit mit anderen Systemen oder Menschen zu kooperieren
- **Systemische Voraussetzungen** - Welche Fähigkeiten muss eine Maschine haben um dieses Verhalten ausführen zu können
- **Systemische Herausforderung –** Welche systemische Herausforderung muss gelöst werden damit diese Systeme gebaut und zugelassen werden können.

[3] "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]

2.2.3 Charakterisierung der Ausbaustufen

Funktionale automatisierte Systeme – z.B. automatisches Einparken,

- **Perzeption**: Die Situation ist im Wesentlichen durch physikalische Größen wie Abstand oder Geschwindigkeit determiniert. Die Struktur der Situation ist quasi statisch. Dynamik wird als Störung in der Situation wahrgenommen und behandelt.
- **Aktion**: Die Funktion wird algorithmisch synthetisiert. Das Fahrzeug folgt im Wesentlichen einer Trajektorie die dynamisch erzeugt wird.
- **Kooperation** – Das System führt die Funktion eigenständig ohne Kooperation mit anderen Systemen aus. Die Schnittstelle zum Menschen wird durch die Mechanismen bei Übergabe der Verantwortung bestimmt.
- **Einordnung (SEA und BAST)**: Funktionale autonome Systeme können teilautomatisiert oder hochautomatisiert sein.
- **Systemische Voraussetzungen**: Frameworks für funktionale automatisierte Systeme stellen Services für die Computing Ressourcen und den deterministischen Ablauf zur Verfügung. Basis Services wie Positionierung, Funktionsbezogene Objekterkennung und einfache Bewegungsmuster werden ebenfalls bereitgestellt.
- Die **Systemische Herausforderung** besteht darin die funktionale Korrektheit und die funktionale Sicherheit des Systems sicherzustellen.

Missionsorientierte automatisierte Systeme – wie z.B. High Way Pilot oder autonome Parkplatzsuche.

- **Perzeption** - Objekte werden ja nach Mission differenziert mit ihren Eigenschaften wahrgenommen. Situationen werden als Relationen zwischen Objekten und z.B. Kartendaten dynamisch erzeugt, Prädiktionen abgeleitet und Interpretiert.
- **Aktion** – Missionen werden situationsbezogen als Kette von Manövern erfüllt. Das System enthält eine Planungskomponente, die die Mission zieleoptimiert (bezüglich Zeit, Verbrauch, Emission, Durchsatz, …) im Rahmen der situativ möglichen Manöver erfüllt.
- **Einordnung (SEA und BAST)**: Das System ist vollautomatisiert. Der Mensch als Rückfallebene steht nicht mehr zur Verfügung.
- **Kooperation** – Das System ist so ausgelegt, dass es seine Mission selbstständig ausführen kann. Dazu kann es sich Hilfsinformationen wie Kartendaten oder Information über verfügbare Parkplätze aus dem Netz selbstständig holen, soweit diese verfügbar sind. Systeme können aber als Sensor dienen und diese Information mit anderen Systemen teilen.
  Die Interaktion mit Menschen beschränkt sich auf die Spezifikation der Mission und die transparente Darstellung des Status der Mission. Weiter ist die Übergabe der Verantwortung am Start der Mission an das Fahrzeug und die Übernahme der Verantwortung am Ende der Mission zu gestalten.
- **Systemische Voraussetzungen** - Neben den Fähigkeiten die schon in funktionalen automatisierten Systemen Teil des Frameworks waren, kommen jetzt Elemente zur Repräsentation, Prädiktion und Interpretation von Situationen dazu. Für die Durchführung der Mission sind Dienste für strategische Planung auf Zieleebene und operative Planung auf Manöver Ebene notwendig. Zudem werden Monitoring Komponenten zur Überwachung der funktionalen Integrität des Systems benötigt.
- **Systemische Herausforderung** – Der Begriff der „funktionalen Korrektheit“ muss sich weiterentwickeln zu „funktionale Integrität“ um auf dieser Basis die Sicherheit des Systems zu gewährleisten. Dazu ist die Fähigkeit zur Diagnose des Eigenzustands notwendig. Da die Information über die Perzeption nicht

100% verlässlich ist, ist die Fähigkeit zum Umgang mit unsicherer Information bei der Repräsentation, Prädiktion und Interpretation von Situationen unerlässlich.

Kooperative automatisierte Systeme

- **Perzeption** – grundsätzlich wie in missionsorientierten automatisierten Systemen. Kooperative automatisierte Systeme sind zusätzlich in der Lage, Informationen über ihre Situation und deren Interpretationen miteinander auszutauschen. Damit erweitern sich die Wahrnehmungsmöglichkeiten von „System lokal" auf die Flotte von Systemen im Umfeld. In der Luftfahrt gibt es heute schon TCAS und ADS-B welche Informationen zur Kollisionsvermeidung zwischen den Teilnehmern automatisch austauschen. Ein optischer oder Radar-Sensor soll jedoch als Rückfallposition in Zukunft integriert werden für den Fall, dass der andere Verkehrsteilnehmer keinen kooperativen Sensor hat.
- **Aktion** – Missionen werden jetzt nicht mehr nur lokal optimiert, sondern mit anderen Verkehrsteilnehmern bezüglich der Strategie, der Ziele oder der durchgeführten Manöver aufeinander abgestimmt.
- **Einordnung (SEA und BAST)**: Das System ist vollautomatisiert. Der Mensch als Rückfallebene steht nicht mehr zur Verfügung.
- **Kooperation** – Kooperation zwischen Systemen findet auf allen Ebenen der Perzeption (Objekterkennung, Situationsrepräsentation, -prädiktion und – Interpretation, Kommunikation bei kooperativen Teilnehmern) und auf allen Ebenen der Aktion (Abstimmung der Ziele, der Pläne und der Manöver) statt. Der Mensch (z.B. als Verkehrsteilnehmer) wird zum Kooperationspartner bei der Erfüllung gemeinsamer Missionen und Zielen, wie z.B. beim Transport, bei der Pflege oder Ausbildung oder als Verkehrsteilnehmer usw.
- **Systemische Voraussetzungen** - Neben den Fähigkeiten wie in den missionsorientierten automatisierten Systemen erweitern sich die Eigenschaften des Frameworks um Komponenten zur Abstimmung von Situationsbewertung, Zielverhandlung, Planungs- und Manöverabstimmung. Das Framework wird ebenfalls Interaktionstechnologien für menschliche Kooperationspartner enthalten die eher auf Intensionen als auf Funktionen beruhen. Zudem ist ein Monitoring der strukturellen Integrität des Systemverbundes (System of Systems) notwendig.
- **Systemische Herausforderung** – Da sich die Systemgrenze dynamisch durch die Kooperationsbeziehung verändert, brauchen wir einen Begriff von struktureller Integrität, um ein sicheres Funktionieren des Systems of Systems zu gewährleisen. Um arbeitsteilig kooperieren zu können brauchen wir Mechanismen zur verteilten Bildung von Hypothesen und der Abstimmung der Interpretationen. Ebenso brauchen wir Mechanismen zur verteilten Planung und der Abstimmung der Handlungsoptionen. Für eine intensionsorientiere Mensch-System-Kooperation brauchen wir Modelle und Theorien über die Interaktionsmuster menschlicher Systemteilnehmer.

Autopoetische Systeme

- **Perzeption**- wie in den kooperativen automatisierten Systemen; zusätzlich werden die Informationen aus dem Umfeld auf neue Muster und Korrelationen hin analysiert und auf Basis bekannter Situationsmuster zu neuen erweiterten Situationsmustern weiterentwickelt. Dabei muss der relevante beobachtete Kontext selbstständig dynamisch erweitert werden.
- **Aktion** – Wie in kooperativen automatisierten Systemen; zusätzlich werden für die erweiterten Situationen angemessene Handlungsstrategien entwickelt und auf ihre Integrität hin überprüft.

- **Einordnung (SEA und BAST)**: Das System ist vollautomatisiert. Der Mensch als Rückfallebene steht nicht mehr zur Verfügung.
- **Kooperation** – Wie in kooperativen automatisierten Systemen; zusätzlich die Fähigkeit Gelerntes auszutauschen, sowohl die Erkenntnisse der Perzeption als auch der (neuen) Handlungsmuster.
- **Systemische Voraussetzungen** - wie in kooperativen automatisierten Systemen; zusätzlich braucht das Framework Fähigkeiten zum „unsupervised learning“, Bildung, Evaluierung und Absicherung von Hypothesen, Erweiterung des Kontexts, Durchführung von Experimenten und Austausch von Erfahrungen auf allen Ebenen.
- **Systemische Herausforderung** – „unsupervised learning“ in allen Ebenen der Perzeption und der Aktion, um selbstständig das Weltmodell in einem System durch angemessene Abstraktionen zu erweitern. Dazu ist ein Begriff von semantischer Integrität notwendig um jede mögliche Erweiterung abzusichern. Autopoetische Systeme werden Entscheidungen treffen, die bisher nur Menschen vorbehalten waren. Dies kann nur erlaubt werden, wenn es eine Möglichkeit gibt, automatisierten Systemen die Werte aus dem jeweiligen Kulturkreis beizubringen, die vom System beachtet und nicht geändert werden können.

2.3 Der Weg zu hochautomatisierten Systemen

Eine zentrale Herausforderung des Autonomen Fahrens stellt angesichts der Umgebungskomplexität die Absicherung der Betriebssicherheit dar. Während die Entwicklung und Auslegung von Straßenfahrzeugen sowie deren rechtliche Rahmenbedingungen in der Vergangenheit den Menschen als verantwortlichen Fahrzeugführer und damit als Mess-, Steuer- und Regelungsglied stets umfasste, bedarf insbesondere die Einführung höherer Automatisierungsgrade eines Umdenkens. Bei höheren Automatisierungsgraden muss das Fahrzeug dazu in der Lage sein, das Umfeld kontinuierlich hinreichend gut zu erfassen, dieses zu verstehen bzw. zu interpretieren und Folgerungen ziehen zu können. Basierend darauf müssen beständig adäquate Handlungen abgeleitet werden. Damit stellt sich die zentrale Frage: welche verkehrlichen Situationen müssen von hochautonomen Fahrzeugen mit welcher Genauigkeit und mit welcher Zuverlässigkeit erkannt werden, damit darauf aufbauend eine autonome Fahrzeugführung erfolgen kann? Wie geben wir im Fahrzeug integrierte selbstlernende Systeme im Feld frei?

Ein zentraler Ansatz des vorliegenden Dokumentes zur Beantwortung dieser Fragestellung stellt der Aufbau eines lernenden Systems dar, in der ausgehend von einem initialen Katalog von zu beherrschenden verkehrlichen Situationen im Rahmen einer Lernkurve dieser in einem durch die öffentliche Hand kontrollierten Prozess schrittweise auf Grund der konkreten Erfahrung im Feld erweitert wird. Abbildung 1 auf der folgenden Seite deutet entscheidende Bausteine dieses Prozesses an.

Allgemein besteht Konsens, dass die traditionellen Methoden der Funktionsabsicherung angesichts der schieren Komplexität der Umgebungssituation nicht ausreichen, um auch nur eine annähernd hohe Überdeckungsrate der denkbaren Umgebungssituation im Feldtest erreichen zu können. Dieses Dokument schlägt in Abschnitt 3.1.1 eine Klassifikation der Komplexität von Umgebungssituationen anhand dreier Dimensionen vor:

1. Welche Situationsklassen müssen wir beherrschen?

2. Welche Artefakttypen umfasst das Umgebungsmodell, und welche Relationen bestehen zwischen den Artefakten? Welche Eigenschaften dieser Artefakte müssen mit welcher Genauigkeit identifiziert werden?

3. Welche Berechungskomplexität ist on-line im Fahrzeug notwendig und was kann zentral (in der Cloud) berechnet werden?

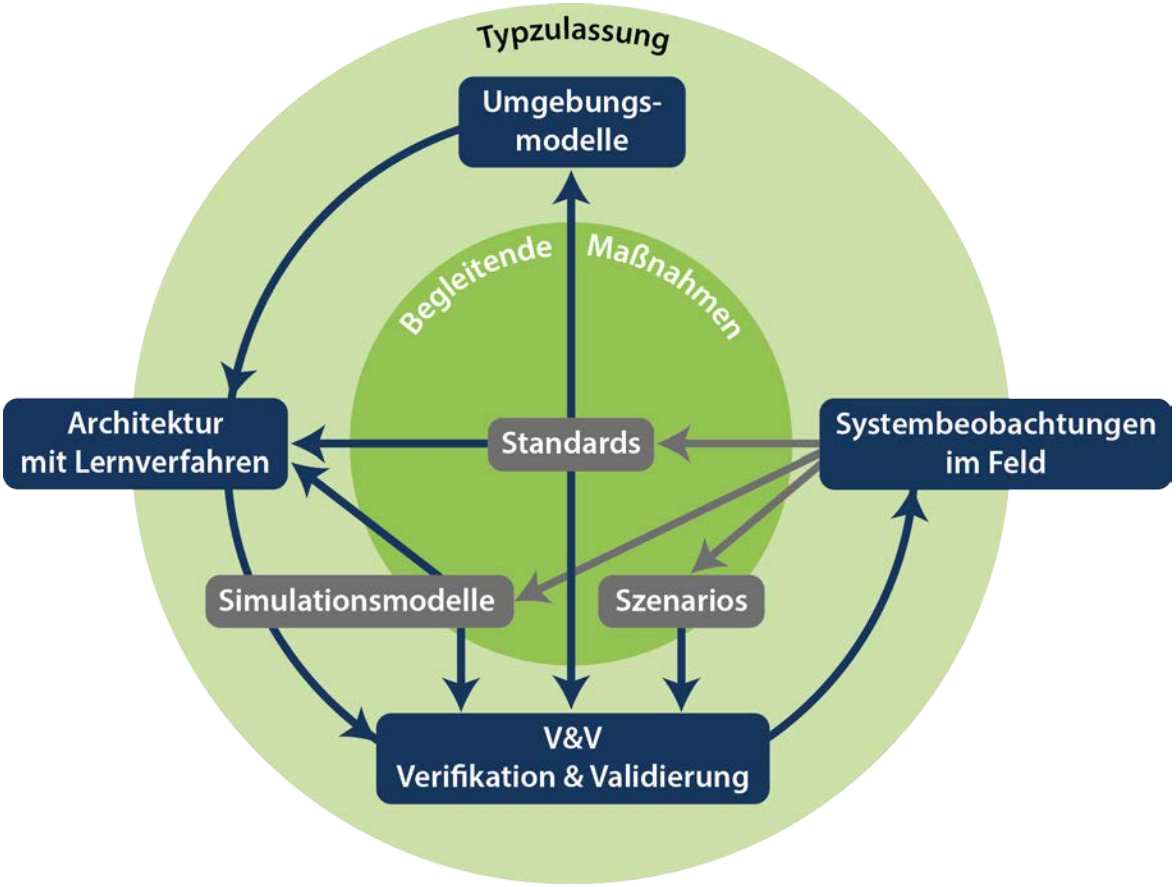


Abbildung 1: Schlüsselelemente eines fortwährenden Lernprozesses aus Beobachtungen im Feld für hochautomatisierte Systeme

Zu Frage 1 ergeben sich die folgenden Teilfragen:

- was ist die relevante Umgebung für die jeweils gegebene zu beherrschende Situation?
- Was ist gültiges Verhalten in diesen Situationen?
- Was ist ungültiges Verhalten?
- Welche Annahmen können wir in den Situationen über Information aus Cloud, Infrastructure oder C2C treffen?
- Wie können wir das Verhalten des Fahrzeugs lernend verbessern?

Frage 2 strukturiert das Umgebungsmodell in die Artefakttypen

- der physikalischen Umgebung (Straßenführung, Straßenzustand, relevante Witterungsfaktoren, ...)
- Verkehrsteilnehmer und Verkehrshindernisse in der relevanten Umgebung des Fahrzeuges
- Fahrerzustand
- aus der Cloud für die autonome Fahrzeugführung verwendete Artefakte

Frage 2 adressiert die Frage der Genauigkeit der Identifikation von Artefakttypen. Werden etwa (über car2X Informationen) dynamische Änderungen des Straßenzustandes („Ölspur“) erkannt? Werden andere Verkehrsteilnehmer so genau klassifiziert, dass eine Prädiktion ihrer Dynamik möglich ist? Welche Fahrerzustände werden erfasst? Lassen diese eine Prädiktion über seine Fähigkeit zur Übernahme der Fahrzeugführung in einer Rückfallsituation zu? Welche Informationen aus der Cloud (Stichwort crowd-sourcing, bsp aktuelle Veränderungen der Fahrbahnführung in Baustellen) werden mit welcher Genauigkeit und welcher Verfügbarkeit erkannt? In der Luftfahrt basiert die Kommunikation nicht über die Cloud sondern über TCAS, ADS-B oder künftig SWIM.

Frage 3 stellt zwar eine abgeleitete Komplexitätsdimension dar, welche allerdings auch umgekehrt als Instrument zur Bewertung der Realisierbarkeit einer komplexen Umgebungswahrnehmung auf der Basis aktueller Prozessortechnologien gesehen werden kann: insgesamt ist die Einschätzung der Experten, dass die zur Verfügung stehende on-line Rechenleistung ein limitierender Faktor in der Beherrschung der obigen Komplexitätsdimensionen darstellt, so dass von Modelltyp zu Modelltyp jeweils unterschiedliche Trade-offs zwischen den ersten beiden Komplexitätsdimensionen zu treffen sind. Insbesondere beschränkt die aktuelle Technologie die Auswahl der initial zu beherrschenden Verkehrssituationen.

So wird schon alleine die zu erwartende Steigerung der on-board verfügbaren Rechenleistung eine dynamische Anpassung der in der Typzulassung zu beherrschenden Umgebungsmodelle bedingen. Nach Auffassung der an der vorliegenden Studie teilnehmenden Experten bedingt allerdings alleine schon die inhärente Unmöglichkeit einer vollständigen Erfassung aller Umgebungskontexte den Aufbau eines lernenden Systems. Die Eingangs dargestellte Leitfrage, welche verkehrlichen Situation mit welcher Genauigkeit, mit welcher Verlässlichkeit wahrgenommen werden müssen, muss schrittweise gelöst werden. Eine Beschränkung auf Einführungsszenarien für hochautomatisiertes Fahren auf etwa Autobahnfahren, oder Fliegen unter IFR Bedingungen, stellt eine deutliche Eingrenzung der Umgebungskomplexität dar. Auch hier sind gemäß der obigen Klassifikation deutlich unterschiedliche Komplexitätsgrade möglich; eine pragmatische Vorgehensweise, welche hier vollständig autonomes Fahren nur in eingeschränkten Witterungssituationen und Abschnitten zulässt, die frei von Wanderbaustellen sind, erlaubt Erfahrungen im Feld zu sammeln und damit höhere Absicherungsgrade für komplexere Verfahren der Objekterkennung wie etwa lernende Algorithmen zu gewinnen. Schließlich bietet der Aufbau eines Lernenden Systems die Möglichkeit, Algorithmen zur Objektidentifikation auf Grund der tatsächlichen Erfahrungen im Feld zu verbessern, etwa in einer weiteren Diversifizierung der Erkennung von Typen von Hindernissen samt deren extrapolierter Dynamik. So könnte durch Regelungen etwa sichergestellt werden, dass im Fahrzeug beobachtete Diskrepanzen zwischen der antizipierten verkehrlichen Umgebung und der tatsächlichen Umgebung zumindest dann automatisch an eine durch die öffentliche Hand einzurichtende Stelle gemeldet werden, wenn diese Diskrepanz zu (Beinahe-)Unfallsituationen führt, so dass ex-post Analysen zu einer Erweiterung der zu berücksichtigen Kontextmodelle führen können, die dann bei einer Typzulassung neuerer Modelle zu berücksichtigen sind.

Abbildung 1 zeigt deswegen auf, das auf Grund von Beobachtungen im Feld dreierlei Einwirkungen erfolgen: zum einen beeinflussen diese Beobachtungen Standardisierungsmaßnahmen, welche die Klasse der zu beherrschende Umgebungssituationen etwa aus Typ-Zulassungssicht regeln. Zum zweiten betreffen diese Beobachtungen dann konkret die Menge der Szenarien, welche im V&V Prozess zu berücksichtigen sind. Hier scheint eine Konvergenz beobachtbar[4], dass durch eine „geeignete" dynamische Kombination parametrisierter Szenarien zumindest für die ersten beiden Artefakte-Typen hinsichtlich eines gegebenen Grades an Umgebungskomplexität ein hinreichend hoher Überdeckungsgrad bei V&V Aktivitäten erzielt werden kann, um in Kombination mit Feldtest eine genügend hohe Funktionssicherheit für diesen Komplexitätsgrad erzielen zu können. Insbesondere werden hierbei intelligent gesteuerte Simulationsverfahren (Stichwort statistical model-checking) eine zentrale Rolle zur Erzielung einer genügend hohen Konfidenz in der Funktionsabsicherung spielen. Darüber hinaus gilt offensichtlich, dass die on-line Fahrzeugarchitektur an sich weiterentwickelnde zu beherrschende Umgebungskomplexitäten adaptiert werden muss – sei es von Modellserie zu Modellserie, oder im Extremfall durch Softwareupgrades, um im Feld erkannte besonders kritische Situationen aufzufangen.

Wenn also nachfolgend Forschungsfelder zur Sicherheit, Architektur, und V&V für hochautonomes Fahren diskutiert werden, sind diese vor dem Hintergrund der Einbettung in ein solches lernendes System zu lesen.

[4] Vgl. z.B. die im durch das BMWI geförderte Verbundprojekt PEGASUS (http://www.bmwi.de/DE/Presse/pressemitteilungen,did=749340.html) oder im Europäischen Verbundprojekt ENABLE-S3 (ECSEL Joint Undertaking, https://www.bmbf.de/de/erfolg-fuer-die-mikroelektronik-2030.html).

3 Forschungsfelder

3.1 Umgebungsmodell

Dieser Abschnitt schlägt eine Taxonomie zur Klassifikation der Komplexität von Umgebungsmodellen vor. Je nach Automatisierungsgrad des Systems (siehe Abschnitt 2.1) kann damit die Komplexität der in Abschnitt 2.2 verwendeten Szenarien der Komplexität der Führungsaufgabe angepasst werden. Es wird empfohlen, die für die Typzulassung verwendeten Szenarien in Abhängigkeit der Komplexität der Führungsaufgabe durch Standards zu regeln. Ein daraus resultierender für einen Fahrzeugtyp gültiger Szenarienkatalog ist wie in Abschnitt 2.2 dargestellt in einen ständigen Überwachungsprozess einzubinden, der überprüft ob in der Praxis die so gegebene Absicherung für die Führungsaufgabe ausreicht, oder gegebenenfalls der Szenarienkatalog anzupassen ist.

3.1.1 Analyse

Ein konkretes Kontext-/Umweltmodell für eine bestimmte Applikation lässt sich anhand von drei Achsen klassifizieren:

- **1. Achse:** Welche Bestandteile/Objekte der realen Welt sind für die Applikation relevant und sollen/müssen daher in dem Kontextmodell modelliert werden?
- **2. Achse:** Welche Genauigkeit/Vollständigkeit der Kontexterfassung ist nötig/möglich?
- **3. Achse:** Welche Berechnungskomplexität resultiert daraus für eine Beherrschung der Szenarien einer durch die ersten beiden Achsen determinierten Komplexitätsklasse von Szenarien

Fundamental für szenarienbasiertes Testen ist eine Normung der in den Szenarien zu berücksichtigenden Artefakte der relevanten Umgebung des Fahrzeuges (andere Verkehrsteilnehmer, Infrastrukturobjekte, Verkehrszeichen, Hindernisse ...). Im Bereich des autonomen Fahrens findet hierzu bereits im Rahmen von Prostep eine herstellerübergreifende Harmonisierung statt.

Für jeden dort identifizierten Artefakttyp ist der Grad an Genauigkeit der Identifikation / Charakterisierung des Artefaktes festzulegen. So mag für Hindernisse ausreichend sein zu identifizieren, ob sie statisch oder dynamisch sind, für andere Verkehrsteilnehmer ist festzulegen, mit welcher Genauigkeit die Objektidentifikation erfolgen muss (z.B. „Kind“ oder nur „Fußgänger“). Für alle Artefakttypen ist festzulegen, mit welcher Genauigkeit deren Lokalisation erfolgen muss. Bei dynamischen Artefakttypen ist festzulegen, welche Modelle für die Prädiktion der Dynamik zu verwenden sind. Somit sind etwa in der höchsten Komplexitätsstufe für alle durch die Norm festgelegten Artefakttypen eine vollständige Objektidentifikation mit höchster Genauigkeit der Lokalisation und detaillierten Modellen zur Prädiktion der Dynamik erforderlich. Für jeden Genauigkeitsgrad ist zu charakterisieren, mit welcher Konfidenz dieser Genauigkeitsgrad erreicht wird. So ist etwa bei Modellen für die Prädiktion des Verhaltens von Fußgängern im Rahmen von standardisierten Szenarien zu charakterisieren, mit welcher Wahrscheinlichkeit Abweichungen vom Prädiktionsmodell auftreten - statistisch relevante Klassen von Abweichungen sind zu dokumentieren und mit Modellen für nicht normatives Verhalten zu unterlegen.

Offensichtlich ist eine Beherrschung einer derart komplexen Umgebungswahrnehmung nur unter bestimmten, durch die Normung ebenfalls festzulegenden Randbedingungen möglich. Diese können zum einen

Witterungsbedingungen charakterisieren, unter denen eine Beherrschung eines solchen Detailgrades der Umgebungssituation möglich ist, aber auch festlegen, dass hierzu das Fahrzeug sich auf weitere Informationsquellen verlassen kann. Diese können aus der Cloud beziehbare aktuelle Kartendaten betreffen, oder durch Infrastruktur oder andere Verkehrsteilnehmer übermittelte Umgebungswahrnehmungen betreffen, wobei in diesem Fall Angaben über die durch diesen Teilnehmer etablierte Konfidenz der Genauigkeit der Wahrnehmung ebenfalls zu kommunizieren ist. Insgesamt ist somit zu erwarten, dass mit zunehmend schärferen Annahmen über die Verfügbarkeit weiterer Informationsquellen sowohl eine differenzierte Umgebungswahrnehmung möglich ist, und dabei eine höhere Präzision mit höherer Konfidenz erzielbar ist.

Teil der „Umgebung“ des Fahrzeuges ist der Fahrer. Auch hier kann durch Normung festgelegt werden, welche Fahrerzustände mit welcher Konfidenz beobachtet werden müssen, damit bestimmte Szenarien durchführbar sind. Dies gilt z. Bsp. für den Nothaltassistenten, in der nur dann auf eine vollautonome Fahrzeugführung umgeschaltet wird, wenn hinreichend sicher ist, dass der Fahrer eine Führungsaufgabe nicht übernehmen kann.

Eine solche explizite Darstellung der Annahmen, unter denen ein Szenario beherrschbar sein muss, ist offensichtlich unverzichtbar für einen Test hochautomatisierter Systeme. Offensichtlich kann selbst unter Einhaltung dieser Annahmen ein solcher Test nur gelingen, wenn keinerlei Fehler die entsprechenden Berechnungen im Fahrzeug beeinflussen. Neben den für eine Typzulassung notwendige Szenarienkatalog samt Klassifikationen der Komplexität und den oben dargestellten Typen von Annahmen ist in der Entwicklung festzulegen, welche Szenarien mit welcher Komplexität bei einem gegebenen degradierten Gesundheitszustand zu beherrschen sind.

Die technische Realisierung einer komplexen Umgebungswahrnehmung ist bis auf weiteres limitiert durch die im Fahrzeug zu Verfügung stehende Rechenleistung. Damit stellt sich in der Festlegung der Anforderungen an hochautomatisiertes Fahren die Notwendigkeit dar unter Berücksichtigung der für eine Generation zur Verfügung stehende Rechenleistung abzuschätzen, wie trade-offs in der Genauigkeit der Umgebungswahrnehmung und Prädiktion für unterschiedliche Umgebungsartefakte zu wählen sind. Offensichtlich steigt die Berechnungskomplexität mit der Anzahl der relevanten Umgebungsartefakte, mit der Anzahl der Freiheitsgrade der Umgebungsartefakte, mit dem Grad an Genauigkeit von Lokalisation und schließlich Prädiktion. Eine darauf basierende Klassifikation der Berechungskomplexität von Umgebungssituationen hilft in der Konzeptphase bei der Abwägung solcher Tradeoffs.

3.1.2 Forschungsfragen

Die obige Darstellung setzt voraus, dass Verfahren zur Sicherung der Konfidenz der Objektidentifikation vorliegen. Für die dazu eingesetzten Lernverfahren sind Methoden zum Nachweise der Konfidenz der sicheren Identifikation von Umgebungsobjekten sowie der Konfidenz im Ausschluss von Scheinobjekten notwendig.

Zur Bewertung der Güte von Szenarienkatalogen muss vor deren Freigabe ein Nachweis erbracht werden, dass diese konsistent und vollständig sind. Szenarien dürfen keine widersprüchlichen Aussagen beinhalten (z.B. bei überlappenden Annahmen von zwei Szenarien zum einen fordern, das ein Nothaltmanöver durchzuführen ist wenn diese verletzt sind, zum andern fordern, dass die eine automatische Spur und Abstandshaltung zu aktivieren ist). Sie müssen darüber hinaus alle während der automatisierten Fahrzeugführung relevanten

Umweltsituationen überdecken. Dazu sind Beschreibungsverfahren zu entwickeln, welche solche Gütenachweise von Szenarienkatalogen erlauben.

Zur Beherrschung der Anzahl der behandelnden Testfälle müssen diese Beschreibungsverfahren eine modulare, parametrisierte Beschreibung samt deren Annahmen unterstützen, welche in der Lage ist, Wechselwirkungen zwischen unterschiedlichen Dimensionen wie etwa Witterungsbedingungen und Dynamikprädiktion darzustellen und gleichzeitig getrennte Beschreibungsmöglichkeiten anbieten um einen exponentiellen Anstieg der Beschreibungskomplexität zu vermeiden.

Schließlich müssen Möglichkeiten zur Beschreibung des erwarteten Systemverhaltens in Ausnahmesituationen entwickelt werden: wie muss mit Fehlklassifikationen entlang der oben dargestellten Komplexitätsgrade der Artefakten Klassifikation umgegangen werden.

Forschungsfragen der Absicherung der Integrität der Umgebungsperzeption auch bei Einbeziehung von Informationen aus der Cloud oder über Car2X Kommunikation betreffen insbesondere den Schutz vor Angriffen, sind aber nicht nur für die Umgebungsperzeption relevant und werden deswegen im Abschnitt über V&V behandelt.

Für den Menschen als „Teil der Umwelt“ und als Kooperationspartner sind relevante Forschungsfragen diejenige nach einer adäquaten Darstellung des für die Fahraufgabe relevanten „Zustands“ des Menschens, einer darauf basierenden Vorhersage der Entwicklung dieses Zustands und der damit verbundenen Fähigkeiten (Capabilities) zur Fahrzeugführung, sowie zu Methoden zur Erkennung seiner Absichten und Ziele.

Schließlich sind Methoden und Prozesse zu definieren, die den in Abschnitt 2.2 definierten Lernprozess ermöglichen. Dazu gehören etwa Verfahren zur Identifikation des Modifikationsbedarfs unter Kenntnis aller für (Beinah) Unfällen oder nicht erkannten Umgebungssituation bereitgestellten Daten über die erkannte Fahrzeugumgebung, den Gesundheitszustand des Fahrzeugs, sowie der aktuellen Manöver/Zielplanung des betroffenen Fahrzeuges (siehe Forschungsgebiet „safe upgrade in operation“ unter V&V).

Für die in Abschnitt 2.1 dargestellte Generation der autopoetischen Systeme stellen sich Forschungsfragen einer Komplexität, die nur grob umrissen werden kann. Wie kann für selbstlernende Systeme nachgewiesen werden, dass das auf der Basis der erlernten Artefakte und Abstraktionen gewonnene Weltbild stets ein je nach Fahrzeugführungssituation genügend genaues Weltbild mit genügend hoher Konfidenz erzeugt? Wie kann dieser Nachweis trotz der beschränkten Rechenressourcen zur Laufzeit erfolgen? Können Teile dieses Nachweises zur Entwurfszeit durch Analyse der für die Identifikation von geeigneten Abstraktionen verwendeten Algorithmen gewonnen werden? Wie können Randbedingungen automatisch gelernt werden, unter denen diese Konfidenz garantiert werden kann? Wie kann sichergestellt werden, dass die gelernten Abstraktionen keinerlei Konsistenzbedingungen des laufenden Systems verletzen?

Insgesamt steht in diesem Abschnitt damit die Frage nach der Vollständigkeit der von einem potentiell unbeschränkten Raum von relevanten Umgebungsartefakten im Raum. Die bereits oben angeschnitten Frage der Vollständigkeit der Umgebung lässt sich approximativ durch Simulation der durch den Szenarienkatalog gegebenen Basisszenarien beantworten. Orthogonal dazu ist jedoch die Frage, ob die für eine Fahrzeugführung relevanten Artefakte alle beobachtet werden. Hier besteht ebenfalls grundlegender Forschungsbedarf, welcher etwa auf aktuellen spieltheoretischen Ansätzen für die formale Synthese von Fahrzeugführungsstrategien aufsetzen kann.

3.2 System-Architektur zur Wahrnehmung, Kognition und Aktion

In der Architektur hochautomatisierter Systeme spiegeln sich die wesentlichen Kernfunktionen wie Wahrnehmung, Aktion und Kooperation sowie Kommunikation wieder. Aufgabe dieses Abschnitts ist es, eine Referenzarchitektur mit ihren funktionalen Elementen einzuführen. Die Architektur muss die Evolution der Systeme im Rahmen der vorhersehbaren Entwicklung abdecken und gleichzeitig die Komplexität durch Definition angemessener Schnittstellen beherrschbar machen. Gleichzeitig muss die Architektur die Aspekte Sicherheit und „value governance“ abdecken.

Der Abschnitt zeigt auf welche Architekturelemente notwendig sind, wo sich Schnittstellen zur Standardisierung anbieten, sowie welche Funktionalität in einem Framework enthalten sein kann. Weiter werden Kernfragen herausgearbeitet und die damit verbundenen Forschungsfragen abgeleitet.

3.2.1 Analyse

Im Gegensatz zu klassischen Embedded Systemen oder „Cyber Physical Systems“, deren Architektur auf die Aktuatorik ausgerichtet ist, orientiert sich die Architektur eines hochautomatisiertes System am Perzeptionsteil mit den Elementen zur Wahrnehmung und Interpretation der relevanten Umwelt inklusive der Selbstwahrnehmung und der Interaktion mit Menschen und Infrastrukturen. Die Information der relevanten Umwelt ist bedingt durch die verfügbaren Sensoren mit Unsicherheit behaftet und damit auch die Repräsentation, Prädiktion und Interpretation der Situation und der daraus abgeleiteten Manöver. Jede Komponente der Architektur muss deshalb Ergebnisse mit einer Konfidenzaussage liefern und das System als Ganzes mit unterschiedlichen Konfidenzgraden umgehen können. Die Selbstüberwachung der für die Konfidenzaussagen einzuhaltenden Systemgrenzen muss Bestandteil eines systemweiten „Health Monitoring“ sein. Die Architektur muss erlauben, dass entsprechend des „System Health States“ das System in sichere Zustände degradiert wird.

Der Aktuator-Teil wird als Service zur Ausführung von situationsangemessenen Manövern betrachtet und ist in sich nach den Regeln klassischer Embedded Systeme entworfen. Da hochautomatisierte Systeme immer als „Connected automated Systems“ gedacht werden müssen ist das Kooperationssubsystem ein weiterer wesentlicher Bestandteil. Für Systeme, die Entscheidungen von immer größerer Tragweite treffen ist Nachvollziehbarkeit eine unverzichtbare Eigenschaft. Zur Sicherstellung dieser Eigenschaft wird die Komponente „Value Governance“ eingeführt.

Das Perzeptionssubsystem besteht aus den Elementen

- Sensorik zur Wahrnehmung der Umwelt und der Objekterkennung und Klassifikation.
- Positionsinformation und Positionserkennung, die alle Information zu einer neuen gültigen Information aggregiert.
- Schnittstelle zu Menschen und Erkennen kognitiver Interaktionsmuster mit Menschen
- Selbstwahrnehmung zur Erkennung des eigenen Gesundheits- und Integritätszustands des technischen Systems inklusive des Sicherheitszustandes.

- Situationsrepräsentation, die den augenblicklichen Zustand des Systems aus der Ego Perspektive in seiner relevanten Umwelt repräsentiert, mit einer situationsabhängigen Aktualisierungsrate
- Situationsprädiktion errechnet wahrscheinliche Zukunftssituationen um die Gültigkeit von Manövern als Reaktion auf die aktuelle Situation abzusichern.
- Situationsinterpretation entscheidet auf Basis der aktuellen Situation und der Prädiktion unter Berücksichtigung der Missionsvorgaben welches Manöver richtig und möglich ist. Die „Value Governance“ setzt hierfür einen Rahmen.

Das Aktionssubsystem besteht aus den Elementen

- Aktuatoren sind funktionale Handlungselemente die Wirkung in der Welt erzielen wie z.B. eine Bremse, ein Antrieb, eine Lenkung, eine Positioniereinrichtung,
- Aktuator Control steuert die einzelnen Aktuatoren auf die jeweiligen Zielgrößen ein
- Aktuator Koordination orchestriert die einzelnen Aktuatoren über der Zeit und gibt die entsprechenden Zielgrößen vor.
- Manöver Planung entwickelt einen Plan nach denen die einzelnen Bewegungselemente ausgeführt werden sollen, dabei werden die Möglichkeiten der Aktuatoren, als auch die Vorgaben der Ziele wie Geschwindigkeit, Verbrauch, Emission, Sicherheit oder andere, berücksichtigt.
- Operational Strategie legt die Rangfolge der Ziele fest nach denen die Manöver ausgeführt werden sollen.

Die Missionsstrategie entscheidet die Handlungsstrategie auf Basis der Optimierung verschiedener Ziele und Entwickelt einen groben Handlungsplan. Sie setzt den Rahmen sowohl für die Planung der Manöver als auch für die Interpretation der Situation und sorgt dadurch für ein konsistentes Systemverhalten im Sinne der Mission.

Das Kooperationssubsystem besteht je nach Kooperationsfähigkeit des Systems aus den Elementen

- Kommunikation stellt die Infrastruktur zur Kommunikation mit anderen Systemen über verschiedene Medien und Basisprotokolle zur Verfügung.
- Wahrnehmungskooperation tauscht mit anderen Systemen Information über die relevante Umwelt aus. Dazu bedarf es standardisierter Protokolle und Metamodelle zum Inforationsaustausch.
- Abstimmung über die Situation tauscht Informationen über die Einschätzung der Situation aus der jeweiligen Perspektive aus.
- Abstimmung über Manöver stimmt zur Erreichung eines gemeinsamen Ziels ab.
- Abstimmung von Zielen (Geschwindigkeit, Emission …) zur Erfüllung der jeweiligen Mission. Dazu bedarf es der Fähigkeit die eigenen Zielgrößen einer übergeordneten unterzuordnen oder eine gemeinsame operationale Strategie mit mehreren Partnern abzustimmen.
- Abstimmung von Missionen um eine übergeordnete Mission zu erfüllen.

Das Value Governance Subsystem sorgt dafür, dass Entscheidungen nachvollziehbar konform zum Wertesystem bleiben und immer nur in vorgegebenen durch den jeweiligen Staat vorzugebenden Grenzen getroffen werden.

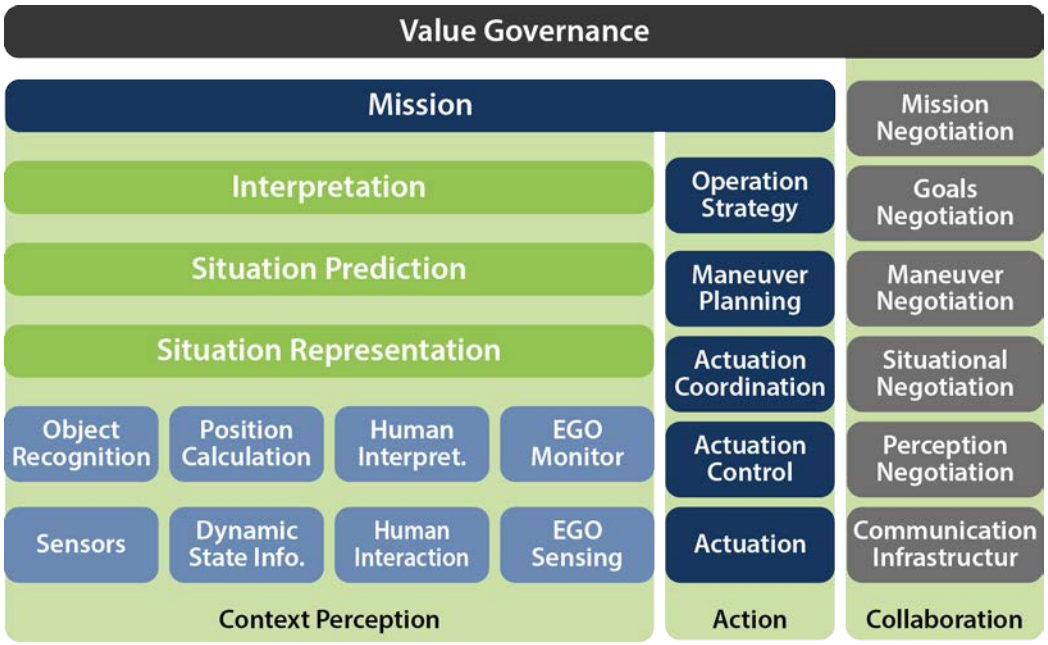


Abbildung 2: Komponenten einer generischen Architektur für hochautomatisierte Systeme

Möglichkeiten für Standardisierung ergeben sich im Bereich

- Sensoren und Objekt Recognition an der Schnittstelle zur Situationsrepräsentation einschließlich Konfidenzaussagen zur Sicherheit der Erkennung / Vermeidung von Fehlerkennungen unter definierten zu überwachenden Umweltbedingungen
- Positionsermittlung und Positionserfassung an der Schnittstelle zur Situationsrepräsentation einschließlich Konfidenzaussagen zur ermittelten Positionen und Systemvoraussetzungen zur sicheren Positionsbestimmung (z.B. höhere Genauigkeit bei hoher Konfidenz bei Verfügbarkeit von Echtzeit digitalen Karten
- Human Interaction und Human Interaction an der Schnittstelle zur Situationsrepräsentation
- EGO Monitoring Spezifikation
- Schnittstelle zwischen Situationsinterpretation und Manöverplanung.
- Framework für Basisservices der Perzeptionsfunktionen, der Aktionsfunktionen und der Kooperationsfunktionen.
- Protokolle zur Kommunikationsinfrastruktur
- Metamodelle für Perzeptionsinformation, Situations-, Manöver-, Ziel- und Missionsabstimmung samt Konfidenzaussagen zur Gültigkeit der zu Grunde liegenden Perzeptionen und Prädiktionen

- Value Governance Spezifikation und Monitoring Formate

3.2.2 Forschungsfragen

Aus den Funktionselementen der Architektur und den Ausbaustufen leiten sich zu den Forschungskomplexen Systemarchitektur, Design und Systemintegrität die folgenden Forschungsfragen ab.

Systemarchitektur für Perzeption, Kognition und Aktion

- Architekturprinzipien, die für die szenarienbasierte V&V eine Dekomposition in (a) V&V unter der Annahme einer perfekten Beobachtung der Umwelt und (b) Nachweis einer ausreichenden Genauigkeit der Umweltbeobachtung mit ausreichender Konfidenz über die gesamte Sensor-Kette – inklusive Sensor Fusion und Einbeziehung von Informationen von anderen Systemen und aus der Cloud -- erlauben.

- Architekturprinzipien, die eine model-zentrierte Typzulassung durch automatische Verifikationsmethoden erlauben.

- Architekturprinzipien, die kompositionelle Safety und Security Nachweise ermöglichen.

- Architekturprinzipien, die Sicherheitsnachweise zur Laufzeit ermöglichen (runtime certification)

- Wissensbasierte Verarbeitung / Fusion von semantisch angereicherten Sensordaten und Umweltrepräsentationen.

- Service orientiertes Framework zur deterministischen Ausführung von Automatisierungsfunktionen.

- Fehlertoleranz-Layer: Konsistente, fehlertolerante Services, die (a) health-state monitoring betreiben und den ermittelten Gesundheitszustand systemweit zur Verfügung stellen, (b) Schutz vor Security-Attacken sowie Erkennen von unbefugten Zugriffen ermöglichen und (c) Selbstheilungs-Mechanismen welche eine jeweils maximal noch mögliche Funktionsfähigkeit des Systems auch in degradierten Gesundheitszuständen bieten und Fehlerisolationstechniken, dynamische Rekonfiguration, Fehlertoleranzverfahren und andere Mechanismen umfassen.

Design

- Entwurfsmethoden und -prinzipien, die eine garantierte Genauigkeit der Umweltbeobachtungen mit ausreichend hoher Konfidenz erlauben

- Angemessene Abstraktionen für die Spezifikation und Darstellung von
  - Situation Repräsentation
  - relevanten Objekten und ihren Attribute

- Reasoning Engines, die eine Interpretation der aktuellen Situation und eine Vorhersage der möglichen Entwicklungen erlauben sowie optimale Handlungsalternativen vorschlagen.

- Spezifikation und Monitoring für Value Governance.

- Methoden zur Online Synthese von Strategien.
- Mechanismen zur abgesicherten „Upgrade“ Fähigkeit im Betrieb (in sicherem Zustand). Dynamische Sicherheitsevaluierung und dynamisches Sicherheitsmanagement.
- Selbst-Management, -Diagnose und –Heilung.
- Methoden zur Integration heterogener Funktionen (statistisch, symbolisch, signalbasiert, algorithmisch, eventbasiert,…)
- Verteilungsarchitektur auf diverse EE und Cloud Konfigurationen, inclusive Trade-Off Betrachtungen zwischen zentraler und verteilter Situations-Wahrnehmung, -Vorhersage, Kognition und Aktion.
- Methoden zum erfahrungsbasierten Lernen neuer Situationen, neuer Artefakte und deren Verhalten.
- Open-World Ansatz: Reduktion der Komplexität auf ein beherrschbares „closed World“ Problem.

Systemintegrität

- Methoden zur Sicherstellung der funktionalen-, strukturellen- und semantischen Integrität.
- Methoden zur Bewertung der Integrität der Umwelt-Wahrnehmung (insbesondere auch des auf Daten aus externen Quellen – Cloud, Infrastruktur – basierenden Teils der Umweltwahrnehmung).
- Behandlung von Unsicherheiten in der Objekt-Wahrnehmung und Situationsinterpretation.

3.3 Verifikation & Validation (V&V)

Im Vergleich zu heutigen teilautomatisierten Systemen, welche für spezifische Situationen und Funktionsausprägungen konzipiert sind, werden hochautomatisierte Systeme für eine erheblich größere Anzahl an auftretenden Situationen ausgelegt. Die Komplexität der zu beherrschenden Situationen lässt demnach keine vollständige Funktionsspezifikation zu, die nach einem V-Modell zu Beginn des Entwicklungsprozesses festgelegt werden kann. Die Anforderungen an eine automatisierte Funktion unterliegen daher keinem definierten Muster und lassen sich dementsprechend nicht mit einer klassischen Methode des statischen Lastenhefts darstellen.

Am Beispiel der Fahrzeugdomäne wird deutlich, dass neue und umfassendere Test-, Validierungs- und Verifikationsmethoden dringend erforderlich sind um vernetzte und automatisierte Fahrzeugfunktionen, welche mit einer sich ändernden Umgebung interagieren, in jeder möglichen Situation und Wetterlage abzusichern (siehe Abbildung 3). Speziell die Absicherung hinsichtlich sogenannter „sensor false positives“ stellt aktuell ein großes Problem dar (z.B. Notbremsassistent: das Fahrzeug bremst ohne ersichtlichen Grund durch eine Fehlinterpretation). Diese sind aktuell auch nicht explizit in der ISO26262 (Funktionale Sicherheitsnorm in der Fahrzeugdomäne) enthalten. Darüber hinaus müssen auch Security-Aspekte sofern diese die Sicherheit beeinflussen entsprechend abgesichert werden.

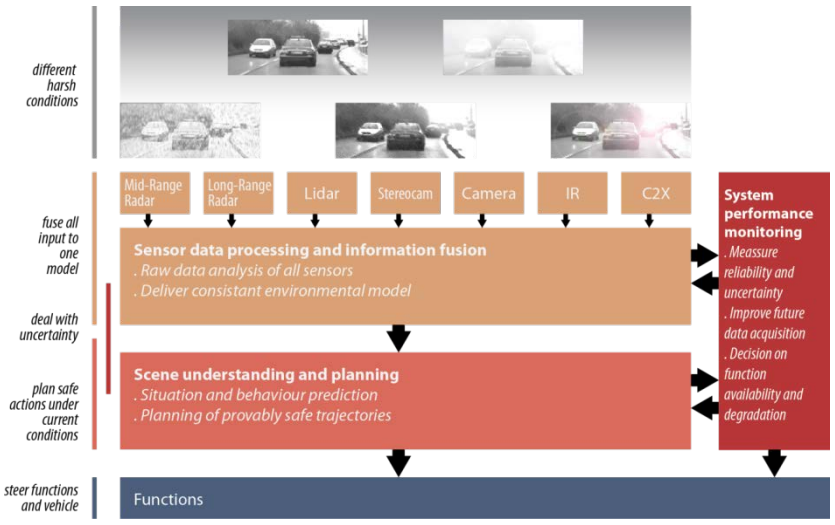


Abbildung 3: Abzusichernde Systemarchitektur eines automatisierten Fahrzeuges (Quelle: ECSEL Projekt RobustSENSE, 2015-2018)

Das Testen sämtlicher möglichen Szenarien im realen Umfeld ist weder für die Fahrzeugindustrie noch für die Flugindustrie oder im Schienenbereich hinsichtlich Kosten und Zeitaufwand leistbar. Wesentliche Erfolgsfaktoren sind daher:

- Verbesserte **virtuelle Testmethoden** um den Aufwand an realen Tests zu senken. In der Automobilindustrie sind nach heutigen Erkenntnissen 100 Mio. bis 4 Mrd. Testkilometer nötig.
- **Segregation**, d.h. Begrenzung der Sicherheitsfunktionen auf ein Minimum und Trennung vom restlichen Funktionsumfang.
- **Sense and Avoid** als Schlüsselthema. Voraussetzung ist allerdings ein validiertes Kontextmodell von kooperativen und nicht-kooperativen Verkehrsteilnehmern. Anhand dieses Modells kann dann gezeigt werden, dass die Kollisionsrate entsprechend gering bzw. deutlich reduziert werden kann.
- **Selbstlernender Ansatz** um agile Entwicklung und agile Validierung zu etablieren. Anhand von mitlaufenden Felderprobungen werden neue Szenarien und Anforderungen erfasst, die dann in eine laufende Softwareverbesserung und immer wieder nachfolgende Validierung einfließen.
- **Selbstdiagnose**: durch unsichere Informationen (Imperfektionen von Sensoren) und dynamischen Szenarien müssen automatisierte Straßen-, Luft-, Schienen-, Wasserfahrzeuge in der Lage sein, nicht getestete Szenarien zu interpretieren und entsprechende Entscheidungen zu treffen (z.B. Fahrerwarnung oder Übergabe). Die Stichworte hierbei sind „fail-operational“ und „fault-tolerant“.
    - **Mindestkatalog an Szenarien**, die zusammen mit Zertifizierungsbehörden definiert werden und Freigaberelevanz für OEMs besitzen. Dieser Mindestkatalog muss entsprechend gepflegt bzw. erweitert werden.

3.3.1 Analyse

Einen großen Beitrag für die Validation und Verifikation eines automatisierten Systems, wird der **virtuelle Systemtest** leisten. Diese Methode erlaubt es, den Szenarienraum für das autonome System aufzuspannen und sukzessive im Entwicklungsprozess zu erweitern. Für eine prospektive, domänenübergreifende Risikobewertung für eine Funktionseinführung müssen hierfür verschiedene, elementare Bausteine des Versuchsdesigns standardisiert werden. Abbildung skizziert, abgeleitet aus dem Beitrag von (Kompass, Helmer, Wang, & Kompass, 2015), einen möglichen Prozess einer künftigen virtuellen Evaluierung automatisierter Systeme und lässt sich in folgende Hauptprozessschritte gliedern:

- Das **Szenarienscreening** erlaubt eine kontinuierliche Betrachtung und Erweiterung des Szenarienraumes auf Basis bestehender Methoden aus den jeweiligen Domänen.
- Im nächsten Schritt der **Szenarienclusterung** werden Szenarien mit gleichem Kontext und Ablaufeigenschaften gruppiert.
- Die **Referenzszenarien** beschreiben den Kern des Testraumes und beinhallten eine Segregation auffälliger, relevanter, und kritischer Szenarien.
- Ein essentieller Schritt der **Umweltmodellierung** bedarf der Darstellung realer Komponenten durch hochwertige und validierte Modelle. In diesem Prozessschritt werden Fahrer, Verkehrsteilnehmer, sowie das System und zugehörige Sensoren modelliert.
- Die **stochastische Variation der Szenarien** erlaubt die nötige Abdeckung des Szenarienraumes zur Identifikation der Funktionsgrenzen und dient zur gesamtheitlichen Funktionsbewertung im Szenarienraum.
- Der abschließende virtuelle Funktionstest auf Basis mannigfaltiger Szenarien erlaubt eine Bewertung der Funktion auf Systemebene und eine Risikobewertung im Szenarienraum.
- Um den Einfluss von verbesserten oder kostenoptimierten Hardwarekomponenten auf das Systemverhalten komplexer automatisierter Fahrzeuge zu untersuchen, sind Szenarientests mit gemischten realen und virtuellen Komponenten erforderlich. Dies erfordert die Entwicklung von echtzeitfähigen Stimuli, die die Signale der virtuellen Komponenten den realen Komponenten einprägen können (Beispiele sind Ultraschall-Stimulatoren, GPS-Stimulatoren, Video-Stimuli, etc.)

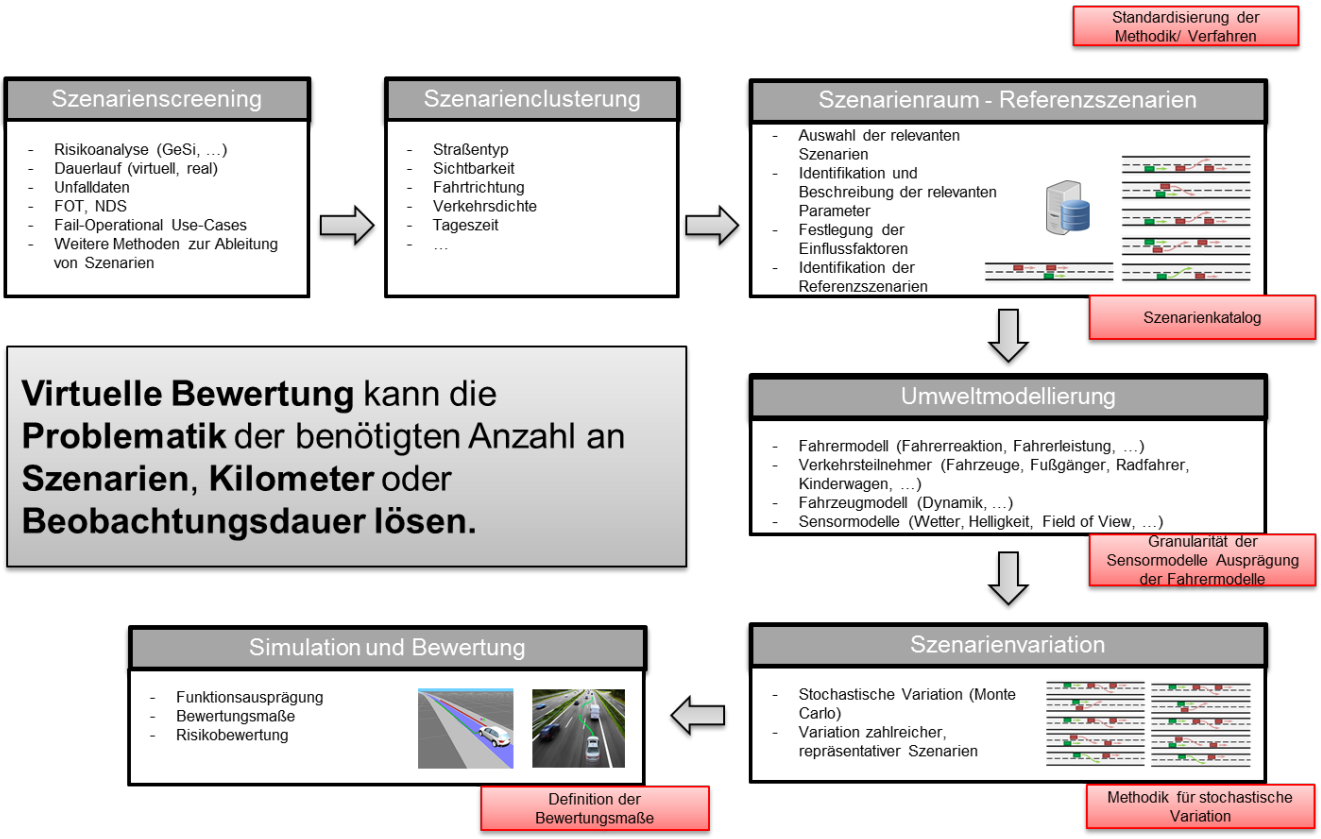


Abbildung 4: Virtuelle Bewertung einer automatisierten Funktion

Das Ableiten verschiedener Effekte aus dem Zusammenspiel diverser automatisierter Systeme benötigt eine Befähigung und Standardisierung von Kernkomponenten im virtuellen Testdesign.

3.3.2 Forschungsfragen

Abbildung weist bereits auf verschiedene Maßnahmen entlang des Prozessbildes hin und lässt auf folgende Forschungsfelder fokussieren:

- **Standardisierung** eines Szenarienkatalogs
- Definition des **Abstrahierungsgrades von Sensormodellen** sowie Standardisierung dieser Modelle
- Ausprägung der **Fahrermodelle** (menschliches Verhalten, stochastische Komponente) für SAE Level 3 und 4 Funktionen
- Entwicklung einer **einheitliche, domänenübergreifende Methode zur stochastischen Variation** von Szenarien
- Definition von **Kriterien** und **Bewertungsmaße** für verschiedene Domänen der Automatisierung
- Definition von abstrahierten Testsystemfunktionen, die einen Reuse von Testszenarien-Definitionen in unterschiedlichen MIL/SIL/HIL/xIL Environments erlauben

Ein künftiges Forschungsfeld stellt die Etablierung einer anerkannten Methode zur intelligenten Verknüpfung verschiedener und bereits vorhandener Testmethoden dar. Abbildung ordnet verschiedene Testmethoden anhand der erzeugten Daten (synthetisch, real) und der Funktionsausprägung (Modulebene, Systemebene) des zu testenden Systems dar. Die dargestellten Methoden dienen zur Wissensaggregation für die Erstellung der Kontextmodelle für das virtuelle Testdesign. Die Qualität der Modelle steht im direkten Zusammenhang mit der Bewertungsqualität der Funktion im virtuellen Test.

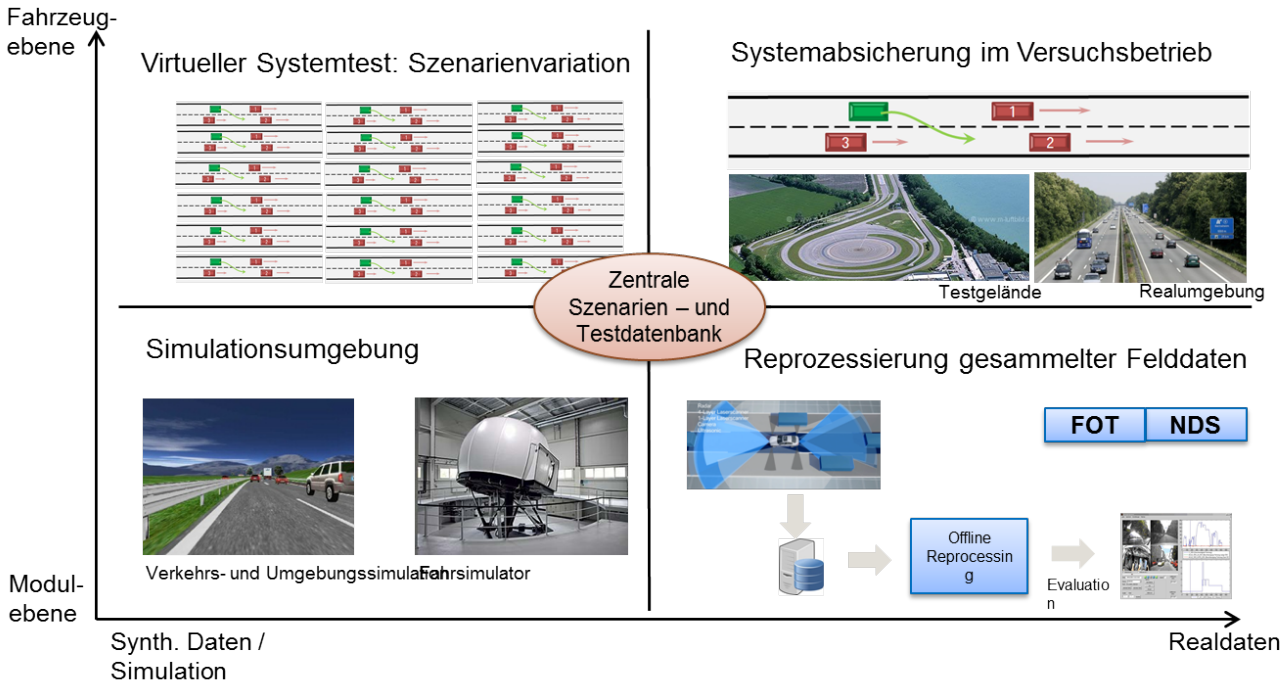


Abbildung 5: Auflistung verschiedener Methoden zur Absicherung automatisierter Systeme

Abbildung zeigt die enge Verknüpfung von virtuellen, hybriden (Hardware in the loop) und Feld- und Flottentests, die über eine gemeinsame Modelldatenbank kommunizieren.

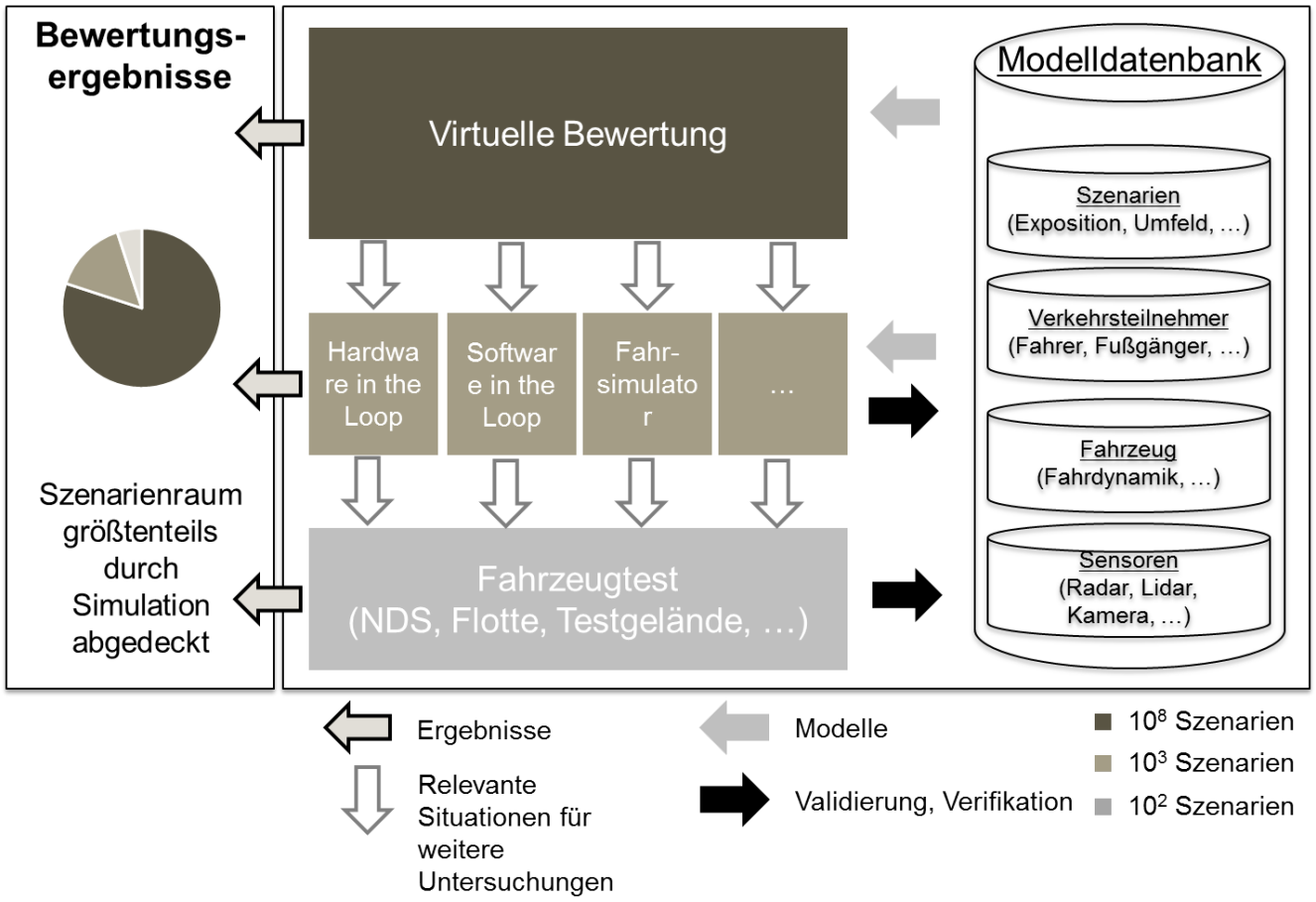


Abbildung 6: Lernende V&V Architektur für hochautomatisierte Systeme

Die Datenbank („model database“) ist Teil eines „lernenden Systems“ und wird ständig mit neuen Felddaten erweitert und aktualisiert. Diese definieren neue Anforderungen, neue Szenarien und neue Testfälle für Entwicklungs- und Testmethoden („agile Entwicklungsmethodik“).

Basierend auf den bisher identifizierten Forschungsfragen lässt sich eine weitere **Detaillierung relevanter Handlungsfelder im Themenfeld Validierung und Verifikation** von hochautomatisierten Systemen ableiten:

- Umfassende Testmethoden für **mehrdimensionale Kommunikationswege** („System of Systems“)
  - System und Mensch (z.B. Übergabe/Übernahme der Fahrzeugführung)
  - System und System (z.B. andere Fahrzeuge – „distributed Sensing“)
  - System und Umwelt (z.B. andere Verkehrsteilnehmer)
  - System und digitale Infrastruktur (Cloud, Backbone etc.)

- Identifikation der dynamischen Systemumgebung/Verkehrssituation – „**Weltmodell**“
    - Welche Artefakte der Systemumgebung (z.B. Verkehrssituation) müssen mit welchen Konfidenzgraden erfasst werden?
    - Wie können wir genügend genaue Projektionen der Weiterentwicklung der Verkehrssituation gewinnen?
    - Wie kann die Integrität solcher internen Weltmodelle sichergestellt werden?
    - Welche Modellierungstechniken können hierfür verwendet werden?
- **Fahrzeugintegrität**
    - Welche **Schutzmaßnahmen** (inkl. Authentifizierungsverfahren) sind erforderlich, um die Integrität eines Fahrzeugs und kooperierender Fahrzeugverbünde sicherzustellen?
    - Durch öffentliche Hand kontrollierte und **abgesicherte statistische Daten** mit Informationen wie sich Verkehrsteilnehmer in potentiell unfallgefährdeten Szenarien verhalten (Eingehen eines gesellschaftlich akzeptierten Restrisikos aufgrund von empirisch abgesicherten Aussagen/Wahrscheinlichkeiten über „rare events“). Ein Beispiel hierfür wäre das Überholen in Baustellensituationen bei engen Fahrspuren.
    - **Vollständigkeitsgrad von vorhandenen Informationen** muss online im Fahrzeug bewertet werden können, um entsprechende Systemreaktionen (Übergabe Kontrolle an Fahrer,...) auszulösen zu können. Insbesondere muss in jeder Situation eine sichere Rückfallebene definiert sein.
    - In Objekterkennung integrierte lernende Verfahren müssen mit durch die öffentliche Hand verwalteten Testfällen angelernt werden. Die **Menge der Testfälle wächst dynamisch**: für jede Fehlerkennungs-Situation wird diese an zentrale Stelle gemeldet
    - Notwendigkeit der **Charakterisierung der Grenzen** aktueller Verfahren/Algorithmen zur automatischen Objekterkennung
    - Sicheres Verhalten bei unsicheren Informationen („**fail-operational**“)
    - **Lernendes Verhalten des Systems** (Selbstdiagnose, d.h. Adaption an konkret beobachtetes Verhalten anderer Verkehrsteilnehmer) bei gleichzeitiger Überwachung eines „Safety-Korridors“ (erlaubte Verhalten des Systems trotz veränderter, gelernter Parameter)
    - **Roadworthiness**, d.h. welche den "Gesundheitszustand" des Fahrzeugs beeinflussende Faktoren können so in Echtzeit überwacht werden, dass jederzeit eine Rückführung auf einen sicheren Zustand gewährleistet werden kann.
- **Hersteller- und Zulieferer-übergreifenden** vorwettbewerblichen Zusammenarbeit
    - „Best Practice Sharing“
    - Identifikation weiterer Forschungsfragen
    - Projektinkubation

Die derzeit bestehende Absicherungs- und Entwicklungsmethodik ist auf Grund der Komplexität nicht direkt übertragbar bzw. linear skalierbar für hochautomatisierte Fahrfunktionen. Dementsprechend ergibt sich folgender methodischer Forschungsbedarf:

- Erschaffung neuer Methoden (inkl. Toolketten) für virtuelle Funktionsbewertung und Evaluierung.
- Bewertung der Vollständigkeit des Testens/der Analysen

- Verfahren zur Bewertung der HMI Schnittstelle, speziell bei Übergabe/Übernahme der Fahrzeugführung
- Verfahren zur Bewertung der Antizipierbarkeit der Fahrzeugführung durch den Fahrer
- Methoden zur Qualitätssicherung von sicherheitsrelevanten aus der Cloud oder Backbone bezogen Informationen
- Generische und Algorithmen (z.B. zertifizierbare Datenfusion)
- Methoden zum Nachweis des sicheren Erkennens von Systemgrenzen
- Qualitätsanforderung bei Einsatz außerhalb der Systemgrenzen und Methoden zu deren Nachweis

3.4 Zusammenfassung identifizierte Forschungsfelder

Die in den vorangegangenen Abschnitten identifizierten Forschungsthemen werden in die in Abbildung 2 dargestellten Forschungsbereiche gruppiert.

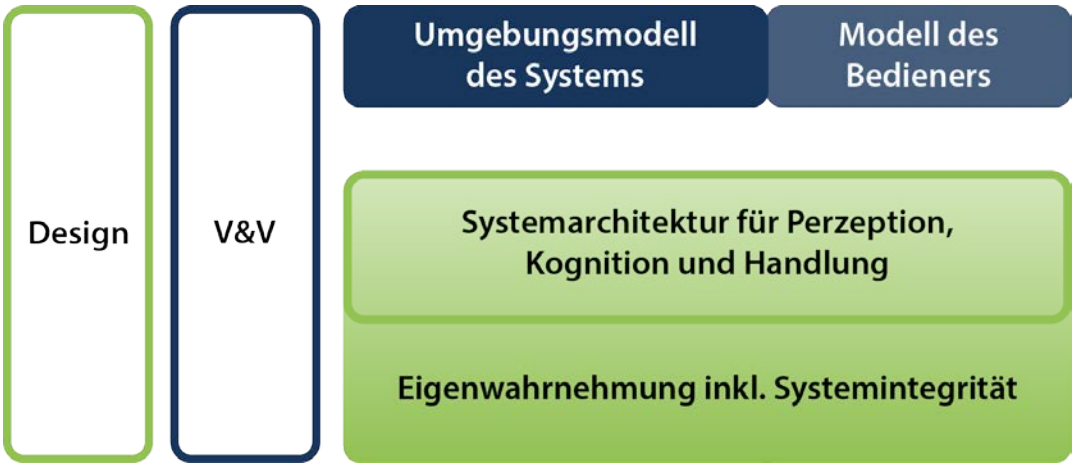


Abbildung 7: Forschungsbereiche

Im Einzelnen behandeln diese Bereiche die folgenden Themen:

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 eine weitere Detaillierungsebene mit den im jeweiligen Bereich identifizierten Forschungsprioritäten dargestellt.

4 Handlungsbedarf und -empfehlungen

Um die wichtigsten Ziele zu erreichen, schlagen wir folgende Maßnahmen vor, die hinsichtlich F&E-Aktivitäten von Industrie und öffentlichen Institutionen parallel umgesetzt werden sollten. Diese konzentrieren sich auf technische Normen und Vorschriften.

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	I. International abgestimmte Klassifikation von Ausbaustufen der Architektur von hochautomatisierten Systemen und ihrer

autonomer Fahrzeuge	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 hochautomatisierte 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 diese Roadmap und das begleitende Positionspapier 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).

Relevante Dokumente and 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

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"	H	S – M

		• consistency checking of scenarios.		
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 system representing value governance.	M	L
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	Methods and tools for compositional safety and security	H	S

	security	proofs		
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 attacks (includes Authentification)	H	S – M
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: November 2017