Highly Automated Systems: Test, Safety, and Development Processes

Research Challenges and Recommendations of Actions

Management Summary

Editors

Peter Heidl, Robert Bosch GmbH

Werner Damm, OFFIS

This document summarizes the key findings and recommendations of the SafeTRANS Working Group "Highly Automated Systems" on regulatory and research challenges to be addressed for cost-effective safe deployment of highly automated systems with excellent quality. We therefore focus on technical challenges and regulatory needs in the overall development process, including architecture and safety aspects as well as V&V (verification and validation). The working group comprised experts from four application domains (automotive, avionics, rail, maritime; see Annex 1 for participating organizations and contributors), striving to identify commonalities and synergies in these domains. It builds on existing roadmaps for highly automated systems both on the national and European level (see Annex 2). The full roadmap will be published in the Summer of 2017, and will in particular include an elaboration and prioritization of the identified research challenges. The document is intended as input for Public Authorities (for regulatory changes and for conceiving corresponding R&D programmes) as well as for industry (to synchronize on R&D activities as well as on standardization).

1 Objectives of this Document

European transportation industries are in danger of losing their leading competitive position to provide sustainable solutions for safe and green mobility across all transportation domains (Automotive, Avionics, Maritime, Rail). Their competitive asset is a profound expertise in developing complex embedded systems[1]. Nevertheless, a bundle of challenges in terms of complexity, safety, availability, controllability, economy and comfort have to be addressed to harvest the opportunities from increasingly higher levels of automation and capabilities outlined in Section 2. These efforts for research, development, validation and infrastructure are so high, that no single organization will be able to afford them. *In order to maintain a leading European position it is therefore necessary to establish collaborations in and across industrial*

[1] see References in Annex 2

domains, learn from field data (Section 3), address the challenges identified in Section 4 and jointly drive the strategic actions (Section 5). Under the overall vision of safety for highly automated transportation systems, the Working Group derived the following key objectives for a joined cross-sectorial R&D strategy:

Key objectives

1. A continuous cross-industry learning processes for the development of highly automated transport systems based upon analysis of fleet data is established, enabling fast take up of new features and capabilities while maintaining and enhancing system safety and performance.

2. A common evolvable fault tolerant system architecture, including onboard systems and infrastructure, is standardized, to facilitate the necessary innovation speed and efficient validation efforts.

3. Research challenges identified in Section 4 are resolved, and methods supporting V&V, engineering and modeling of safe open world systems are developed and matured, allowing model centric validation and verification approaches. An open development environment and a development and validation process accepted by OEMs, regulatory authorities and certification bodies are established.

4. Established deterministic model-centric development approaches are combined with cognitive automation and semantic algorithms, to enable the safe operation of dynamic open world systems and their validation.

5. Self-awareness in systems guarantees that the risk produced by highly automated transport systems is reduced to an acceptable minimum.

6. Man machine interaction and cooperation is enabled on an intentional level. Cognitive automation increases the safety of the system by reducing the unpredictability of human behavior.

7. Traffic space infrastructure and cloud-based infrastructure provide the automated transport systems with validated information about the operational context, enabling safe automated operations and significant reductions in the complexity of the vehicles themselves.

2 Evolution stages of highly autonomous systems

The current state of industrial practice in three transportation domains (Rail, Aerospace, Maritime) already includes Remotely Operating Vehicles (ROVs), systems operating autonomously for restricted time periods and for restricted objectives when the data-link is lost, such as RPAS (Remotely Piloted Air Systems), and even fully autonomous systems such as autonomous underwater vehicles (AUV´s) in the maritime domain, and driverless metros in controlled urban environments. Yet, we are only at the beginning of an evolution of automated and autonomously acting machines. This evolution is characterized by an increase in autonomous system behavior

- in increasingly complex environments
- fulfilling missions of increasing complexity
- including the ability to collaborate with other machines and humans
- and including the capability to learn from experiences and adopt an corresponding behavior.

We see four such evolutionary stages for highly autonomous systems. Each of these stages is characterized by distinguishing novel conceptual properties, inducing new challenges for system theory and architecture. These evolutionary stages will be realized with a phase shift of roughly one decade; market availability of products of neighboring evolutionary stages is expected to overlap, rather than being sequential.

Stage	Characterization
1	*Functional automated systems* handle tasks of limited complexity in an exactly specified context autonomously, like automated parking or automated landing. The mission is planned offline or during development time. The system does not learn during operation, and collaboration with other systems is restricted to the exchange of information about the system context.
2	*Mission oriented systems* fulfill a sequence of tasks, in which each single task is manageable and exactly specified in advance, but their order and the transitions between them are situation dependent, and determined by the system during operation, typically taking into account specified goals like optimizing time or other resource consumption. The system does not learn during operation and collaboration with other systems is limited to the exchange of information about system context and the system itself. Examples are a highway pilot, or exploration and mapping of areas.
3	*Collaborative systems* are able to collaborate with other systems and humans on an intentional level to fulfill their mission, such as for collision avoidance and area surveillance. They negotiate their goals, plans and actions with other systems and humans, and adapt their own behavior to the negotiated plan. They exchange relevant context information, but are not able to learn during operation.

4	*Autopoietic systems*[2] *go beyond self-learning systems in* that they extend autonomously their perception, their situational representation and interpretation of the perceived world, their actions and collaboration patterns, and are able to communicate such learned capabilities to other systems. This is close to human behavior. The ability of (unsupervised) learning during operation is the major characteristic of this class of systems.

We expect these stages to become market reality within the next few decades. Each step has a value of its own and the potential to create economic benefit. Most current systems are functional autonomous systems, and we are on the edge of rolling out mission-oriented systems. Some collaborative systems with simple collaboration schemes exist already. Unsupervised learning during operation is not possible yet, neither now nor in the near future. Progress in this evolution is enabled by progress in corresponding concepts in Research and Engineering, targeting the challenges detailed in the following sections.

3 The Need for Learning from Fleet Observations

Each of the above stages demands for each new system precise answers to the following questions:

1. Which environmental situations have to be recognized and interpreted at which level of precision and confidence so as to enable that level of autonomous behavior?
2. What evidence must be supplied for type certification so as to demonstrate safe and reliable performance?
3. What methods, processes, and regulatory systems must be in place for deploying such systems in the field?

[2] "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]

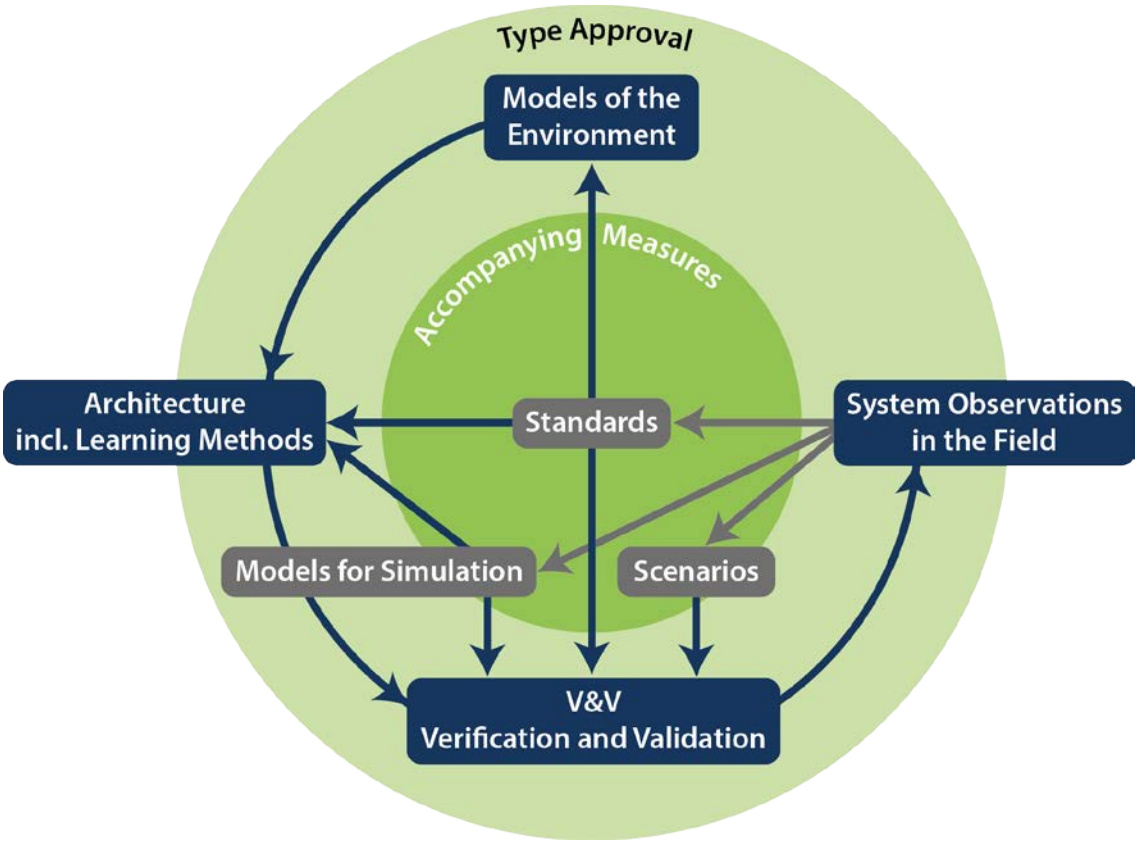

Figure 1: Key elements of a system of continuous supervision and learning from field observations for highly automated systems

Given the sheer environmental complexity precluding a sufficient level of field testing as a basis for deployment, we strongly recommend to implement a system of continuous supervision and learning from field observations. We can thus improve the current level of understanding of Questions 1 and 2, and propose initial recommendations answering Question 3, with key elements indicated in Figure 1.

Figure 1 shows a meta-level learning process that learns from the experiences of the systems in the field through an assessment of such field data by an independent authority. This assessment provides directives or recommendations for new features and/or new capabilities to be integrated in the development and validation processes with the twofold goal of improving the perception abilities of the system and of assuring its adequate behavior. The mechanism of such a learning process supports the evolution of autonomous systems thanks to the ability of their virtual release within the frame of a model-centric development process. Central building blocks of this process are architecture and algorithms, environmental models, verification and validation procedures and systematic gathering of operational data from the field. These basic elements need appropriate standardization, a common open simulation environment and an accepted set of scenarios for homologation.

4 Research Challenges

The full Roadmap Document elaborates the following research areas (see also Figure 2 below) to achieve the key objectives in the context of the meta-level learning process of Section 3.

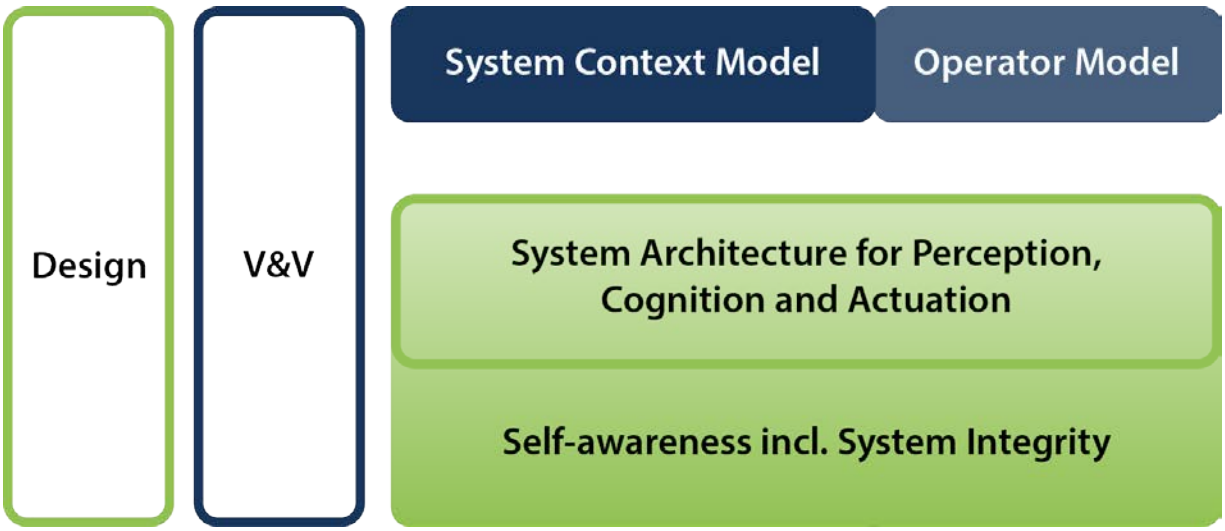

Figure 2: Research Areas

1. The Research Area *System Context Model* addresses the challenge of concise, yet comprehensive specification of the systems operative context in a form supporting model centric virtual system testing
2. Research Area *Operator Models* investigates and conceives models of human operators that support prediction of their behavior, intentions, awareness, health state, capabilities, etc. in their interaction with technical systems.
3. The Research Area *System Architecture for Perception, Cognition and Actuation* comprises foundational and engineering methods for evolvable top-level architectures for autonomous perception, decision making, and control taking into account technology constraints.
4. The Research Area *Design* addresses the challenge of providing design methods and processes supporting the creation of evidences of system integrity when integrating cloud-based services critical for system behavior as well as in the case of on-line integration of new features or capabilities.
5. The Research Area *Verification and Validation* (*V&V)* addresses the challenge of demonstrating through virtual test environments with affordable effort that the autonomous system will operate safely in all possible environmental context situations, even in the presence of security threats.
6. The Research Area *Self-awareness incl. System Integrity* addresses the challenge of establishing on-line methods guaranteeing system integrity under all operational conditions, even in the presence of security attacks

Annex 3 provides one more level of detail in terms of identified research priorities per research area.

5 Recommendations

To achieve the key objectives, we propose the following measures to be implemented in parallel to R&D activities by industry and public authorities. These focus on technical standards and regulations. Other issues of equal importance are summarized below.

Action Area	Proposed measures
1. Context models	I. Develop an open European industry driven standard for models in the different domains with different levels of complexity and evolution steps. II. Set up a public authority driven process and infrastructure for virtual system validation. This includes a. Accreditation Instances / Notified Bodies b. A public accessible validation framework c. Additional specifications for validation in the field III. Create a formal chain of argumentation for an overall safety case combining virtual releases and field-based release procedures, accepted by public authorities and the society
2. Learning Community	I. Set up a public authority driven process for learning from field situations. This includes a. Accredited trust centers b. Commitment of the industry to provide the relevant data in an anonymous way to industrially accepted trust centers c. Feedback of the analysis result of the trust centers into the validation process.
3. Architecture	I. Industry-driven standardization of the representation of exchangeable information for objects and situations to enable the collaboration between systems. II. Industry-driven standardization of a functional architecture for automated systems and their modules, supporting compositional safety proofs and safe degradation abilities with guaranteed minimal functionality according to SAE and related classifications in other domains. III. Publicly accepted safety and development process for highly automated systems, including the ability of safe upgrades IV. Industry-driven standards allowing online validation of compatibility of E/E upgrades to the existing E/E Architecture V. Safe, standardized degradation levels with guaranteed minimum functionality
4. Validation of interoperability of automated vehicles	I. Internationally negotiated evolution stages of architectures for highly automated systems and their interoperability. II. Introduction of certificates for architecture compliance to these stages by public authority accredited instances. III. Internationally agreed upon release processes for new evolution stages of highly automated systems.
5. Framework	I. Establishment of a platform providing basic services for the

	different evolution stages of system automation. II. Domain specific industry standards for frameworks, accepted and certified by public accredited trust centers. III. Establishment of representation engines for the relevant context information, prediction engines, and interpretation engines.

To develop and especially to roll-out highly automated systems, there are a large number of non-technical issues that have to be implemented and realized. Some of these are shown below. Although this position paper and the accompanying roadmap focus on the technical dimension, we acknowledge the importance of these issues, whose solutions are highly interrelated with the technical standards and regulations described here.

Action Area	Proposed measures
Training	I. Training of drivers/operators wrt. a. automated functions and (standardized) degradation modes b. necessary actions of operators in case of degradation
Competitiveness	I. Analysis of dependencies of technical solutions on market and business constraints; definition of measures for separating these aspects or compensating for them (especially for: establishment of appropriate infrastructure, establishment of highly redundant system architectures without endangering competitiveness)
Legal liability	I. Legal framework for highly automated systems, including regulations for their operation, liability in case of accidents, and product liability. II. Public authority driven process and infrastructure for determining liability in case of accidents (e.g., wrt. voice-, video- or data-recorders).

Annex 1: Participating Organizations and Contributors

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

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

Annex 2 Relevant Roadmaps and References

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

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

[12] ERTRAC (Eds.). Automated Driving Roadmap. Version 5.0. Status: final for publication. Brussels. 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, Last accessed on 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. To appear (State of 2015)

[17] H.R. Maturana, F.J. Varela (1980). "The cognitive process". Autopoiesis and cognition: The realization of the living. Springer Science & Business Media. p. 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. Last accessed on 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

Annex 3: Research Challenges

The following table gives a detailed overview about the Research Challenges identified (c.f. Figure 2 in Section 4). It lists the Research Areas, the Research Topics (plus a short explanation) and for each identified topic

- a priority, with possible values **L**ow, **M**edium, and **H**igh), giving the importance of this topic for the overarching topic of highly automated systems
- an urgency, with possible values **S**hort Term (within 5 years), **M**edium Term (within 10 years), and **L**ong Term (more than 10 years), indicating when results in this topic will be needed.

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

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

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

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

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

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

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

Imprint

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

Date: August 2017