DLR Deutsches Zentrum
für Luft- und Raumfahrt
German Aerospace Center

SafeTRANS
SAFETY IN TRANSPORTATION SYSTEMS

Workshop Report

Societal and Technological Research Challenges for Highly Automated Road Transportation Systems in Germany and the US

Diversities and Synergy Potentials

Washington D.C. 30/31 October 2018
Organized by the NSF/DFG-PIRE project "SD-SSCPS" (Science and Design of Societal Scale CPS)

Workshop hosted by DLR and organized by German Aerospace Center (DLR), SafeTRANS, Vanderbilt University, University of California at Berkeley

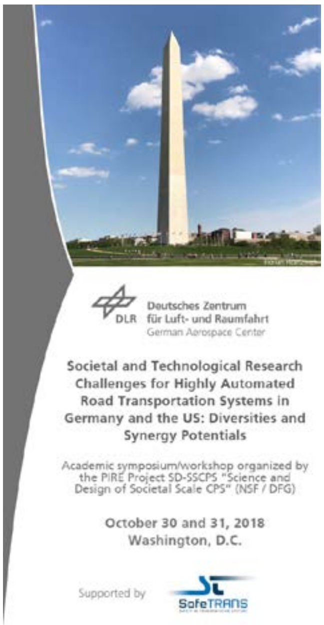
Steering Committee: Karsten Lemmer, Werner Damm, Janos Stzipanovits, Shankar Sastry, Claire Tomlin, Frank Köster, Meike Jipp

Operational Organizing Team: Henning Mosebach, Werner Damm, Frank Köster, Jürgen Niehaus, Janos Stzipanovits, Florian Plötzwich

1 Workshop overview

1.1 Motivation

The rapidly increasing presence of automation systems, driven by the confluence of advancements in Cyber-Physical Systems (CPS) and Artificial Intelligence (AI), creates fundamental societal and technical challenges that link liability, certification, assurance, and policy issues. Initialized by the DFG and NSF funded PIRE project "SD-SSCPS – Science of Design of Societal Scale Cyber-Physical Systems", a two-day expert workshop titled "Societal and Technological Research Challenges for Highly Automated Road Transportation Systems in Germany and the US: Diversity and Synergy Potentials" brought together experts from research organizations and public authorities from the US and Germany to discuss these challenges for the specific context of highly automated driving.



DLR Deutsches Zentrum für Luft- und Raumfahrt
German Aerospace Center

Societal and Technological Research Challenges for Highly Automated Road Transportation Systems in Germany and the US: Diversities and Synergy Potentials

Academic symposium/workshop organized by the PIRE Project SD-SSCPS "Science and Design of Societal Scale CPS" (NSF / DFG)

October 30 and 31, 2018
Washington, D.C.

Supported by SafeTRANS

The workshop was hosted by the German Aerospace Center and took place in Washington, D.C, on October 30 and 31, 2018. Its main objective was to establish a mutual understanding about current approaches and research activities for building, validating, and testing Highly Automated Driving Systems on both sides of the Atlantic, by giving selected presentations from experts of both nations, by having roundtable discussions on dedicated topics from this area, and by getting to know each other for future shared activities and collaborations.

This report summarizes the workshop's content and its key findings. It is one of three documents created as a result of the workshop:

- A half-page summary document (which is essentially the same as Section 1.3. of this report)
- A summary of the main findings of the workshop (essentially Secton 2 of this report)
- The full report of the workshop (this document)

1.2 Venue, Program, Participants

The workshop took place in Washington, D.C., on the premises of the German Aerospace Center (DLR) Washington Office (see Appendix 5.3). It gathered some 50 participants from leading US and German research organizations and regulatory authorities (see Appendix 5.2. for a complete list of participants).

Presentations and roundtable discussions were structured in five thematically aligned sessions

- Session 1: Welcome and Introduction
- Session 2: Assuring Safety and Security for HAD
- Session 3: V&V and Testing for HAD
- Session 4: Large Scale Research Initiatives of Testing for Safety, Security, V&V and HAD
- Session 5: Regulatory, Legal and Societal Challenges for HAD

The complete program is shown in Appendix 5.1; Section 3 gives details about the content of each of these sessions. At the end of the first day, all speakers and participants ended the evening in the traditional Old Ebbitt Grill Restaurant in Washington D.C. (next to the White House).

Picture 1: Come together in Old Ebbitt Grill, Washington D.C.

1.3 Summary

The workshop gathered some 50 participants from leading US and German research organizations and regulatory authorities, and funding authorities to discuss research challenges, social impact, and regulatory issues for highly automated driving.

It served to establish a mutual understanding about current approaches and research activities on safety and security analysis, V&V and testing, regulatory, societal, and legal issues for Highly Automated Driving (HAD) for participants from the US and Germany (resp. Europe) representing academia, R&D funding organizations, standardization and regulation bodies, and public authorities.

Presentations of leading US and German scientists highlighted key aspects that must be mastered for assuring safety of Highly Automated Vehicles (HAV), such as assuring high confidence in the perception of complex traffic situations, assessing what can be handled in simulation test-beds and what must be proven through field tests, assuring seamless communication and mutual understanding in mixed traffic, and market-introduction strategies assuring consumer confidence.

Such research would greatly benefit from instruments allowing data sharing in a way that protects IP from industry while facilitating cross-company learning from experiences with typical failures in the perception chain, typical dynamics of various classes of traffic participants, and typical forms of implicit and explicit communication in current traffic.

The conspicuous differences in regulatory approaches between the self-certification approach in the US and government enforced homologation in Europe were discussed, pointing to the need for harmonization that encourages industry-wide convergence towards safety and security standards that are acceptable for societies.

Overall, the participants highly valued the informal nature of the forum in assessing similarities and differences between US and German ways forward towards HAD.

2 Key Findings

2.1 Similarities and Differences between US and German approach to HAD

On a **technological level**, the baseline for the development and introduction of Highly Autonomous Driving (HAD) are the same in US and Germany. These are

- HAD has a great potential to increase performance and safety of road traffic, as well as decreasing environmental impact of individual mobility.
- Although industry is in principle able to build highly automated vehicles , there is a lack of methods, processes and standards to ensure the required qualities – e.g., safety, security, reliability, and similar – of these systems. Existing methods and processes are as of now either insufficient to assure these qualities with acceptable confidence or they are unable to handle the complexity of such systems.
- Quality assurances – i.e. safety cases, but also those with respect to security, reliability, etc. – cannot be done in the traditional way, i.e., ultimately by test driving alone. Instead, simulation (of test drives) becomes a major tool in (virtual) testing, as do scenarios (i.e. descriptions of traffic situations and their evolutions) to be used as test cases, requirements etc.

Both in the US and in Germany there are a multitude of R&D projects to establish design-time and operation-time quality assurances. Main research questions to be solved within these (and potential follow-up) projects are:

- How to recognize all relevant objects within vehicle path?

  - Safety requires virtually zero false negatives (always detect real hazards)
  - Functionality requires very low false positives
- How to detect and respond to every hazard, including those that are hard to perceive?
  - Including extreme external conditions arising without advance warning
- How to predict future motion of all mobile objects (vehicles, pedestrians, bicyclists, animals…)?
- How to achieve a system that at least matches perception capabilities of experienced human drivers under all environmental conditions within Operational Design Domain (ODD)?
- How to design the suite of test cases to identify the ability of an AV system to manage these complex circumstances?
- How many and which tests can be moved to simulation? How much physical testing is still needed?
- How to ensure that simulation accurately reflects reality? The main issue here is the (non-) ex-istence of (executable, accurate) models of
  - Sensors (including their failure behavior)
  - Car dynamics (in different environments with different environmental/weather conditions)
  - Environmental data, especially weather, but also object properties (and their interac-tion with sensors)
  - Human drivers interacting with the HAD
- How to ensure relative completeness of testing?
  - How do virtual and physical testing interact (i.e. which physical tests must be passed to validate a (series of) virtual test(s))
  - How to factor in human driver behavior in mixed (human and HAD) scenarios?
  - Which scenarios are relevant (must be tested) for a given application?
  - Related to the two above: 'How safe is safe enough?', i.e. what minimum set of tests is sufficient, what is the accepted residual risk (and how is this determined?)
  - Are testing processes sufficient to establish safety within societally acceptable risk levels at all possible within reasonable cost budgets and development time scales?

Regarding scenarios, there are a number of open issues that have as yet only partly been solved:

- Completeness of scenario catalogues. How to ensure that there exists a corresponding scenario for every reasonably foreseeable traffic situation and every possible evolution?
- Prediction of occurrence of scenarios. How to recognize traffic patterns that may lead to specific scenarios?
- Source of scenario descriptions
  - Can such scenario catalogues be constructed from real-live data alone?
    - What are the relevant physical properties of objects that have to be included?
    - What are the properties of human drivers, vulnerable road users and the societal context that have to be included?
    - How to construct scenarios from real-live data?
  - Can such scenarios be synthesized?
  - From what source data?
  - How to ensure match with reality?
- Standardized description language and semantics
  - Richness of language must allow scenario descriptions on many different abstraction levels as well as capture all relevant physical data
  - Language must have well-defined, unambiguous semantics

These research questions are already pursued both in Europe as well as in the US. Although the ap-proaches used and the preliminary results differ in detail, the achieved state of the art is more or less on the same level and naturally points to a number of future research tasks where a common effort would be beneficial (see next section).

On the **regulatory side** and with respect to homologation / type approval, there are obvious differences between the approaches pursued in the US and Germany. The self-certification approach pursued in the US could lead to faster innovations and market introduction of HAD, but it suffers risks of HAV-induced crashes at deployment. Also regulations for granting permits for testing HAV vary significantly between states, exposing the population to greater accident risks in states with lower standards. The government enforced third party principle for homologation pursued in Germany and Europe circumvents this risk, but puts a significantly higher burden on OEMs for developing and introducing these new technologies into the market. Both sides strongly suffer from the lack of standards for safety and security of HAD, which need to set the target for (self- or third party) certification and need to be acceptable by society.

With respect to **market introduction** of HAD, strategies and user acceptance in the US and in Germany have been different in the past, but seem to be converging recently. Whereas in Germany new technologies like HAD are traditionally accepted very cautiously, with a strong emphasis being placed on the existence of regulations and certification of safety properties, acceptance in the US has been more enthusiastic, with only a few voices of caution. However, triggered by recent crashes and experiences, user acceptance in the US became more reserved by mid-2018, with for example a coalition of civil society organizations opposing the unrestricted introduction of this technology and seeking stronger policy guidance from the U.S. Congress, which was developing legislation. On both sides, there is a strong need for carefully constructed standards and regulations that while enabling innovation, would still increase user trust and acceptance of emerging new technologies and mitigate liability risks to the developers.

2.2 Synergies and Cooperation Potential

Based upon the assessment of the state of the art of the technology and the similarities and differences outlined in the previous section, the participants of the workshop identified the following research topics as having a good potential for synergies and cooperation:

- **Standards**: Car manufacturers need to sell their cars world-wide. To enable homologation in different countries/regions, harmonized standards are of utmost necessity. However, many aspects that would need to be standardized differ between countries. It is therefore important to establish global standards for methodologies, definitions, and processes, while leaving the concrete acceptance criteria to country-specific extensions of such standards.
    - Technical standards about components of highly automated vehicles (i.e. sensors), in-cluding their quality and confidence levels/properties.
    - A global, harmonized agreement on quality criteria (i.e., metrics, Key Performance Indicators and their confidence) is essential for highly automated driving.
    - Procedural standards about test methodology, determination of residual risk, etc Although the approaches to safety and the accepted risks of new technologies differ from country to country, a common general test methodology and definition about similar safety approaches – including definitions of ODDs (Operational Design Domains) and determination of residual risk – is needed both for self- or third-party certification and for achieving user trust and acceptance. First steps in this direction have been taken already (e.g., the emerging SOTIF – Safety Of The Intended Functionality – standard ISO PAS

21448), but a far broader approach is needed.

  - Security Standards, including best practices for intrusion detection and elimination.
  - Crash reporting standards, which would enable transparency and publicly accessible information for crash and disengagement reports.
  - Ethical Standards governing the development of highly automated vehicles and – most important – ways to show compliance with these rules (these standards need not nec-essarily be the same for each country, but the way the specific rules are expressed and the way to show compliance to them should be).
  - Privacy standards would establish protocols for ensuring limited use of data about travel patterns, insurance standards would establish definitions of liability and responsibility, safety standards would establish the conditions under which the hand-off occurs with human drivers, communication standards would establish common terms for HAV technologies and common modes of communication of the uses and limits of the technology across different manufacturers.
- **Scenario Description Language:**
  - There is a strong need for a common scenario description language. This language must be
    - expressive enough to allow definition of scenarios on all required abstraction levels as well as human elements/behavior
    - expressive enough to allow description of dynamics of scenarios with both normative as well as erroneous behavior of actors
    - have unambiguous semantics
    - allow for IP protection to enable exchange of scenarios between stakeholders.
- **Scenario creation / generation:** To achieve completeness of scenarios with respect to real live traffic conditions, methods and tools for scenario creation and generations are needed:
  - Methods and tools to create scenarios from real-life data, to synthesize scenarios from statistical data, to check for completeness and relevance as well as to convert them between different abstraction levels.
  - Methods and tools to define pass/fail criteria for scenarios, including relevance of each criterion (safety, comfort, user experience, country & cultural differences), as well as (global) consequences of failures.
- Simulation
  - Executable models of
    - Sensors (including their failure behavior)
    - Car dynamics (in different environments with different environmental/weather conditions)
    - Environmental data, especially weather, but also target object properties (and their interaction with sensors)
  - Assessing what can be handled in simulation test-beds and what must be proven through field tests
- Human Machine Interaction / Cooperation
  - Two aspects need to be covered: humans as driver/occupants and as traffic participants (including as pedestrians and bicyclists).
  - Ensure situation awareness of each (technical and human) traffic participant
  - Communication and cooperation principles between humans and technical systems.

2.3 Recommendations

After discussing the state of the art as well as further research directions, the participants of the work-shop issued the following recommendations:

- Scenario Catalogue / Real life data base

  Set up a common data base containing real-life data of traffic situations as a basis for
  - Scenario identification
  - Sensor tests

    Set up a common scenario catalogue with scenarios mined from this real-life database as well as synthesized scenarios as a common basis for type homologation/certification, including pass/fail criteria, relevance of each criterion and consequences of criteria failure.

    Both data bases need to be openly available and maintained (i.e., data needs to be add-ed/updated, made more precise, be deleted or corrected) by an independent group/organization.
- Data Sharing

  Stakeholders must be enabled and willing to share data in a way that protects their IP. This in-cludes data sharing for the following purposes:
  - for scenario identification/definition and labelling (see above), especially about critical scenarios
  - for the definition of pass/fail criteria (see above) and quality/performance measures (e.g. for sensors, etc.)
  - for the definition/extraction of models, e.g. data allowing to learn
    - models for sensors, including typical failures in the perception chain
    - typical dynamics of various classes of traffic participants
    - typical forms of implicit and explicit communication in current traffic situations
- Human Trust, User Acceptance, and Regulations

  With respect to market introduction, it is absolutely necessary to employ introduction strategies that assure consumer confidence. The advent of HAD is changing an existing socio-technical system that is already working quite well. Changes should therefore not be motivated by technical feasibility, but by improvements for the customer and society in general. Important aspects here are
  - The necessary standards for safety and security, (1) against which (self- or third party) certification can be carried out, (2) that need to be accepted by society, and (3) that can be used for assessing residual risks and trust in compliance testing.
  - When developing these standards, it might be necessary to increase effort for developing functionality and certifiability of L1 and L2 systems, and learn from these experiences for L3 and higher level systems
  - Regulations might differ from country to country and even between states in the same country. However, regulators need to avoid situations where countries or states compete for HAD introduction by lowering requirements / regulations.
  - Systems must be developed in a way that enables a continuous shared awareness of the state, the capabilities, the plans and the actions of both, the human and the technical system. Especially
    - the system needs to be able to discern and react to wishes and needs of the user
    - the user must be able to discern at each time what the system is doing as well as its reasons for doing so.
- Research and Standards

  Enable transatlantic activities to pursue the research questions as well as the standardization activities identified in Section 2.2.
- Bilateral Exchange

  A continuation of the bilateral exchange and discussions, as exemplified by this workshop, is necessary.

3 Workshop in detail

3.1 Session 1 – Welcome and introduction

Prof. Karsten Lemmer, Chairman of German Aerospace Center opened the workshop emphasizing the importance of harmonized research activities especially in the area of smart future transport systems. DLR is engaged in a wide range of technological and human factors research in the thematic area of connected and automated driving (e.g., DLR is the project leader of the national V&V-project PEGASUS (https://www.pegasusprojekt.de/en/home).

Subsequently the leaders of both the German and the US part of the PIRE project SD-SSCPS, **Prof. Werner Damm** and **Prof. Janos Stzipanovits**, pointed out that bringing autonomous systems, like self-driving cars, to market raises many more challenges than only building them. The current lack of sufficient methods for quality assurances of these systems, especially for safety cases, and especially for those systems that include components based on Artificial Intelligence methods and learning, impose high demands on research and industry, and directly affects user acceptance and trust.

Finally **Dr. Rainer Gruhling** from DFG emphasized the importance and eligibility of transnational and cross-domain research approaches. Organizations like DFG and NSF are predestined to foster high-level research without any market constraints closing the gap between technology driven product innovations on the one hand and innovative research results on the other hand.

Picture 2: Welcome words by Prof. Lemmer, DLR board of directors (top left), Prof. Damm University of Oldenburg and SafeTRANS (top right), Prof. Stzipanovits, Vanderbilt University (bottom right) and Dr. Gruhling, DFG (bottom left).

3.2 Session 2 – Assuring Safety and Security for HAD

3.2.1 Presentations

In the session "Assuring Safety and Security for HAD" **Dr. Steven Shladover** (UCB) took a broad view to the topic, spanning the arc from the challenges in assuring safety of HAD via residual risk considerations ("How safe is safe enough?") and effort estimations for reducing the residual risk to acceptable levels, to pointing out regulatory needs, and impact of HAD technology on society.

- Three main challenges for assuring safety of HAD are the closely related topics of
  - Perception: The system needs to be able to perceive its environment and all relevant objects within it with an accuracy that must match that of experienced human drivers under all environmental conditions of its ODD (Operational Design Domain, i.e. situa-tions for which it is designed to work). Currently, no single sensor can provide this accuracy, and technologies like sensor fusion and/or AI based learning algorithms are currently struggling to guarantee this required accuracy in every situation.
  - Safety: Current Safety arguments require guarantees with respect to perception accuracy; they also face many other challenges, like our inability to physically test a sufficient amount of test cases (e.g., the number of kilometers one would have to drive to test a fully automated car with the required accuracy is well beyond anything that can actually be done, at least in a cost efficient way), the difficulties in showing that simulation – as a test method complementing physical testing – accurately reflects reality, the criticality of choosing the right – and enough – test cases for simulation, the rarity of critical situations in real life, and many more.
  - All of which increases the inertia of mobility and transportation systems; although technology for automating driving is advancing, it cannot replace drivers yet because of the lack and slow progression of processes, methods and tools to assure its safety. In addition, many solutions require changes in infrastructure (i.e., physical roadside infrastructure in traffic applications or digital information infrastructure), which typically requires a large investment whose Return (RoI) can only be assessed with confidence after it has been built.

Providing adequate processes and methods to ensure safety is made even more difficult by conflicting requirements: Safety itself requires that the method should never yield a false negative: When in doubt about the safety of a situation or a behavior of the system, err on the negative side, i.e. do not allow this situation or behavior to occur. Functionality, on the other hand, requires next to zero false positives, i.e. all situations and behaviors of the system should be allowed, unless they are unsafe. Together, these two requirements put safety considerations in direct opposition to functionality opportunities, and thus market potential.

In addition, safety arguments require a sufficient amount of testing. With highly automated driving systems, the multitude of situations in which such a system might operate and the enormous variances in environmental conditions, behavior of other systems and last but not least humans with which the systems interact, renders physical testing of these systems (i.e., test driving Automated Driving Systems on closed test tracks and/or on public streets) infeasible. Physical tests have therefore to be augmented with virtual tests, i.e. simulations, which poses the challenge of validating the simulators. Critical events (i.e. 'situations worth testing') are rare events in reality, i.e. they occur seldom, and in addition, more than one of these events might be required to actually make the system fail. The challenge is therefore to devise a test strategy that tests a sufficiently large amount of an almost infinite number of possible combinations of rare events.

To overcome these challenges we need breakthroughs in software system design, verification and validation methods to overcome the limitations of formal methods and brute-force testing methods as well as learning systems; robust threat assessment, sensing and signal processing to reach zero false negatives and near-zero false positives; robust control systems; fault detection, identification and accommodation, within 0.1 s response; ethical design processes for CPS; and cyber-security protections.

Steven continued his talk by looking at some of the regulatory requirements and social impact factors imposed by highly automated driving. He pointed out that regulations need to balance protection of the public from unsafe systems with encouraging safe innovations; regulation bodies will be eager to approve automated systems once they are shown to be safe, because there is a public demand for them. However, because of the still remaining challenges in showing safety for these systems and because of the huge number of ODDs that must be met (and proven safe), he predicts a gradual market introduction of highly automated systems, not the 'automation revolution' that is often shown in the media.

Steven recommended to focus on implementing systems that are technically feasible today, to enhance their performance and to use them to gain public confidence; to then develop more highly automated systems within well-constrained ODDs to ensure safety, to finally gradually relax ODD constraints as technology advances, and to work toward the fundamental breakthroughs needed for high automation under general (relatively unconstrained) conditions.

In contrast to Steven's technology orientated overview and statements, **Prof. John Rushby** from SRI looked into the general nature of assurance cases and on how much testing is needed for such assur-ances for highly automated systems; he also gave insights into ethical questions for this topic and pointed out potential migration strategies for the market introduction of such systems.

Starting from the formal structure of assurance cases, he pointed out that by necessity some qualities of systems cannot formally be proven. Instead, in assurance cases, evidence has to be collected until its credibility crosses a certain threshold deemed to be sufficient to support the claim. This threshold is an informal requirement and is highly subjective; a good technique therefore is not (only) to show that a claim holds (by collecting evidence), but actively look for 'defeaters', i.e. situations, system behavior and/or system properties that would invalidate the claim, and then show that these defeaters do not exist or occur in reality ('defeat the defeaters'). In addition, due to assurance cases being often based on probabilities (of a system fault, of fault leading to an actual failure, etc.), it can help to start with a small number of systems and use their behavior to predict the failure rate of large 'fleets' of such systems. This technique might also help to partially overcome the challenge of an infeasible large number of tests being needed for highly automated systems (i.e., large number of test kilometers needed for highly automated cars), because the results of the first tests can be used to predict the results of the later ones.

John continued with presenting the five basic principles of ethics, namely care, fairness, loyalty, authority/respect, and purity, pointing out that different societies exhibit different priorities for (combinations of) them. However, even if these priorities are known in advance, many situations require ethical reflections that go beyond simple utilitarian accounting according to these value systems. A 'computational ethics' must observe neutrality (all ethical decisions must be independent from age, gender, race, and many other qualities of the involved actors), and may require utilitarian considerations, rule-based decisions, 'virtue ethics' and possibly a reputation system.

In summary, advanced computer systems raise numerous questions that have traditionally been the province of philosophy; thus, they can learn from 2,500 years of philosophical contemplation on the one hand, and contribute a less anthropomorphic perspective on the other hand.

Prof. Dr. Daniel Watzenig (TU Graz) stressed again, that HAD systems are more complex than traditional embedded or Cyber-Physical Systems by several orders of magnitude; current methods and tools for testing and homologation are therefore not sufficient any more, and 'brute force' tests – i.e. testing each and every test case that can occur in reality – are too expensive or – more often than not – even not feasible. He pointed out that the key to succeed in testing HAD to a sufficient degree is twofold: Shift as much as possible to virtual development and virtual validation and accompany this with the definition of methods and tools for virtual type approval and certification/homologation. Such valida-tion methods have already been pointed out in various roadmaps, e.g. in SafeTRANS RM HAD[1].

Daniel then pointed to ways how safety can be demonstrated for HAD: False positives (ie. the car should brake, but does not) are typically caused by functional insufficiencies – e.g., in sensors, or in the perception chain – or by false assumptions of the developers; these can be kept to a minimum by following standards for the development of HADs, like ISO26262 (covering errors and failures in system components) or ISO PAS 21448 SOTIF (Safety of the intended functionality, which covers functional insufficiencies). Avoiding false negatives (i.e., the system should not brake, but does) requires an even more thorough approach, i.e., the virtual validation approach described above. The main question here is to determine when enough testing has been performed, i.e., answering the question 'when is the system safe enough?'. Daniel demonstrated again that purely physical testing is not sufficient here, since the required FIT rates (FIT: Failures in time) cannot efficiently be reached with physical testing alone. However, from accident research it is known that a large majority of all accidents can be tracked down to a comparatively low number of 'types' and 'causes'. Testing concrete traffic situations – i.e. 'scenarios' – therefore has the potential of finding a large proportion of unwanted behaviors of the system with a manageable number of scenarios.

Daniel then took a look at homologation, pointing out its goals and how scenario based verification and validation can be one of the methods to achieve them, as e.g., pointed out in the EuroNCAP[2] roadmap for 2025.

Although as much testing as possible should be done by virtual testing (simulation), physical testing cannot and should not be neglected. Daniel continued with presenting three large scale proving grounds that allow physical testing of highly automated vehicles, namely the Austrian Alp.Lab – a proving ground specifically designed for testing vehicles of SAE level 3 and above --, the Hungarian ZalaZone – proving ground for Uran Scenarios and Smart Cities – and a proving ground on a public highway, i.e. the A2 highway in Austria.

Putting all these ingredients together, Prof. Watzenig proposed a scenario-based test and homologation approach for HAD, relying on virtual and physical tests and on receiving data from the field.

Whereas the previous presentations focused on functional safety of HAD, **Rens van der Heijden** (University Ulm) pointed out the importance of considering security of highly automated vehicles. Although security is an important topic in its own right, that needs to be addressed right from the beginning of the design of the system, it also impacts functional safety. Therefore, an integrated safety and security design and analysis for Cyber-Physical Systems is a must. Rens presented results from the SecForCars project, which set out to provide a holistic analysis of security for connected and automated cars, to investigate novel methodologies for joint design of secure and safe vehicles, and to design and develop new security mechanisms to protect such vehicles. Maat, the toolset evolved from this project, is used to detect misbehavior of actors (and thus potential security attacks/breaches) and respond to them. Rens pointed out that attack prevention can never be complete, thus any cyber-physical system, especially safety critical ones, have to deal with the consequences of such attacks. Since these systems are more and more connected and communicate more, they present a larger attack surface. MAAT will be extended to support these findings.

[1] Peter Heidl and Werner Damm (eds.). Highly Automated Systems: Test, Safety, and Development. Available at https://www.safetrans-de.org

[2] European New Car Assessment Programm, https://www.euroncap.com/en

3.2.2 Roundtable Discussion

The first roundtable discussion centered around the question of topics that need to be harmonized between nations like Germany/Europe and the USA for homologation of highly automated cars. It was moderated by Werner Damm.

The participants pointed out that different nations have different approaches to safety and are willing to accept different levels of remaining risk (i.e. SUV vehicles are the most dangerous cars in terms of number and consequences of accidents; they are used in the US in a much higher number than in Europe). Harmonizing any requirements for homologation thus is difficult, if the goals are diverse. However, technical standards regarding for example sensor qualities and assurances, test methods, and procedures that enable developers to ascertain the remaining level of risk (not the acceptable threshold) could and should be set up.

Picture 3: Round table of session „Assuring Safety and Security for HAD“. Participants (from left to right): Rens van der Heijden, Daniel Watzenig, Steven Shladover, John Rushby, Werner Damm (standing).

The participants confirmed that procedures and measures asserting the residual risk need to be analogous and comparable between different nations, to enable car manufacturers to re-use safety arguments for homologation in different countries.

According to a participant, this difference in approaches for safety and acceptance of residual risk also defins the need for cross-nation wide databases with an agreed set of scenarios against which to test for homologation. Such databases are still necessary, but will be individual ones per nation. The contributor also confirmed that countries would benefit from using the same (standardized) methods and processes for residual risk determination and safety assessment. The newly published SotIF Standard (ISO PAS 21448) is a good example for a standard of this type.

The pannel discussed the need for harmonizing security standards. However, it was also pointed out that ethical/societal standards are not, should not, and cannot be harmonized between nations. Werner Damm remarked that this lack of standardization would hinder car manufacturers to sell the same highy automated cars in different nations. It will also be a hindrance for a country to accept cars that have undergone type homologation in other countries.

3.3 Session 3 – V&V and Testing for HAD

3.3.1 Presentations

The following session was dedicated to Verification & Validation methods and to testing methodology. It started with a presentation by **Prof. Shankar Sastry** (University of California at Berkeley), who presented a mathematical framework to compute safety margins for trajectory planning. Starting from the observation that accurate, safe planning has high computational overhead and is typically slow, whereas fast computation of safety margins is typically less accurate, he devised a method to pre-compute a tracking error bound around trajectories derived from simple, fast planning, thus combining accuracy and speed. Shankar continued to present current results from UCB in building systems that learn trajectories of other participants for collision avoidance, using reinforcement learning and reward functions. His main observation was that in interaction with human beings, CPS should not only be safe, but also be perceived as safe. Systems must be able to communicate their safety. One way to do so is to avoid false positives, i.e. a situation in which a human anticipates a collision, but the automation system has detected the danger and will avoid the obstacle. Although this is a safe behavior, the human will lose trust in the system. Modeling supervisory behavior as safe sets allows interventions to be distilled into an actionable rule which will decrease supervisory false positives thereby increasing team performance and trust. Shankar concluded that systems need not only be safe, but also appear safe.

Prof. Rahul Mangharam (University of Pennsylvania) reported on scientific research validating the typical 'PPC-pipeline' for highly automated vehicles, ranging from (sensors and) Perception, (hierarchical) planning (of trajectories, …) and (actor and) Control. Observing that non-linear vehicle dynamics and mode switching lead to intractable or even undecidable decision problems, thus making validation of these systems very hard, he presented a way to devise 'robust algorithms' for HAD, where 'robust' means that the system always includes a safety margin in all of its decisions that allows it to recover from unforeseen disturbances and errors. The research reported by him centered on the question of whether low robustness scenarios can always be found or generated, which indeed they can. They were able to extract 37 driving scenarios from synthetic data, which account for 99.4 percent of light-vehicle crashes. These scenarios are highly parametrized and are a good source for testing new highly automated driving algorithms. Future work will include learning of scenarios.

Prof. Dr. Werner Damm (University of Oldenburg) stressed the safety impact of object detection and identification and thus the importance of guaranteeing functional safety of the perception chain of HAD, since inaccuracies or counterfactual sensing ultimately lead to wrong characterization of the situation, wrong prediction of the evolution of such situations and thus inadequate plans for the system's behavior, ultimately leading to inadequate decisions and actions of the system.

He continued by presenting an approach for the identification of the relevant scenarios for validation and testing of HAD. The set of relevant scenarios are those scenarios that (a) are needed to test the correct function of a highly automated vehicle, and (b) cover as much as possible of the possible real world situations relevant for the current function under test. The presented approach is based on a database of real traffic situations; these are generalized using mathematical models of (a) criticality, (b) behavior of other traffic participants, and (c) uncertainty in perception, thus yielding composable building blocks for generic scenarios. Such building blocks are then combined to yield the set of scenarios relevant for the function under test, where each scenario is parametrized according to the relevant environmental conditions, the perception chains of the system under test and error models. Relevant scenarios can then be used for formal verification, for testing and simulation, thus yielding high validity of the resulting safety cases for the system under test.

Since these scenarios are ultimately generated from a database of real traffic situations, which can always only contain a subset of all possible situations that occur in reality, the method also contains mechanisms for refining the database (i.e., by adding additional real world situations, especially those gathered from automated vehicles encountering an 'unknown situation'). This learning from field data process is similar to the one proposed in current R&D roadmaps, like e.g., the SafeTRANS RM HAD1 or the report of the Ethics Commission on Automated and Connected Driving[3].

In the second part of his talk, Werner Damm gave an overview about Traffic Sequence Charts (TSCs), which are a visual formalism to describe traffic scenarios. The formal semantics of TSCs is completely defined, thus meeting a necessary pre-condition for using them for system analysis and formal verification. TSCs also enable a requirement analysis process that is staged with respect to different aspects: (a) from 'sketches' (describing selected possible behaviors of the system) to formal requirements (mandatory or forbidden behaviors); (b) from ideal observer models to realistic object identification through sensor fusion and exchange of perceived world models; (c) from nominal behavior of the system to degraded behaviors; and (d) from an ego-central perspective to cooperative situation awareness and cooperative maneuvers. In all these stages and combinations thereof, TSCs allow for a formal verification of the consistency of requirements. Using a method called 'play out', the set of all possible runs for validation of requirements can be generated; in a similar way, the method allows automatic generation of monitors for design time verification on all development levels (XiL: model- / hardware- / vehicle-in-the-loop) as well as for the runtime verification and detection of disallowed activations of automatic driving functions. TSCs also allow for automatic test case generation for requirement- or scenario-based testing. Werner concluded by summarizing the main advantages of having a description language for scenarios with a formally defined semantics, which are (a) the ability to check and improve the completeness of scenario catalogues, (b) the ability to include new scenarios from data learned from the field while avoiding duplicates and guaranteeing completeness w.r.t. newly learned facts, (c) the ability to derive concise scenario descriptions, and (d) the ability to unambiguously interpret scenarios and test results.

Dr. Houssem Abdellatif (TÜV Süd) pointed out that for type approval of automated vehicles (or sys-tems) scenario-based testing including verified simulation methods will be essential and necessary. He started by giving an overview about the legal bases of homologation / type approval in different coun-tries, and continued by presenting the two main approaches for homologation: Self-certification entails that the entity bringing a product (i.e., Automated Driving System) into the market ascertains the legal and technical approval of the product. In order to give this guarantee, it typically employs its own, internal procedures. Homologation via the third party principle entails that the entity bringing a product into the market must provide 'reasonable evidence' for the product's conformity to legal and technical requirements to an independent third-party organization. This independent organization then decides about type approval of the product.

With highly automated driving, the complexity of the products to be type approved and therefore the effort needed for type approval increases dramatically; using only traditional methods, type approval of such systems will not be possible anymore – or at least require an effort that cannot reasonably be undertaken. In order to cope with this complexity increase, Dr. Abdellatif presented the following changes for the homologation process of HAD systems, which together describe an approach that is currently examined by many third-party approval organization as well as within many R&D projects:

[3] German Federal Ministry of Transport and Digital Infrastructure (ed.). Ethics Commission: Automated and Connected Driving. Report (Extract), June 2017.

1. Establish scenario based testing as State of the Art basis for type approval.
2. Install and maintain a public database of traffic scenarios, which provides a uniform description of scenarios and their pass/fail criteria, and which is updated regularly by an appropriate com-mittee.
3. Define measures for criticality coverage (i.e., answer the question "how much testing is needed to ensure a given safety level).
4. Use Simulation (i.e., virtual testing) for approval (in order to reduce (physical) testing effort).
5. Consider functional safety assessment, based on standards and with mandatory submission of corresponding documents to regulators (in order to approve compliance to standards, etc.).
6. Close the loop by real-world driving (i.e. let systems collect data in the field to identify new situations/ scenarios, unknown problems, etc.).

3.3.2 Roundtable Discussion

The second roundtable discussion was centered around the Session 3 topic "Validation and Verification of Highly Automated Driving". It brought together all speakers from this session and was moderated by Gabor Karsai.

The discussion started with shedding some light upon the use of Machine Learning (ML) techniques for V&V and testing for HAD. It was pointed out that usage of ML in this area is in its infancy. Learning typically happens in an adversary environment, and although ML uses Generative Adversarial Networks (GANS), most learning schemes do not converge and often miss the equilibrium points. There are other learning schemes that may fare better. However, by their very nature, ML algorithms are brittle (small amount of 'noise' often already causes misclassification). One main problem with using ML for recognizing and classifying traffic situations still is the non-availability of sufficiently large ('complete') data sets for learning and testing.

Picture 4: Round table of session „V&V and testing for HAD" Participants (from left to right): Rahul Mangharan, Shankar Sastry, Houssem Abdellativ, Werner Damm.

All agreed and pointed out that although creation of traffic scenarios from synthetic data as reported in a talk is a very successful method for getting easy access to data covering a lot of relevant scenarios, this data must still be extended by physical models and real-world photos (which a lot of start-up companies are busy doing). In addition, there are other methods of generating test data, especially for finding rare events.

Werner Damm stressed the importance of making extensive use of databases (DBs) of real driving situations both, for finding critical situations and typical behaviors. Usage of such DBs leads to the notion of 'completeness with respect to the DB', which can therefore be separated from the notion of 'completeness with respect to the real world'. The content of the DB is checked for quality by completeness test (does a system run in behavior where there is no scenario) and expert judgement (does the system go into situations that are not real/physically impossible, etc.). Critical scenarios for testing of HAD can be extracted from the DB by ML techniques.

The participants of the workshop agreed that the creation of such a database should be a common effort undertaken by all industry supported by academia. Since this DB must be rich enough – i.e., cover 'enough' scenarios – approaches by single actors will typically fall short. On the other hand, intellectual property (IP) concerns must of course be taken into account: data from industry – i.e., from their existing DBs as well as new data collected from systems in the field – must be 'IP-filtered' before being entered into the DB. Additionally, there must be clearly defined business cases for industry for using this DB and putting data into it; such business cases exists and have already been implemented for other forms of data/method sharing.

The attendees then discussed various aspects of such a common DB and its usage. First, they pointed out that because of the complexity of the real world and the rarity of critical events, such a DB will never be 'complete with respect to the real world'; in addition, the description of situations/scenarios in this DB must be at a certain abstraction level (like, e.g., in the Traffic Sequence Charts described in Werner Damms talk), leaving lots of parameters and details open. However, there are a lot of approaches of how to fill these details and also combine this data with data about different environmental conditions. The techniques for this are already available on the market.

Another aspect being highlighted was that the scenarios in this DB can be used for a variety of analysis techniques, safety cases and ML processes: 'Driver license like' approaches, 'naturalistic driving behavior' testing, and machine learning of cooperation strategies are all possible in addition to the typical simulation based testing of safety (collision/accident freedom).

Usage of the situations resp. scenarios in this DB will be different in each country, depending on the respective national regulations and processes for homologation of HAD systems. Setting up this database, sharing it between countries and inserting traffic data from all over the world into it, are necessary precondition for successful usage; equally important is a sharing of methodologies about how to initialize and continuously extend the content of the DB, as well as on methods how to use the data (i.e., critical scenario selection, synthesis of new scenarios, combining scenarios with environmental data, etc.). The concrete homologation processes building on this data and these methodologies, however, will probably be defined by each nation harmonized between legislation, regulation, industry and probably insurance companies, too.

The roundtable continued to discuss special aspects of virtual testing – i.e., simulation based methods – for safety cases of HAD. It was pointed out that simulation is a very important topic, in order to be able to cover the multitude of different test cases; however, simulation of sensors, their functions, and especially their errors and misreading of sensors, still is the weak link in this approach. In order to completely simulate a sensor, today it has to be modelled and executed at the physical level (i.e., on the electro-magnetic wave propagation level for a radar sensor), which is very difficult to represent and computationally intensive. Simulation models that are both easy to compute as well as accurate, are difficult to achieve; appropriate mathematical models are often missing. Using data from the field in order to test sensors and characterize their behavior is also not easily done, since the needed data is often of much higher order of magnitude than can efficiently be captured today. Nonetheless, there are various companies today that follow this approach.

For real systems, intelligent sensor fusion – using sensors whose strengths and weaknesses are complementary – seems to be the only way to achieve at least some level of accuracy.

The last topic in the discussion covered the topic of taking into account the consequences of (failed) scenarios. Typically, scenario based methods talk about frequencies in which scenarios occurs, placing more effort on validating more frequent scenarios; however, scenarios with worse consequences should probably receive more test efforts than those with milder consequences. Werner Damm pointed out that within the training process of Neural Networks one often uses measures of 'risk of miss-calculations', so this issue is at least partly covered. However, such measures only take into account an individual object; there is as yet no way to account for the global consequences of an accident. Research in this area is needed.

3.4 Session 4 – Large Scale Research Initiatives

3.4.1 Presentations

The afternoon of the first day was dedicated to presentations of selected large scale research activities in Europe and the US.

Prof. Frank Köster (DLR) reported on "PEGASUS", a large sale German national project that addresses methods, criteria, quality metrics and levels, as well as generally accepted and reliable procedures to test and assess automated driving functions (focusing on level 3 functions on highways). The project aims at the definition of standardized and reliable procedures for the test of automated vehicle func-tions based (a) upon a variety of tools for data management, data processing and analysis, simulation and simulators, test stands and proving grounds, and test fields and real environments, (b) the integration of test and assessments in the development processes at early stages, and (c) the development of a continuous and flexible tool chains to safeguard automated driving. One main research question is to determine the necessary level of analysis and tests ("How safe is safe enough?") based on a realistic application ("Highway Chauffeur"). Frank also presented the plans for a follow-up project called "SetLevel 4to5" which will start in 2019 and aims to set up a scenario based approach for simulation based testing of HAD, enhancing the PEGASUS approach to also cover urban scenarios.

Frank also gave an overview about a large scale research infrastructure as a test ground for HAD, namely the 'Application platform Intelligent Mobility' AIM and its integration into the even larger "Test Field Lower Saxony". AIM is located in the city of Brunswick (Germany), where the entire city serves as a platform for application-oriented research and development-activities in the field of intelligent mobility. It consists of databases, models, simulation toolboxes and simulators, dedicated test tracks in real urban areas within the city of Brunswick as well as in selected surrounding areas. AIM is an integral part of the Test Field Lower Saxony, which adds approx. 280 km of different types of roads to the test field with a focus on highways.

Prof. Dr. Werner Damm (University of Oldenburg) reported on a second follow-up project of PEGASUS, namely the planned "V&V Methoden" (Verification and Validation Methods) project planned to start in 2019. This project aims to set up such methods for the validation of SAE level 4 and 5 automotive systems in urban scenarios, focusing on (a) the identification and definition of representative test scenarios, (b) incremental testing of such systems ranging from components to the full system, and (c) seamless test approaches across all test levels.

A complete modular validation framework including methodology and virtual validation platform was presented by **Dr. Andrea Leitner** (AVL), coordinator of the large scale European project "ENABLE-S3". This project consortium consists of some 70 partners from 16 European countries, who develop a Sce-narios-based Validation Methodology as well as a large number of re-usable 'technology bricks', which are – based upon a generic test architecture – instantiated into application specific test platforms for 12 use-cases from Automotive, Avionics, Maritime, Health, and Farming. The project also successfully installed standards for a description language for Scenarios.

Dr. Sandeep Neema presented the Assured Autonomy Program of DARPA, whose goal is to develop rigorous design and analysis technologies for continual assurance of learning-enabled autonomous systems, in order to guarantee safety properties in adversarial environments. The fact that these systems use neural networks (or other forms of KI) to learn new or different behaviors in the filed implies that V&V has to be split into one part at design-time and another part at operational-time. The objective of the program is to (a) increase coverage and scalability of design-time assurance, (b) reduce overhead of operation-time assurance, (c) integrate design-time and operation-time assurance for continual assurances, and (d) reduce trials to assurance. Specifically, the program enhances design-time assurances by developing a deep neural network (DNN) verification tool and a method for verifying systems containing DNNs. It enhances operation-time assurance by developing an assurance measure for systems containing Neural Networks and uses past experience to determine precise levels of confidence in predictions based on Neural Networks.

Prof. Alex Bayen (UCB) reported on predictions of the effect of deploying HAD cars into normal traffic situations. He started with an overview about prediction methods using macroscopic and microscopic models and presented the four main barriers for microscopic models and simulation that cover an entire city. By using a novel method and reinforcement learning, these barriers can be circumvented. Using simulation techniques on a microscopic level he was able to show that by introducing a relatively small amount of Connected Automated Vehicles (CAV) into regular traffic situations (with the exact number being dependent on the overall scenario, but typically 5-10%), traffic would efficiently be regulated (e.g., run more smoothly in terms of preventing flow oscillations, running with higher throughput, and similar quality metrics). The methods used for these simulations have been collected within the FLOW framework.

Prof. Andreas Malikopoulos (UDel) finalized the day with his presentation about Socio-Technical sys-tems approaches combining the role of future automated traffic in smart cities meeting the require-ments of energy efficient mobility.

3.5 Session 5 – Regulatory, Legal and Societal Challenges

3.5.1 Presentations

The scope of the second day was "Regulatory, Legal and Societal Challenges for HAD".

Prof. David Hess (Vanderbilt University) opened the session with a presentation on the perspective of civil society and public opinion on AV policy in the US. He started with an introduction of (industrial) technology changes and their success factors, giving ample examples of successes and failures of such transitions in various technology domains. He then sketched the theory of industrial transitions, and continued with an analysis of the role of civil society and public opinion in the public sphere debates over highly automated vehicles in the US.

Public opinion is represented – amongst others – by consumer organizations, which includes general groups like the Consumers Union as well as transportation consumer groups such as the American Automobile Association (AAA), which has some 58 million members in the US. These organizations conduct research – mostly in the form of opinion polls – to elicit public opinion. For example, according to a poll the AAA conducted in 2016, two thirds of the Americans are afraid to ride in highly automated vehicles; however, almost the same percentage of respondents (61%) wanted to have at least one automation feature in their own car (like automatic emergency braking, adaptive cruise control, self-parking, lane assistant, or similar). In an additional poll, which took non-drivers and non-passengers into account, the AAA discovered that two-thirds of the respondents would feel less safe sharing the road with a highly automated vehicle if they were pedestrians or bicyclists. This led to a policy statement that sought "the gradual, safe introduction of these technologies to ensure that American drivers are informed, prepared and comfortable with this shift in mobility", conforming with the poll results. More generally, the public interest voiced by the AAA supported federal and state policy for continued development of driver-assisted technologies but with a much slower pace for the introduction of driverless vehicles on the roads.

David continued with an inspection of the interrelation of federal government policy and public interest organizations. In 2017, the National Highway Traffic Safety Administration (NHTSA) issued the "Automated Driving Systems (ADS): A Vision for Safety 2.0" document that updated and replaced their previous policy guidance. It contained voluntary guidance for developing and building level 3 and above HADs, voluntary safety self-assessments, and their voluntary disclosure. The statement also made state governments responsible for human drivers and vehicle operation (not for safety design) and gave guidance to state legislatures. Consumer groups responded by voicing the need for a mandatory– instead of voluntary – approach to safety regulations and standards. They also argued that the NHTSA should implement the National Transportation Safety Board's (NTSB) recommendations for Level 2 and 3 vehicles as well as set minimum standards for cybersecurity and over-the-air vehicle updates. Since then, there have been various public discussions and (successful and failed) legislation initiatives about the level of regulation required for the introduction and testing of Automated Driving Systems. These discussions, which involve civil society organizations in the policy process, attempt to balance the rapid market introduction of HAD technology with public demands to ensure the required safety and quality measures for these systems before market introduction. The crashes that have happened involving HAD also led to high public interest in these questions. In response to federal legislation under consideration in the U.S. Congress in 2017-2018, civil society organizations formed a coalition of more than seventy organizations in order to modify crucial aspects of the proposed legislation.

In the last part of David's talk, he reported about impact of different state regulation policies. As an example, he cited the case of Uber, which chose to move and operate their highly automated car fleets from California to Arizona due to less restrictive regulations there. However, after a fatal crash in which an Uber car was involved and after criticism by consumer groups and others, the governor temporarily suspended operations by Uber in that state. David concluded with a discussion of civil organizations and private governance, that is, advocacy for changes in how corporations convey their HAD products and vehicle information to drivers and users. This form of advocacy includes a need for clear consumer guidance on the limitations of systems as well as the need for technology-based enforcement of correct usage of the system (e.g., infrared camera in the cockpit that monitors the drivers' attendance and readiness to take over control).

As an example of public discussions and policy making in Europe in a similar line to those that David Hess used in his talk, **Prof. Dr. Werner Damm** (University of Oldenburg) then pointed out the strategy paper of the German Ethics Commission, an expert group that gives recommendation to the German Federal Government concerning ethical issues of highly automated driving. Unfortunately, the planned talk about this issue could not be given due to illness of the speaker, but the document itself was presented at the workshop and given to the participants.

Prof. Dr. Klaus Bengler (TU Munich) reported on several German and European research activities defining roles between human driver and automation and research on models to estimate driver's behavior, recommended communication methods between humans and automated vehicle (inside and outside vehicle). He put a special focus on human machine cooperation, pointing out the explicit and especially the implicit communication that is necessary for this. Implicit communication is used a lot in traditional traffic situations. However, HAD systems have difficulties both in understanding – or even recognizing – and in using this form of communication. In addition, implicit communication can also not fully be simulated, which makes development and testing difficult. The goal of this research is to make HAD systems – and robots in general – 'legible', which they are if and only if their 'intention' can be understood by a human (observer or interactor) and this behavior meets the expectations of that human. Central design considerations for HAD systems include an identification of the information needed by other road users and finding novel means to communicate this information implicitly.

In 2017, the German Road Traffic Act was adapted towards the requirements of automated driving. **Dr. Tom Gasser** from the German BASt, gave a detailed summary of this adaptation, which includes a definition of autonomous vehicles in terms of required functionality, clarifies the role and responsibilities of drivers of AV, sets rules for liability and demands a 'black box' as a data recorder that is accessible to the authorities if they request this after a crash.

Dee Williams (National Highway Traffic Safety Administration – NHTSA) gave an overview about NHTSA, its mission and research programs for HAD. The programs' primary outputs are evaluating emerging safety issues and trends, building knowledge of new technologies and Issues, developing technology neutral test procedures and assessment tools, modernizing requirements and performance criteria, issuing best practices and guidance and building new and enhanced capabilities for Automated Driving Systems (ADS).

In addition, NHTSA publishes guidelines like the ADS 2.0: A Vision for Safety voluntary guideline, which supports industry and states, as they consider innovative approaches to safety and develop best prac-tices, and add transparency to complicated and new technologies for consumers. The US Department of Transportation is currently preparing a document ADS 3.0., which will provide new multimodal safety guidance, will clarify policies and roles and will reaffirm that the ADS 2.0 document remains central to the US DOT's approach. ADS 3.0 will also cover trucks, buses and other vehicles / traffic participants, thus interaction with more administration groups like NHTSA will result.

In the discussion that followed this talk it was established that there are currently only a few transatlantic research programs in place. Dee confirmed that NHTSA would be open to discuss the installation of such programs. The participants also established that there are currently too few research programs that fund the cooperation of academic and industrial players.

In the last presentation of this session, **Claus Pastor** (BASt) reported on the United Nations UN ECE WP 29 activities to define scenario based test approaches for highly automated vehicles. For this, they installed an IG (informal group) on the topic of ACSF (Automatically Controlled Steering Functions), which aims to define changes to UN Regulation No. 79 (on steering systems) and overcome the 10 km/h limit for automated steering. Whereas the capabilities of AVs are divided in different categories (principles of operations: A – information and warning; B – continuously automating; C – temporarily intervening in accident-prone situations), and whereas category A is information only and regulations for ESF and CSF systems in category C have already been adopted, the current discussions center around category B, where the ACSF under considerations are discussed via several scenarios. These scenario range from low speed maneuvering (like park assistant) via different lane keeping scenarios to scenarios for lane change. For low levels of automation (SAE level 1-2) technical specifications have already been adopted for some of these scenarios; for higher SAE levels (level 3-4) and more complicated scenarios, some specifications have already been drafted, while other discussions have not yet started. Claus continued giving a detailed description of technical specifications for a lane change maneuver before presenting a potential future approach for homologation of AVs based upon the regulations and recommendations of UN ECE WP29. This approach relies heavily on the existence of a 'pool' (database) of relevant traffic scenarios.

3.5.2 Roundtable Discussion

In the final roundtable, moderated by the head of institute of DLR's transportation systems Prof. Katharina Seifert, the speakers of the previous session discussed societal and regulatory topics for the introduction of HAD amongst themselves and with the audience.

They started by observing that public opinion is formed and influenced in Europe and the US probably in very similar ways, but that media campaigns in this area are much more common in the US. The members of the roundtable then discussed how changes in public opinion can be introduced in current regulatory activities and recommendations, like for example the ADS 3.0 regulations. It was pointed out that there was broad participation in defining these rules, also including consumer groups. However, both consumer opinions as well as industry policies change over time, so a very cautious approach with transparent strategies should be followed. The strategies for regulations followed in the US and in Europe are very different, partly because of different safety rules. Whereas the NHTSA mandates no new regulations for AV test systems, in Europe regulations need to be in place before market introduction at least for some systems. NHTSA will only intervene when data from existing systems show that there is a market failure or a particular safety issue. This avoids the slow process of regulatory approval and also supports innovation and the marketplace testing of new products. However, existing regulations – like vehicle safety standards – continue to apply to AV test vehicles (c.f. 'how safe is safe enough?'). Currently, the public seems to be poorly informed about the benefits and the risks of using HAD systems, especially when taking into account the different SAE levels and the particular capabilities of current, planned and future systems.

Picture 5: Roundtable session 5. Participants (from left to right): Dee Williams, Tom Gasser, David Hess, Claus Pastor, Klaus Bengler, Katharina Seifert (standing).

Unlike for other safety-critical technologies, for Automated Driving Systems there are currently no or at least very few standards that would govern certification beyond existing processes for vehicles with human drivers. Self-certification for AV systems, as occurs for vehicles in general in the U.S., is limited because it requires reference to meeting the requirements of specific standards, and no such standards exist yet for Automated Driving Systems. Although AV systems are tested extensively, the public and consumer safety organizations view recent crashes in which these systems were involved as proof that they were not tested adequately off the road before being introduced into on-road test sites. The 'Silicon Valley culture' of testing systems in the market and then providing corrections via software updates does not translate well for the automotive industry for HAD systems. To the contrary, this industry would need regulations and standards for AV testing even out of self-interest. Basing these regulations and standards on scenarios, with requirements adjusted to the different automation levels and operational design domains, seems to be a good way of achieving these goals and will also be a good way of communicating capabilities and limitations of AVs to the public. Last, but not least, common regulations and standards as targets for AV testing would also prevent states from competing for early introduction of HAD systems by engaging in a regulatory race to the bottom.

3.6 Summary of findings and results

The last roundtable discussion seamlessly led to a discourse involving all participants, where they re-capped the workshop findings and results. They identified similarities and differences between the US and the German approach to HAD validation and homologation on the technological and regulatory levels as well as regarding market introduction. Central to these is the move towards scenario-based testing and validation of HAD systems on both sides of the Atlantic. Based upon the similarities, a set of research topics was identified, which have a high synergy potential and would benefit from transatlantic cooperation: These topics include the definition of standards, description languages for scenarios, generation and creation of scenarios, (scenario-based) simulation techniques and methods, and Human-Machine Interaction. Finally, the participants agreed to a set of recommendations to politics, regulation authorities, and funding agencies concerning the creation of a scenario catalogue, sharing of data between actors, methods to increase human trust and user acceptance as well as on standards and regulations.

These observations, cooperation potentials and recommendations are described in detail in Chapter 2 of this document.

4 Conclusion and Way forward

The workshop provided an excellent opportunity for the participants to establish a mutual understanding about current approaches and research activities on safety and security analysis, V&V and testing, regulatory, societal, and legal issues for Highly Automated Driving (HAD). The participants were able to discuss in detail the similarities and differences between the approaches taken in the US and in Europe for certification and homologation of Automated Driving Systems (ADS). Specifically, they discussed synergies and cooperation potentials in this area, which centered around the topics of standards definitions (as basis for certification), scenario description, generation and creation as well as appropriate simulation techniques and methods for scenario-based testing, and more. The participants also worked out a set of recommendations that they feel are necessary to follow in order to ensure a successful development and market introduction of these systems. These results of the workshop have been detailed in Section 2 of this document.

In addition, the workshop showed a large potential for future collaboration activities amongst the par-ticipants in the thematic area of automated driving. These activities involve harmonization of research, method- and toolchain exchange and even enhancement of existing or developed methodologies to cover further CPS domains. Since 2018 the organizers and stakeholders of this workshop have started many research and harmonization activities regarding test methods and assurance methods of automated driving technologies and corresponding functionalities of systems and subsystems. Many of these activities are and will be discussed between the members of this workshop by knowledge sharing over dissemination activities, by discussing standardization and harmonization of procedures in the relevant groups and by project-driven bilateral discussions.

The most important ones are highlighted in the following passage – further activities are also picking up the workshop results in many bilateral discussions.

The German government has decided to continue the PEGASUS verification and validation methods for automated driving by setting up new projects under the headline "PEGASUS family" under participation of many workshop partners. In a first stage the projects "SetLevel 4to5" and "Verification and Validation methods for automated driving" will harmonize the German research and industrial activities in the field of test specifications, scenario definitions and simulation tools for assurance of automated driving. DLR will start international dissemination events as well as liaison activities in 2020, leading to harmonization and standardization.

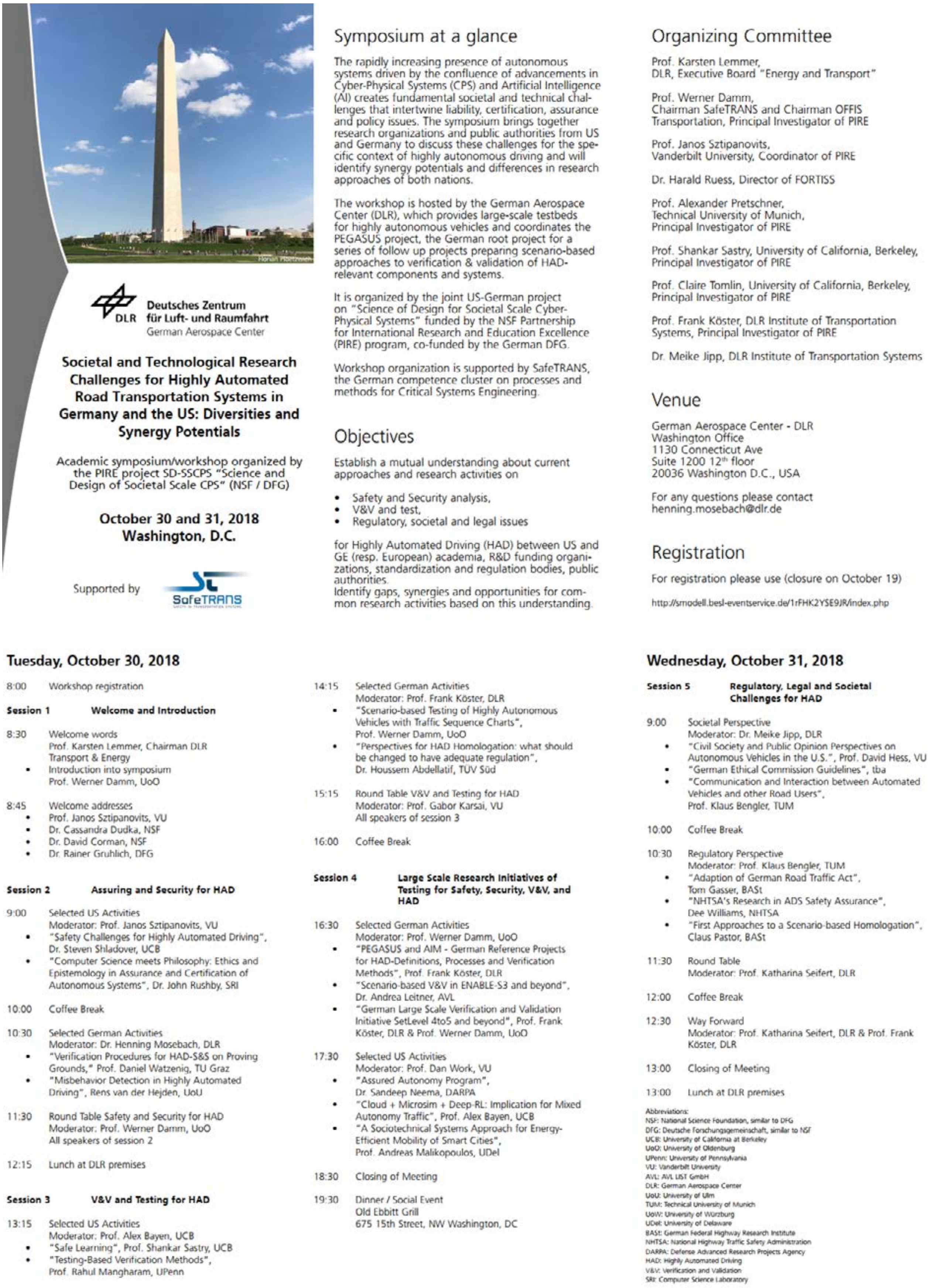
Two large scale European project initiatives have been submitted as part of the European ECSEL-research program. They will develop toolchains and relevant test specifications as close-to-series ap-proach for automated driving validation methods. Workshop participants are leading this project and will share all publishable knowledge on the projects' websites.

A high level academic research project called “Assuring Individual, Social, and Cultural Embeddedness of Autonomous Cyber-Physical Systems (ISCE-ACPS)” was proposed as enhancement of the initiative “Science and Design of Societal Scale CPS” (SD-SSCPS). Whereas the SD-SSCPS project, which also initiated this workshop, was dedicated to the automotive domain and its challenges regarding validation of HAD, the new project also takes further domains such as aviation and energy into account. Smaller workshops are following under participation of Washington workshop members.

The organizers of the first Washington workshop would like to thank again all participants for their key contributions at the workshop itself and the editorial work that led to this reporting document. Especially the key findings will act as leading research questions in further project- and collaboration activities. All participants are encouraged to distribute these questions into the research community, to participate in further US/German collaboration activities following the invitations and to share their knowledge and methodologies as well as tools between the participants.

5 Appendix

5.1 Agenda



Deutsches Zentrum
für Luft- und Raumfahrt
German Aerospace Center

Societal and Technological Research Challenges for Highly Automated Road Transportation Systems in Germany and the US: Diversities and Synergy Potentials

Academic symposium/workshop organized by the PIRE project SD-SSCPS "Science and Design of Societal Scale CPS" (NSF / DFG)

October 30 and 31, 2018
Washington, D.C.

Supported by SafeTRANS

Symposium at a glance

The rapidly increasing presence of autonomous systems driven by the confluence of advancements in Cyber-Physical Systems (CPS) and Artificial Intelligence (AI) creates fundamental societal and technical challenges that intertwine liability, certification, assurance and policy issues. The symposium brings together research organizations and public authorities from US and Germany to discuss these challenges for the specific context of highly autonomous driving and will identify synergy potentials and differences in research approaches of both nations.

The workshop is hosted by the German Aerospace Center (DLR), which provides large-scale testbeds for highly autonomous vehicles and coordinates the PEGASUS project, the German root project for a series of follow up projects preparing scenario-based approaches to verification & validation of HAD-relevant components and systems.

It is organized by the joint US-German project on "Science of Design for Societal Scale Cyber-Physical Systems" funded by the NSF Partnership for International Research and Education Excellence (PIRE) program, co-funded by the German DFG.

Workshop organization is supported by SafeTRANS, the German competence cluster on processes and methods for Critical Systems Engineering.

Objectives

Establish a mutual understanding about current approaches and research activities on

- Safety and Security analysis,
- V&V and test,
- Regulatory, societal and legal issues

for Highly Automated Driving (HAD) between US and GE (resp. European) academia, R&D funding organizations, standardization and regulation bodies, public authorities.
Identify gaps, synergies and opportunities for common research activities based on this understanding.

Organizing Committee

Prof. Karsten Lemmer,
DLR, Executive Board "Energy and Transport"

Prof. Werner Damm,
Chairman SafeTRANS and Chairman OFFIS Transportation, Principal Investigator of PIRE

Prof. Janos Sztipanovits,
Vanderbilt University, Coordinator of PIRE

Dr. Harald Ruess, Director of FORTISS

Prof. Alexander Pretschner,
Technical University of Munich,
Principal Investigator of PIRE

Prof. Shankar Sastry, University of California, Berkeley,
Principal Investigator of PIRE

Prof. Claire Tomlin, University of California, Berkeley,
Principal Investigator of PIRE

Prof. Frank Köster, DLR Institute of Transportation Systems, Principal Investigator of PIRE

Dr. Meike Jipp, DLR Institute of Transportation Systems

Venue

German Aerospace Center - DLR
Washington Office
1130 Connecticut Ave
Suite 1200 12th floor
20036 Washington D.C., USA

For any questions please contact
henning.mosebach@dlr.de

Registration

For registration please use (closure on October 19)

http://smodell.besl-eventservice.de/1rFHK2YSE9JR/index.php

Tuesday, October 30, 2018

8:00 Workshop registration

Session 1 Welcome and Introduction

8:30 Welcome words
Prof. Karsten Lemmer, Chairman DLR Transport & Energy
- Introduction into symposium
Prof. Werner Damm, UoO

8:45 Welcome addresses
- Prof. Janos Sztipanovits, VU
- Dr. Cassandra Dudka, NSF
- Dr. David Corman, NSF
- Dr. Rainer Gruhlich, DFG

Session 2 Assuring and Security for HAD

9:00 Selected US Activities
Moderator: Prof. Janos Sztipanovits, VU
- "Safety Challenges for Highly Automated Driving", Dr. Steven Shladover, UCB
- "Computer Science meets Philosophy: Ethics and Epistemology in Assurance and Certification of Autonomous Systems", Dr. John Rushby, SRI

10:00 Coffee Break

10:30 Selected German Activities
Moderator: Dr. Henning Mosebach, DLR
- "Verification Procedures for HAD-S&S on Proving Grounds," Prof. Daniel Watzenig, TU Graz
- "Misbehavior Detection in Highly Automated Driving", Rens van der Hejden, UoU

11:30 Round Table Safety and Security for HAD
Moderator: Prof. Werner Damm, UoO
All speakers of session 2

12:15 Lunch at DLR premises

Session 3 V&V and Testing for HAD

13:15 Selected US Activities
Moderator: Prof. Alex Bayen, UCB
- "Safe Learning", Prof. Shankar Sastry, UCB
- "Testing-Based Verification Methods", Prof. Rahul Mangharam, UPenn

14:15 Selected German Activities
Moderator: Prof. Frank Köster, DLR
- "Scenario-based Testing of Highly Autonomous Vehicles with Traffic Sequence Charts", Prof. Werner Damm, UoO
- "Perspectives for HAD Homologation: what should be changed to have adequate regulation", Dr. Houssem Abdellatif, TÜV Süd

15:15 Round Table V&V and Testing for HAD
Moderator: Prof. Gabor Karsai, VU
All speakers of session 3

16:00 Coffee Break

Session 4 Large Scale Research Initiatives of Testing for Safety, Security, V&V, and HAD

16:30 Selected German Activities
Moderator: Prof. Werner Damm, UoO
- "PEGASUS and AIM - German Reference Projects for HAD-Definitions, Processes and Verification Methods", Prof. Frank Köster, DLR
- "Scenario-based V&V in ENABLE-S3 and beyond", Dr. Andrea Leitner, AVL
- "German Large Scale Verification and Validation Initiative SetLevel 4to5 and beyond", Prof. Frank Köster, DLR & Prof. Werner Damm, UoO

17:30 Selected US Activities
Moderator: Prof. Dan Work, VU
- "Assured Autonomy Program", Dr. Sandeep Neema, DARPA
- "Cloud + Microsim + Deep-RL: Implication for Mixed Autonomy Traffic", Prof. Alex Bayen, UCB
- "A Sociotechnical Systems Approach for Energy-Efficient Mobility of Smart Cities", Prof. Andreas Malikopoulos, UDel

18:30 Closing of Meeting

19:30 Dinner / Social Event
Old Ebbitt Grill
675 15th Street, NW Washington, DC

Wednesday, October 31, 2018

Session 5 Regulatory, Legal and Societal Challenges for HAD

9:00 Societal Perspective
Moderator: Dr. Meike Jipp, DLR
- "Civil Society and Public Opinion Perspectives on Autonomous Vehicles in the U.S.", Prof. David Hess, VU
- "German Ethical Commission Guidelines", tba
- "Communication and Interaction between Automated Vehicles and other Road Users", Prof. Klaus Bengler, TUM

10:00 Coffee Break

10:30 Regulatory Perspective
Moderator: Prof. Klaus Bengler, TUM
- "Adaption of German Road Traffic Act", Tom Gasser, BASt
- "NHTSA's Research in ADS Safety Assurance", Dee Williams, NHTSA
- "First Approaches to a Scenario-based Homologation", Claus Pastor, BASt

11:30 Round Table
Moderator: Prof. Katharina Seifert, DLR

12:00 Coffee Break

12:30 Way Forward
Moderator: Prof. Katharina Seifert, DLR & Prof. Frank Köster, DLR

13:00 Closing of Meeting

13:00 Lunch at DLR premises

Abbreviations:
NSF: National Science Foundation, similar to DFG
DFG: Deutsche Forschungsgemeinschaft, similar to NSF
UCB: University of California at Berkeley
UoO: University of Oldenburg
UPenn: University of Pennsylvania
VU: Vanderbilt University
AVL: AVL LIST GmbH
DLR: German Aerospace Center
UoU: University of Ulm
TUM: Technical University of Munich
UoW: University of Würzburg
UDel: University of Delaware
BASt: German Federal Highway Research Institute
NHTSA: National Highway Traffic Safety Administration
DARPA: Defense Advanced Research Projects Agency
HAD: Highly Automated Driving
V&V: Verification and Validation
SRI: Computer Science Laboratory

5.2 List of Participants

First Name	Last Name	Association	Short
John	Maddox	American Center for Mobility	ACM
Phil	Koopman	Carnegie Mellon University	CMU
Sandeep	Neema	Defense Advanced Research Projects Agency	DARPA
Katelyn	Morris	Defense Advanced Research Projects Agency	DARPA
Andrea	Leitner	ENABLE-S3 Coordinator	AVL
Tom	Gasser	Federal Highway Research Institute	BASt
Claus	Pastor	Federal Highway Research Institute	BASt
Rasmus	Adler	Fraunhofer Institute for Experimental Software Engineering	IESE
Karsten	Lemmer	German Aerospace Center	DLR
Frank	Köster	German Aerospace Center	DLR
Henning	Mosebach	German Aerospace Center	DLR
Anke	Gilliam	German Aerospace Center	DLR
Marc	Jochemich	German Aerospace Center	DLR
Meike	Jipp	German Aerospace Center	DLR
Florian	Plötzwich	German Aerospace Center	DLR
Magnus	Lamp	German Aerospace Center	DLR
Katharina	Seifert	German Aerospace Center	DLR
Lothar	Neuhoff	German Embassy	DFG
Bettina	Schuffert	German Research Foundation	DFG
Rainer	Gruhlich	German Research Foundation	DFG
Aino	Bannwart	German Research Foundation	DFG
Daniel	Watzenig	Graz University of Technology	TUG
Nat	Beuse	National Highway Traffic Safety Administration	NHTSA
Dee	Williams	National Highway Traffic Safety Administration	NHTSA
Chris	Greer	National Institute of Standards and Technology	NIST
David	Corman	National Science Foundation	NSF
Cassandra	Dudka	National Science Foundation	NSF
Charles	Estabrook	National Science Foundation	NSF
Sonia	Ortega	National Science Foundation	NSF
Jürgen	Niehaus	OFFIS e.V.	OFFIS
Alexander	Trende	OFFIS e.V.	OFFIS
Werner	Damm	OFFIS e.V.	OFFIS
John	Rushby	SRI International	SRI
Klaus	Bengler	Technical University of Munich	TUM
Severin	Kacianka	Technical University of Munich	TUM
Jane	Lappin	TriGlobal	TRI
Houssem	Abdellatif	TÜV Süd AG	TÜV Süd
Rens	van der Hejden	Ulm University	UU

First Name	Last Name	Association	Short
Bharat	Balasubramanian	University of Alabama	UoA
Shankar	Sastry	University of California, Berkeley	UCB
Steve	Shladover	University of California, Berkeley	UCB
Alexandre	Bayen	University of California, Berkeley	UCB
Andreas	Malikopoulos	University of Delaware	UDel
Rahul	Mangharam	University of Pennsylvania	UPenn
Gabor	Karsai	Vanderbilt University	VU
Raphael	Stern	Vanderbilt University	VU
Janos	Sztipanovits	Vanderbilt University	VU
David	Hess	Vanderbilt University	VU
Dan	Work	Vanderbilt University	VU

5.3 Venue

DLR (German Aerospace Center)
premises in Washington
1130 Connecticut Ave NW
Suite 1200
Phone: +1 202 785 4411

DUPONT CIRCLE
Lebensmittelhändler
Whole Foods Market
P St NW
Dupont Circle
23rd St NW
22nd St NW
Rhode Island
N St NW
N St NW
Burgerrestaurant
Shake Shack
1200
telhändler
L St NW
Nordstrom Rack
Downtown DC
DOWNTOWN
Farragut North
29
Park
Farragut
Square
Farragut West
I St NW
Founding Farmers DC
McPherson

5.4 Abbreviations

NSF: National Science Foundation
DFG: Deutsche Forschungsgemeinschaft
UCB: University of California at Berkeley
UoO: University of Oldenburg
UPenn: University of Pennsylvania
VU: Vanderbilt University
AVL: AVL LIST GmbH
DLR: German Aerospace Center
UoU: University of Ulm

TUM: Technical University of Munich
UoW: University of Würzburg
UDel: University of Delaware
TUG: Technical University of Graz
BASt: German Federal Highway Research Institute
NHTSA: National Highway Traffic Safety Administration
DARPA: Defense Advanced Research Projects Agency
HAD: Highly Automated Driving
V&V: Verification and Validation