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

Workshop organized by the NSF/DFG-PIRE project Science and Design of Societal Scale CPS, the German Aerospace Center DLR, and SafeTRANS

Washington D.C. 30/31 October 2018

Werner Damm

Chairman SafeTRANS

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.

Participating Organisations

American Center for Mobility
Carnegie Mellon University
Defense Advanced Research Projects Agency
Federal Highway Research Institute
Fraunhofer Institute for Experimental Software Engineering
German Aerospace Center
German Embassy
German Research Foundation
Graz University of Technology
National Highway Traffic Safety Administration
National Institute of Standards and Technology
National Science Foundation

OFFIS e.V.
SRI International
Technical University of Munich
TÜV Süd AG
Ulm University
University of Alabama
University of California, Berkeley
University of Delaware
University of Pennsylvania
Vanderbilt University

Around 50 participants from research organization and regulatory bodies

Key Findings

- 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 assurance – 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.

Key Challenges I: sufficiently precise situational awareness

- 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 achieve a system that at least matches perception capabilities of experienced human drivers under all environmental conditions within Operational Design Domain (ODD)?
- 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…)?

Key Challenges II: Simulation and Testing

- How to design the suite of test cases to assess the ability of an AV system to manage these complex environmental factors?
- 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-) existence of (executable, accurate) models of
  - Sensors (including their failure behaviour)
  - 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?
- Are testing processes sufficient to establish safety within societally acceptable risk levels at all possible within reasonable cost budgets and development time scales?

Recommendations: Standards

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), including 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.
- 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

Recommendations: Standards (cont.)

- 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 necessarily 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,
- 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.

Recommendations: Common Reference

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

Recommendations: Data Sharing

- Stakeholders must be enabled and willing to share data in a way that protects their IP. This includes 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

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

8:45 Welcome addresses
- Prof. Janos Sztipanovits, VU
- Welcome address by NSF
- Welcome address by DFG

Session 2 Assuring and Security for HAD

9:00 US Perspective
Moderator: Prof. Janos Sztipanovits
- "Safety Challenges for Highly Automated Driving", Dr. Steven Shladover, UCB
- "Model based testing in real life", Dr. John Rushby, SRI

10:30 Coffee Break

10:45 German Perspective
Moderator: tba
- "Verification Procedures for HAD-S&S on Proving Grounds," Prof. Daniel Watzenig, TU Graz, Austria
- "Misbehavior Detection in Highly Automated Driving", Rens van der Hejden, UoU

11:45 Round Table Safety and Security for HAD
Moderator: tba
All speakers of session 2

12:30 Lunch at DLR premises

Session 3 V&V and Testing for HAD

13:30 US Perspective
Moderator: Prof. Alex Bayen, UCB
- "Safe Learning", Prof. Claire Tomlin, UCB
- "Testing-Based Verfication Methods", Prof. Rahul Mangharam, UPenn

14:30 German Perspective
Moderator: Prof. Frank Köster, DLRr
- "Scenario based Testing of Highly Autonomous Vehicles with Traffic Sequence Charts", Prof. Dr. Werner Damm, Carl von Ossietzky Universität Oldenburg
- "Perspectives for HAD Homologation: what should be changed to have adequate regulation", Dr. Houssem Abdellatif, TÜV Süd

15:30 Coffee Break

16:00 Round Table V&V and Testing for HAD
Moderator: tba
All speakers of session 3

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

17:00 German Perspective
Moderator: Werner Damm
- "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", Dr. Michael Siegel, OFFIS

18:00 US Perspective
Moderator: Dan Work, VU
- "Assured Autonomy Program", Dr. Sandeep Neema, DARPA
- "Large Scale Research Initiatives in California - Autonomous driving Test Bed", Prof. Alex Bayen, UCB
- "Model based testing in real life", Prof. Andreas Malikopoulos, UDel

19:00 Closing of Meeting

19:30 Dinner / Social Event

Wednesday, October 31, 2018

Session 5 Regulatory, Legal, and Societal Challenges for HAD

8:00 Societal Perspective
Moderator (BASt), tba
- "Civil Society and Public Opinion Perspectives on Autonomous Vehicles in the U.S.", Prof. David Hess, VU
- "German Ethical Commission Guidelines", Prof. Eric Hilgendorf, UoW
- "Communication and Interaction between Automated Vehicles and other Road Users", Prof. Bengler, TUM

10:00 Coffee Break

10:30 Regulatory Perspective
- "Adaption of German Road Traffic Act", Tom Gasser, BASt
- US-approach to Safe Deployment of Automated Vehicles, N.N., NHTSA, tbc
- "First Approaches to a Scenario-based Homologation", Claus Pastor, BASt

11:30 Round Table
Moderator: tba

12:30 Way Forward
Prof. Karsten Lemmer

13:00 Closing of Meeting

13:30 Lunch at DLR Premise

Abbreviations:
NSF: National Science Foundation
DFG: Deutsche Forschungsgemei
UCB: University of California at
UPenn: University of Pennsylva
VU: Vanderbilt University
AVL: AVL LIST GmbH
DLR: German Aerospace Ce
UoU: University of Ulm
TUM: Technical University
UoW: University of Würzbu
UDel: University of Delaware
BASt: German Federal Highway Research Institu
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