TECHNISCHE UNIVERSITÄT DRESDEN

IFA LS-AT

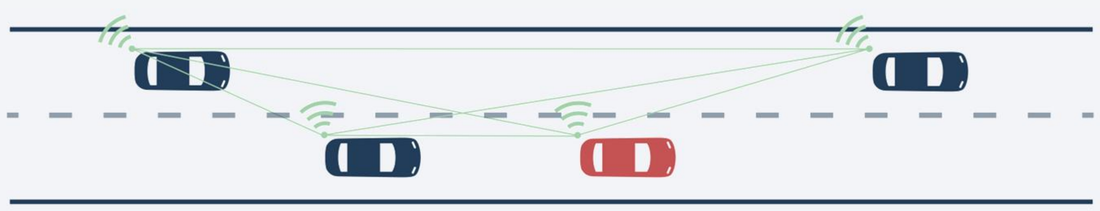
Fakultät für Elektrotechnik und Informationstechnik • Institut für Automatisierungstechnik

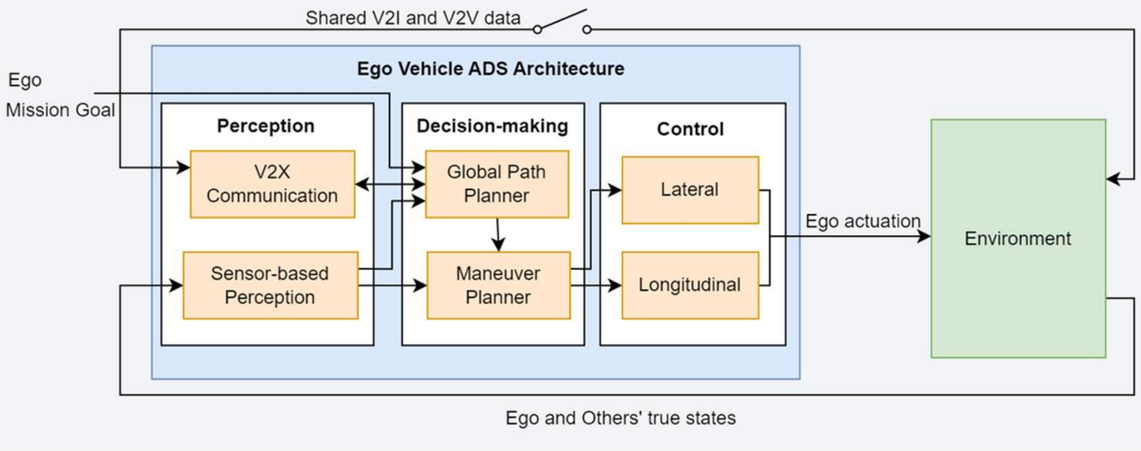
On Safety Assessment of Automated Driving Systems using Simulation-based Testing and Formal Methods

Motivation

- Automated driving systems need to provably safer than the current systems and human drivers to be acceptable
- Testing of control and decision algorithms and autonomous driving functions of intelligent vehicles in urban traffic
- Intelligent transportation systems consist of complex decision and control algorithms

Automated Driving Systems and Main Challenges





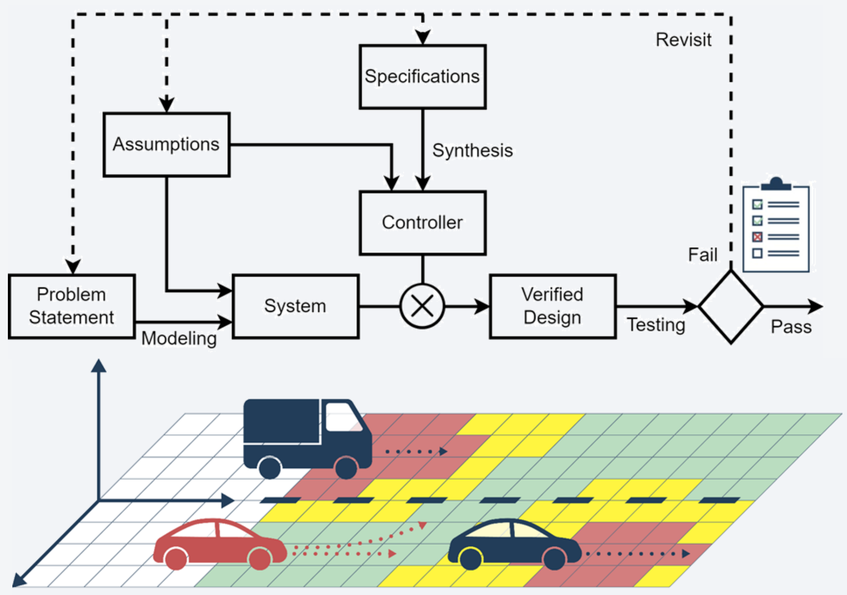
- Automated driving systems (ADS) consist of complex subsystems and components
- Modeling ADS in the right level of abstractions becomes challenging
- Synthesis of provably controllers depend on the abstraction and the specifications

Therefore,

- Complex systems and specifications cannot be always formalized easily
- Simulating and testing for every possible input is not possible for such systems

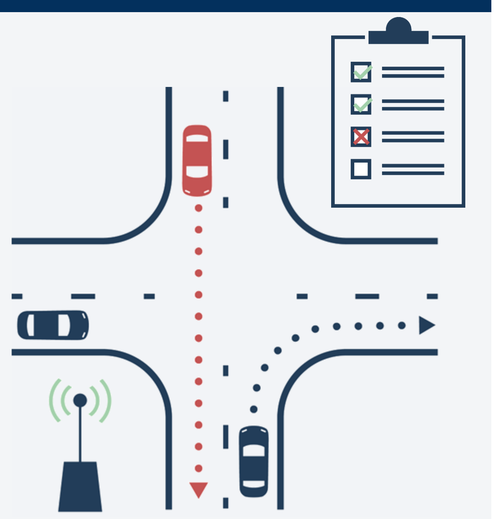
Methods and the Proposed Approach

- Safety assessment needs to combine simulation-based testing with formal methods
- Formal design based on modeling assumptions and specifications
- Abstraction of hybrid systems and over-approximation
- Using receding horizon algorithms to avoid collisions
- Testing for the validation of the assumptions and specifications



Results – Safety Assessment of ADS

- Efficient simulation-based testing strategies for ADS using fault injection
- Determining fault-error-failure chain and error propagation analysis yield limits for fault tolerance capabilities of ADS
- A holistic approach starting with safe design based on synthesis, then supported by simulation-based testing on different levels of abstraction for detecting edge cases



Publications

- IAV2022
- FKFS2021
- DSN-W2020
- FKFS2020
- IAV2019
- Simulink Challenge 2018 and 2019
  1st Place
- NECSYS2018

Technische Universität Dresden
Fakultät Elektrotechnik und Informationstechnik
Institut für Automatisierungstechnik
www.et.tu-dresden.de/ifa

Ansprechpartner: M.Sc. Mustafa Saraoğlu
E-Mail: mustafa.saraoglu@tu-dresden.de
Besucheradresse: Barkhausen Bau, Room E29