TECHNISCHE UNIVERSITÄT DRESDEN

IFA LS-AT

Fakultät für Elektrotechnik und Informationstechnik • Institut für Automatisierungstechnik

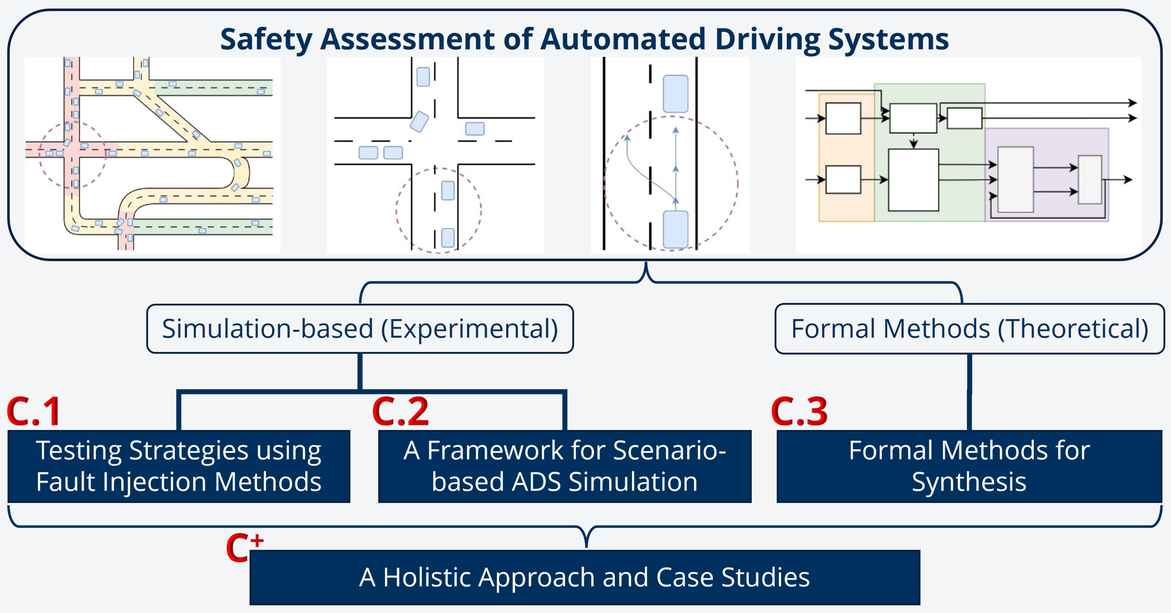
On Safety Assessment of Automated Driving Systems using Simulation-based Testing and Formal Methods

Motivation and Main Challenges

- Automated vehicles (AVs) need to be significantly and provably safe for future mobility
- The automated driving tasks for AVs are mainly categorized as perception, decision-making, and motion control
- Safety assessment of automated driving systems (ADSs) is challenging:
  - Integrating various components for automated driving makes the ADS architecture complex
  - The AVs interact with each other in difficult traffic situations

Key Contributions

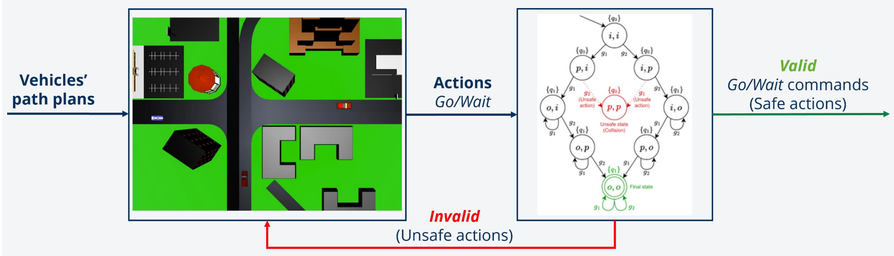
- **C.1: Safety assessment** of **ADS** using **simulation-based testing** strategies with fault injection
- **C.2:** Development of **an autonomous traffic simulation** framework, **MOBATSim**, for scenario-based ADS simulation
- **C.3:** Using Formal Methods for Safe Algorithms Design: **formal methods for synthesis** for discrete systems, and **reachability analysis and game theory** for maneuver planning for highway driving



Chosen ADS Applications and Used Methods

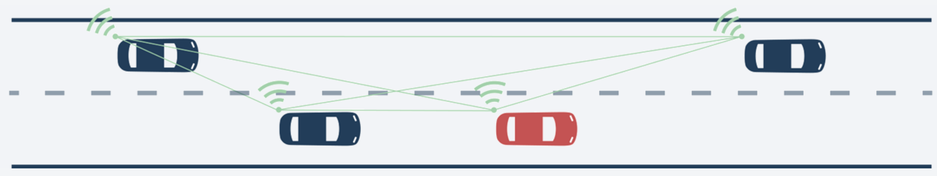
Autonomous Intersection Management

- Finite Transition Systems and Büchi Automaton
- Linear Temporal Logic (LTL) specifications
- Correct-by-construction control protocol synthesis



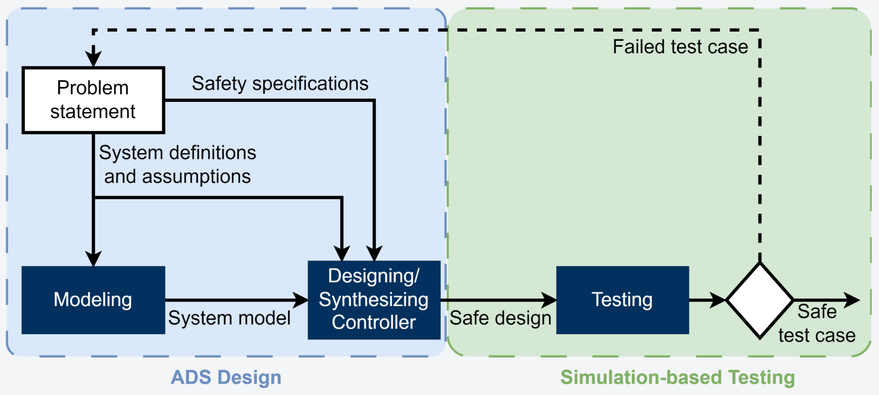
Highway Driving - Maneuver Planning

- Reachability analysis for dynamical systems
- Trajectory generation in Frenet coordinates
- Fixed Abstraction and Over-approximation
- Game-Theoretical Decision-making in a receding horizon



Main Findings - The Holistic Approach

- Incorporating formal methods and simulation-based testing into a holistic approach **C+** for safety assessment
- A useful workflow for modeling, designing/synthesizing, and testing ADSs
- Provides helpful results that point out the weaknesses in the safety of the tested the control and decision-making algorithms used in these ADS components



Highlights

- **Doctoral Thesis:** Saraoglu, M. (2024). On Safety Assessment of Automated Driving Systems Using Simulation-based Testing and Formal Methods.
- **ACC2023:** Saraoglu, M., Jiang, H., Schirmer, M., Mutlu, İ., and Janschek, K. (2023). A Minimax-based Decision-Making Approach for Safe Maneuver Planning in Automated Driving, 2023 American Control Conference (ACC), pages 4683–4690. IEEE.
- **IAV2022:** Saraoglu, M., Pintscher, J., and Janschek, K. (2022). Designing a safe intersection management algorithm using formal methods. IFACPapersOnLine, 55(14):22–27.
- **IAV2019:** Saraoglu, M., Morozov, A., and Janschek, K. (2019). Mobatsim: Model-based autonomous traffic simulation framework for fault-error-failure chain analysis. IFAC-PapersOnLine, 52(8):239–244.
- **Simulink Challenge 2018 - 1st Place:** The MathWorks, Inc. Simulink Student Challenge Winners. https: //www.mathworks.com/academia/student-challenge/simulink- student- challenge- 2018.html. 2018. (Announced on 14-Jan-2019). [Accessed: 11-Jun-2024].

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

Ansprechpartner: Dr.-Ing. Mustafa Saraoğlu
E-Mail: mustafa.saraoglu@tu-dresden.de
Besucheradresse: Barkhausen Bau, Room E12