The UnCoVerCPS Verification Approach to Automated Driving

Daniel Heß
Motivation: Safety of (Highly) Automated Vehicles

- AV are Safety critical, **Cyber-Physical Systems**
- High degree of **Adaptability** and **Decisional Autonomy** required

⇒ **Testing at its limit:**

Official press release from Robert Bosch GmbH [1]: "If you were to test an automated car like a 'normal' vehicle, you’d have to drive it for several 100,000 years. Therefore, entirely new testing processes need to be developed for automated vehicles and the entire industry is still in the early stages, in this regard.“

⇒ **Offline Verification at its limit („verification barrier“):**

Estimation of the number of variables for classical verification approach [2]:
- (4) For every surrounding vehicle: Position (x,y), velocity, orientation
- (3) For each lane: Width, curvature, change of curvature
- (8) Ego-vehicle: Position (x,y), velocity, orientation, yaw rate, slip angle, road friction, current loading

Assuming that for each variable we only consider 20 values and do not distinguish between vehicle types (car, truck, pedestrian, motorbike, bicycle), that we consider no more than 10 surrounding vehicles and no more than 5 lanes, we obtain a problem description with

\[(20^4)^{10} \times (20^3)^5 \times 20^8 \approx 10^8 \text{ variables} \]

UnCoVerCPS (2015-2018)

- **Unifying Control** and **Verification** of **Cyber-Physical Systems**
- EU Horizon 2020, [http://cps-vo.org/group/UnCoVerCPS](http://cps-vo.org/group/UnCoVerCPS)
- **Objectives:**
  - Model-based development & online verification ➔ guarantee safety in unknown environment
  - Cross-domain approach: Synthesizing and verifying controllers on-the-fly
  - Develop a tool chain implementing the concepts
  - Demonstration of “Safe Cooperative Automated Driving“

- Tech. Univ. München (Lead)
- Univ. J. Fourier Grenoble
- Univ. Kassel
- Politecnico di Milano
- GE Global Research EU
- Robert Bosch GmbH
- DLR
- Esterel Technologies
- Tecnalia
- R.U. Robotics Ltd
Agenda

- Motivation and Overview of the UnCoVerCPS Project
- Our Approach to Safe Automated Driving
- Testing, Offline- and Online-Verification Steps
- Generation of Safe Maneuver Automata
- Emergency Maneuver Planning
- Conclusion
Our Approach to Safe Automated Driving

1. Verification of the closed-loop behavior for short maneuver stubs „safe motion primitives“
   ➔ Reachable sets of system state
   ➔ Occupancy of x-y-t-space

2. Initial conditions for sequencing of the motion primitives
   ➔ Safe Maneuver Automaton

3. Prediction of other participants with formal guarantees

4.-5. Planning of a safe overall maneuver

6. Execution of maneuver

Testing, Offline- and Online Verification Process

Diagram:
- C2C
- High-Level Behaviors
  - Set points
  - Measurements
  - Low-Level Control
  - Set points
  - Physical Vehicle
Testing, Offline- and Online Verification Process - 1

1. Conformance Testing

- Control-Loop/Online
- Design process/Offline

High-Level Behaviors

Low-Level Control

Physical Vehicle

set points

measurements

test drives

validated vehicle model f(x)
Testing, Offline- and Online Verification Process - 2

1. Conformance Testing

- Test drives
- Validated vehicle model $f(x)$
- State space bounds

2. Reachability Analysis

- Equation $u(x)$
- Set points
- Measurements

Low-Level Control

- Set points
- Measurements

High-Level Behaviors

- C2C

Physical Vehicle

- Measurements

Control-Loop/Online

Design process/Offline
C2C

1. Conformance Testing

- Test drives

2. Reachability Analysis

- Equation \( u(x) \)
- Set points
- Measurements

3. Maneuver Database

- Dynamically safe set points
- State space bounds
- Validated vehicle model \( f(x) \)

Physical Vehicle

Low-Level Control

High-Level Behaviors

set points

Design process/Offline

Control-Loop/Online
Testing, Offline- and Online Verification Process - 4

1. Conformance Testing
   - test drives

2. Reachability Analysis
   - equation $u(x)$
   - validated vehicle model $f(x)$
   - state space bounds

3. Maneuver Database
   - dynamically safe set points
   - set points
   - measurements

4. Emergency Maneuver Planner
   - desired set points
   - safe set points
   - "situation"

   - C2C

High-Level Behaviors

Low-Level Control

Physical Vehicle

Physical Vehicle

Low-Level Control

High-Level Behaviors

Control-Loop/Online

Design process/Offline
Testing, Offline- and Online Verification Process - 4

1. Conformance Testing
   - Test drives
   - Validated vehicle model $f(x)$
   - State space bounds
   - Maneuver Database

2. Reachability Analysis
   - Equation $u(x)$
   - Safe set points
   - Low-Level Control
   - Measurements

3. Maneuver Database
   - Dynamically safe set points
   - “Situation”
   - C2C

4. Emergency Maneuver Planner
   - Desired set points
   - High-Level Behaviors

Physical Vehicle

Low-Level Control

High-Level Behaviors
Computation of a Safe Maneuver Automaton (offline)

Reference behavior, defined by set points and error free model
Computation of a Safe Maneuver Automaton (offline)

Example open-loop behavior with errors
Computation of a Safe Maneuver Automaton (offline)

Example closed-loop behavior with errors
Computation of a Safe Maneuver Automaton (offline)

- Reference behavior
- Set of reachable system states $R_1(t)$ (containing all closed-loop behaviors with errors)

Comput Reachable Set trajectory $R_1(t)$
- For closed loop system
  - with bounded disturbances
  - with given set point / reference behavior
- For an initial set $R_1(0)$
- With an end set $R_1(t_f)$
Computation of a Safe Maneuver Automaton (offline)

Nominal trajectory $\tau_1^*$

Set of reachable system states $R_1(t)$ (containing all closed-loop behaviors with errors)

Set of positions possibly covered by vehicle body ➔ Used for collision tests
Computing of a Safe Maneuver Automaton (offline)

1. Repeat computation of reachable sets for multiple, short maneuvers
Computation of a Safe Maneuver Automaton (offline)

1. Repeat computation of reachable sets for multiple, short maneuvers

Nominal trajectory $\tau_1^*$

Set of reachable system states $R_1(t)$ (containing all closed-loop behaviors with errors)

Set of positions possibly covered by vehicle body $\rightarrow$ Used for collision tests
Computation of a Safe Maneuver Automaton (offline)

1. Repeat computation of reachable sets for multiple, short maneuvers

---

Nominal trajectory $\tau_1^*$

Set of reachable system states $R_1(t)$ (containing all closed-loop behaviors with errors)

Set of positions possibly covered by vehicle body ➔ Used for collision tests
Computation of a Safe Maneuver Automaton (offline)

1. Repeat computation of reachable sets for multiple, short maneuvers
Computation of a Safe Maneuver Automaton (offline)

1. Repeat computation of reachable sets for multiple, short maneuvers

---
Nominal trajectory $\tau_1^*$

Set of reachable system states $R_1(t)$ (containing all closed-loop behaviors with errors)

Set of positions possibly covered by vehicle body ➔ Used for collision tests
Computation of a Safe Maneuver Automaton (offline)

1. Repeat computation of reachable sets for multiple, short maneuvers

--- Nominal trajectory $\tau_1^*$

Set of reachable system states $R_1(t)$ (containing all closed-loop behaviors with errors)

Set of positions possibly covered by vehicle body ➔ Used for collision tests
Computation of a Safe Maneuver Automaton (offline)

1. Repeat computation of reachable sets for multiple, short maneuvers
2. Decide which maneuvers can be safely connected
   ➔ Defines order of online execution

- - -  Nominal trajectory $\tau_1^*$

Set of reachable system states $R_1(t)$ (containing all closed-loop behaviors with errors)

Set of positions possibly covered by vehicle body ➔ Used for collision tests
Computation of a Safe Maneuver Automaton (offline)

Safe Maneuver Sequences:

- Final set of maneuvers 1-3
- Initial set of maneuver 4
- $m_4$ can be executed after $m_1$, $m_2$ or $m_3$
Computation of a Safe Maneuver Automaton (offline)

- System state: Tracking error
  - $e_t$ longitudinal deviation
  - $e_n$ lateral deviation
  - $e_\varphi$ heading error
  - $e_v$ velocity error
  - $e_\omega$ yaw rate error
  - $e_\beta$ slip angle error

- Red: $R_i(0)$ initial set, before maneuver $i$
- Blue: $R_i(T_i)$ final set, after maneuver $i$
- Gray: Intermediate sets
- Black: Example traces
Testing, Offline- and Online Verification Process - 4

1. Conformance Testing
   - Measurements
   - Test drives

2. Reachability Analysis
   - Set points
   - Equation \( u(x) \)
   - Validated vehicle model \( f(x) \)
   - State space bounds

3. Maneuver Database
   - Safe set points
   - Dynamically safe set points
   - Desired set points

4. Emergency Maneuver Planner
   - "Situation"
   - C2C
   - Desired set points

High-Level Behaviors

Low-Level Control

Physical Vehicle
Emergency Maneuver Planner answers following questions:

- A High-Level Behavior **selects a certain set point**.
  - Is it safe to execute?
- A High-Level Behavior **agrees to a cooperation request**.
  - Is it safe to accept the additional constraints?

- Yes - if a safe emergency maneuver exists
  - which starts after execution of the set point
  - which brings the vehicle to a stand-still
  - which respects all safety constraints
  - which respects the additional cooperation constraints
Emergency Maneuver Planning (online)
Emergency Maneuver Planning (online)
Emergency Maneuver Planning (online)
Emergency Maneuver Planning (online)
Emergency Maneuver Planning (online)
Emergency Maneuver Planning (online)
Conclusions

➢ Validation of Automated Vehicles is hard
  ➢ If using either offline verification or testing exclusively

➢ The UnCoVerCPS approach
  ➢ Uses a combination of testing, offline verification and online verification
  ➢ Requires relatively little test km to validate vehicle model
  ➢ Provides a safe high-level cooperation mechanism
  ➢ Guarantees* low-level control performance for validated vehicle model
  ➢ Guarantees* safety of the high-level decisions by acting as a gateway
    * “Formal Guarantees” under comprehensive assumptions:
      ▪ Errors have to remain inside specified bounds
      ▪ Other traffic participants have to adhere to specified rules

Thoughts:
➢ Other high-level driving behaviors no longer have to be considered safety critical
➢ Ideal for combination with informal, highly sophisticated approaches?
Challenges & Future Work

- Detailed analysis of computing speed and false positive rate
- Real-Life Demo with two cooperating vehicles: Braunschweig in mid 2018