FUTURE CHALLENGES FOR CPS THEORY: AUTOMOTIVE SYSTEMS

JENS OEHLERKING,
ROBERT BOSCH GMBH

BOSCH

Future challenges for CPS Theory: Automotive Systems
Bosch Key figures 2016*

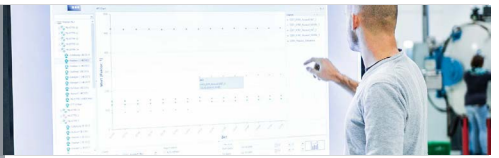
Bosch Group

- 73.1 billion euros in sales
- 389,281 associates

Mobility Solutions
- One of the world's largest suppliers of mobility solutions

60% share of sales

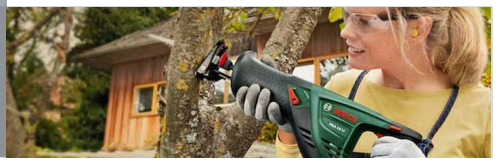
Industrial Technology
- Leading in drive and control technology, packaging, and process technology



Energy and Building Technology
- One of the leading manufacturers of security and communication technology
- Leading manufacturer of energy-efficient heating products and hot-water solutions

40% share of sales

Consumer Goods
- Leading supplier of power tools and accessories
- Leading supplier of household appliances

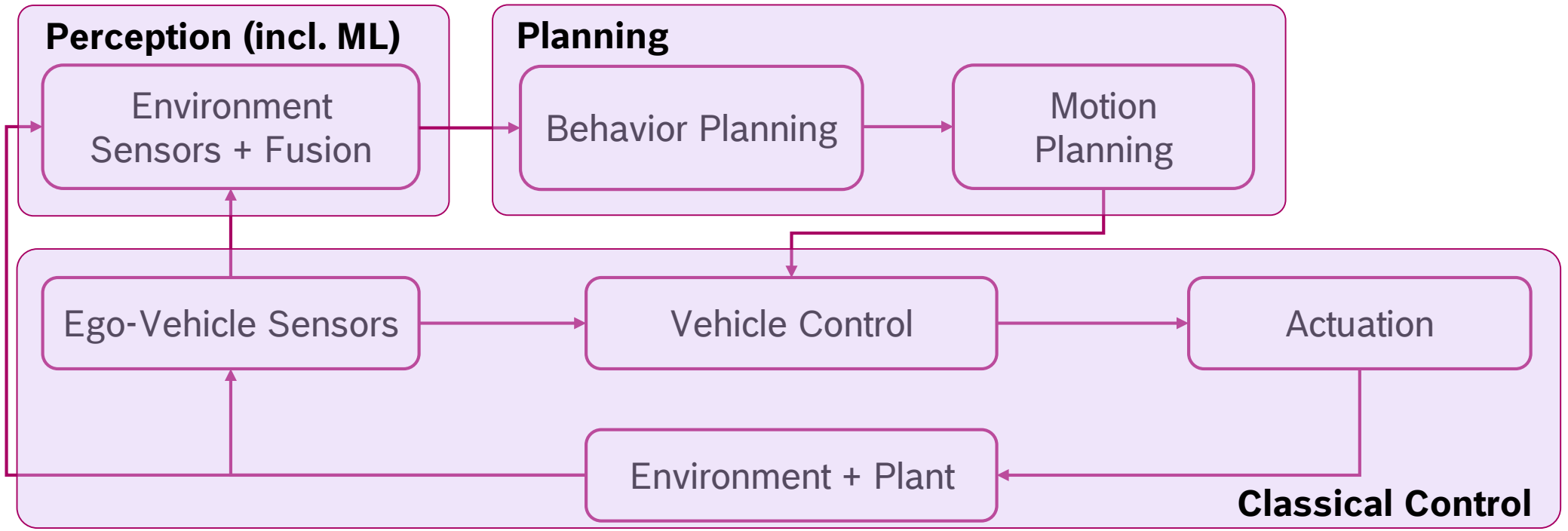


* As of 12.16

C/CCB, C/CCD | 2018-03-22

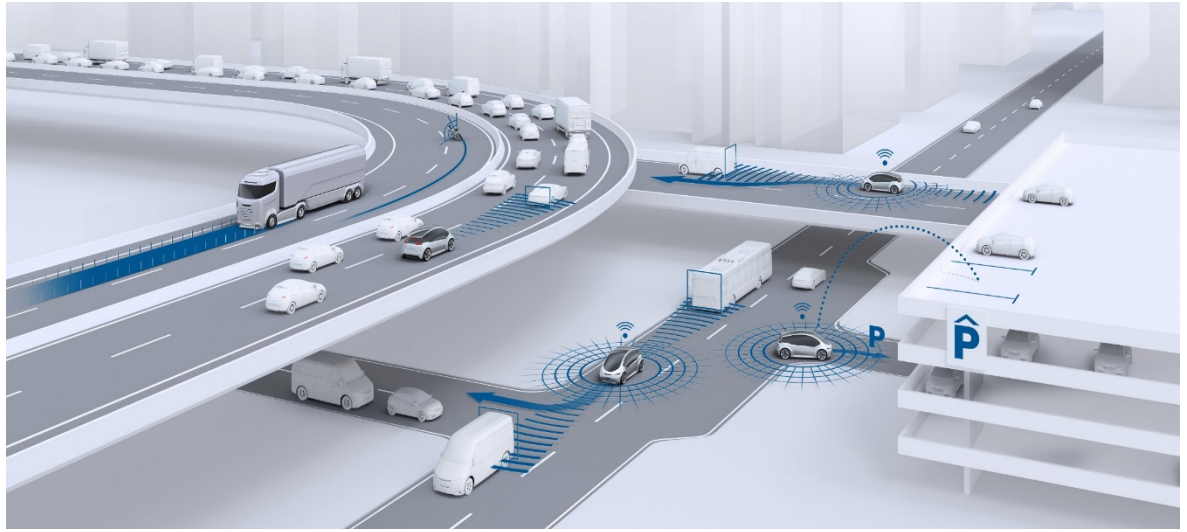
BOSCH

Future challenges for CPS Theory: Automotive Systems
Sketch of a Possible HAD Architecture



Requires a formal framework beyond classical hybrid systems!

Future challenges for CPS Theory: Automotive Systems
Challenges in Automated Driving Verification



What is new?

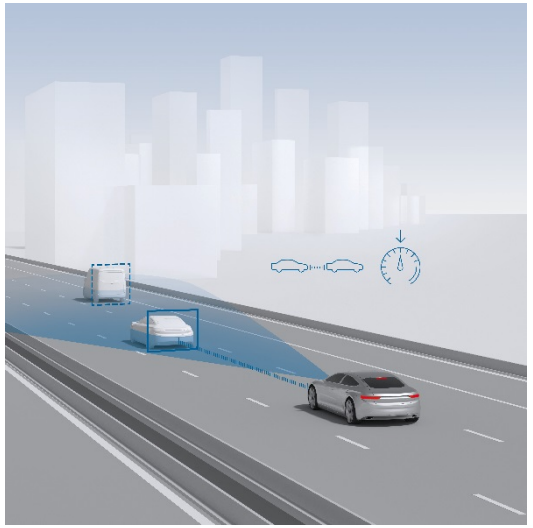
- Sensor uncertainties difficult to quantify
- Perception: data-based models (deep neural networks)
- Complexity of physical environment
- Interaction between multiple agents
- Communication in a safety critical context

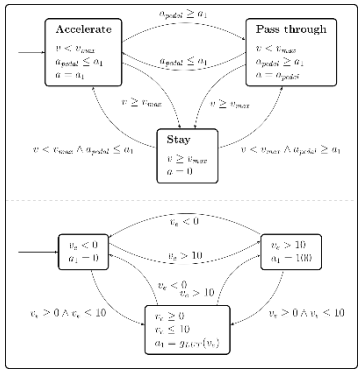
Q: How many miles driven are required to demonstrate for a given automated driving system with 95% confidence that they cause 20% less fatalities than human drivers?
A: 8.8 billion miles [*Kalra and Paddock: "Driving to Safety". RAND Corporation, 2016]*

Intractable without some form of formal methods!

Future challenges for CPS Theory: Automotive Systems

Modeling





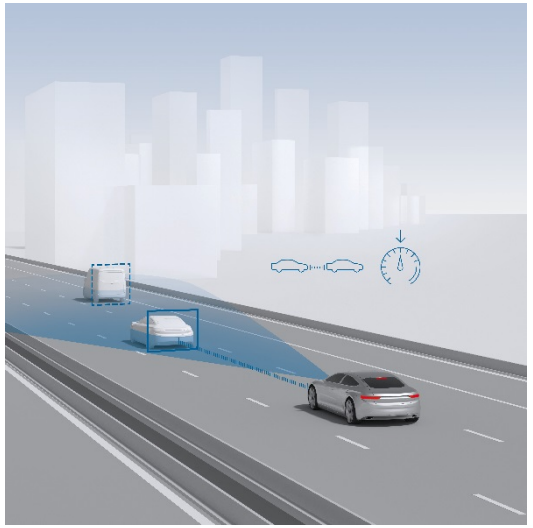
$$\dot{X} = v_x \cos(\varphi) - v_y \sin(\varphi)$$
$$\dot{Y} = v_x \sin(\varphi) + v_y \cos(\varphi)$$
$$\dot{v}_x = u_1 + v_y \omega$$
$$\dot{v}_y = f_{y,f}(x,u) + f_{y,r}(x) - v_x \omega - b\dot{\omega}$$
$$\dot{\Psi} = \omega$$
$$\dot{\omega} = a\frac{m}{J} f_{y,f}(x,u) - b\frac{m}{J} f_{y,r}(x)$$

- interacting agents
- ML-based perception
- models of complex sensors
- geometric structure of the environment

?

Future challenges for CPS Theory: Automotive Systems

Specification



$\square$ (cut_in $\rightarrow \Diamond_{[0,T1]} |d - d_{set}| < \varepsilon) \wedge$

$\square$ (cut_in $\rightarrow \square_{[T2,T3]}$ d > d_{min}) $\wedge$

$\square$ ((free_lane $\wedge$ $|\Delta v_{set}| > 0) \rightarrow$
$\Diamond_{[0,T4]} |v - v_{set}| < \varepsilon) \wedge$ ...

- formalized traffic rules
- explicit and implicit contracts between traffic participants
- assumptions on human behavior
- societally acceptable risk

?

BOSCH

Future challenges for CPS Theory: Automotive Systems

Occupancy Prediction for Mobile Robots

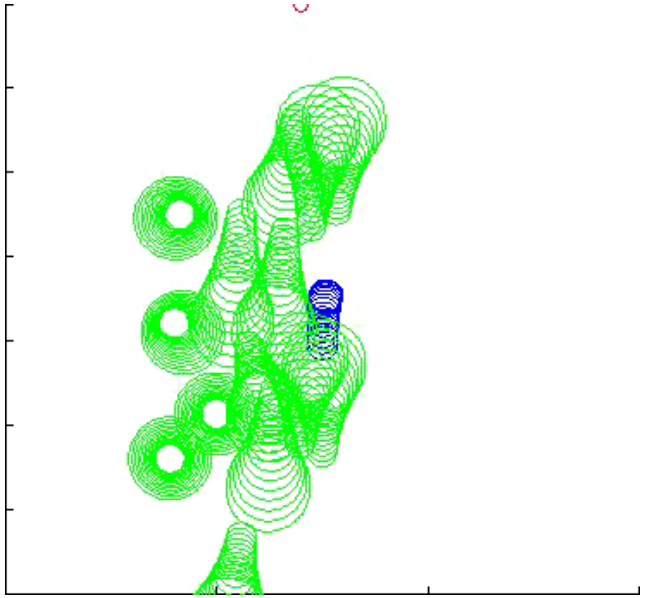
TABLE II: Results from ROS Simulation (Lightly Populated Scenarios)

	Flow				Cross-flow				Anti-flow			
Approach	@Goal	Time(s)	Len(m)	Vel(m/s)	@Goal	Time(s)	Len(m)	Vel(m/s)	@Goal	Time(s)	Len(m)	Vel(m/s)
Braking ICS	10	34.3	22.9	0.73	10	40.0	23	0.63	10	116.1	23.0	0.21
Safety Field	10	37.9	22.9	0.64	10	35.7	23	0.68	10	74.8	22.9	0.32
Onl. Verif.	10	22.4	22.9	1.04	10	26.3	23.2	0.91	10	52.3	23.0	0.45

TABLE III: Results from ROS Simulation (Densely Populated Scenarios)

	Flow				Cross-flow				Anti-flow			
Approach	@Goal	Time(s)	Len(m)	Vel(m/s)	@Goal	Time(s)	Len(m)	Vel(m/s)	@Goal	Time(s)	Len(m)	Vel(m/s)
Braking ICS	10	108.0	22.9	0.25	10	114.2	23.1	0.21	10	519.5	23.2	0.05
Safety Field	10	96.0	22.9	0.27	10	76.9	23	0.31	10	251.5	23.0	0.10
Onl. Verif.	10	26.0	23	0.92	10	37.8	23.1	0.65	10	159.2	23.2	0.15

- Implemented using CORA in MATLAB (online)
- Successfully checked conformance of pedestrian model against labeled video data
  - Only 16 errors in ~16.000 test cases (resulting from violated assumptions) for unbounded velocity
  - 71 errors for velocity bounded to 2.0 m/s (several running persons)

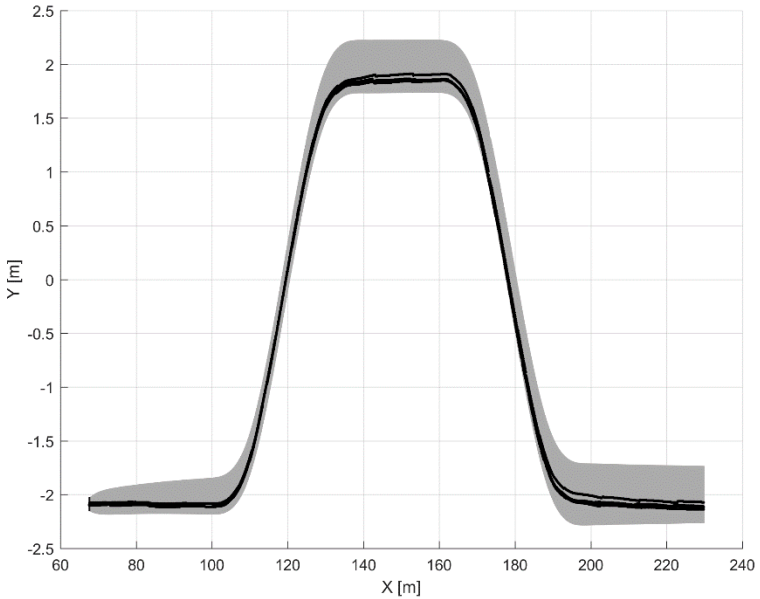


Future challenges for CPS Theory: Automotive Systems

Conformance & Monitoring

Classical hybrid systems verification:

Given a model of the “cyber” and the “physical” component, prove that some property holds on the composed system!



In safety critical contexts, trustworthiness of models is key!

This requires:

- Formalizable arguments about the quality of physical models
- Explicit assumptions on why a set of measurements for model validation/parameter identification was sufficient

→ conformance notions, falsification, coverage metrics, online monitoring

BOSCH

Future challenges for CPS Theory: Automotive Systems
Open questions

- How do we go beyond established modeling paradigms to enable the creation of the complex models that are needed?
- How do we argue the quality of models used in safety critical contexts?
- What formal arguments can be made about data-based software (e.g., neural networks)?
- How de we formalize the expected behavior of individual agents, so that their composition is (sufficiently) safe?
- What should be considered “sufficiently safe”?