This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 643921.

Overview of UnCoVerCPS

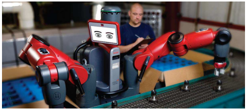
Matthias Althoff, Technische Universität München

UnCoVerCPS Workshop, Milan, 06 June 2018

Examples of Cyber-Physical Systems

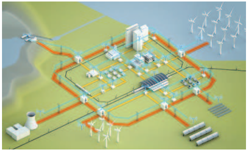
automated driving

source: Carnegie Mellon University



human-robot collaboration

source: Rethink Robotics



smart grids

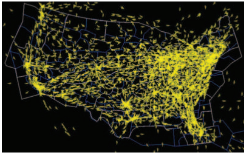
source: Siemens

automated farming

source: Kesmac

surgical robots

source: daVinci



air traffic control

source: NASA

Emerging technologies are increasingly safety- or operation-critical!

EU Project UnCoVerCPS: Partners

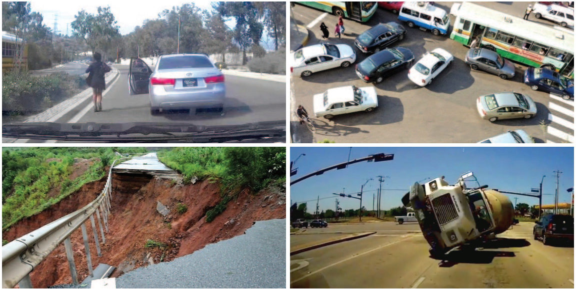
Unifying Control and Verification of Cyber-Physical Systems
(UnCoVerCPS)

Funding: 4.9 mio Euro

Participant organisation name	Country
Technische Universität München (TUM)	Germany
Université Joseph Fourier Grenoble 1 (UJF)	France
Universität Kassel (UKS)	Germany
Politecnico di Milano (PoliMi)	Italy
GE Global Research Europe (GE)	Germany
Robert Bosch GmbH (Bosch)	Germany
Esterel Technologies (ET)	France
Deutsches Zentrum für Luft- und Raumfahrt (DLR)	Germany
Tecnalia (Tec)	Spain
R.U.Robots Limited (RUR)	United Kingdom

Expect the Unexpected

How to ensure safety in uncertain environments?

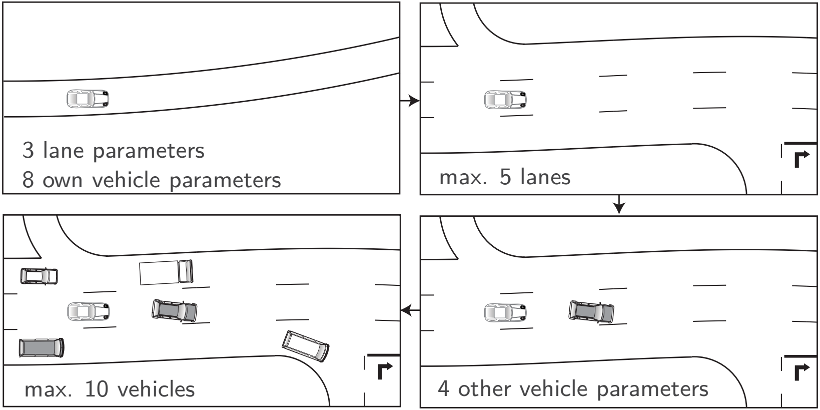


Automated driving: classical testing [N. Kalra and S. M. Paddock (2016)]

- 440 million km to demonstrate better performance than humans (95% confidence).
- 12.5 years with 100 test vehicles continuously driving.

Possible Traffic Situations: A Rough Estimation

We assume that each variable of the verification problem has 20 values.



$(20^3)^5 \cdot (20^4)^{10} \cdot 20^8 \approx 9.2 \cdot 10^{81}$ scenarios

Main Idea

Paradigm shift in verification of CPS

Verification before deployment $\rightarrow$ **continuous self-verification**.

- Each momentary situation is considered;
- each action is only executed if it is formally verified;
- each verification is performed just-in-time.

Main Idea

Paradigm shift in verification of CPS

Verification before deployment $\rightarrow$ **continuous self-verification**.

- Each momentary situation is considered;
- each action is only executed if it is formally verified;
- each verification is performed just-in-time.

Advantages:

- Current scenario is always considered.
- Only current scenario required (smaller problem).

Main Idea

Paradigm shift in verification of CPS

Verification before deployment $\rightarrow$ **continuous self-verification**.

- Each momentary situation is considered;
- each action is only executed if it is formally verified;
- each verification is performed just-in-time.

Advantages:

- Current scenario is always considered.
- Only current scenario required (smaller problem).

Requirement: efficient and online-adaptable verification procedure.

Main Idea

Paradigm shift in verification of CPS

Verification before deployment $\rightarrow$ **continuous self-verification**.

- Each momentary situation is considered;
- each action is only executed if it is formally verified;
- each verification is performed just-in-time.

Advantages:

- Current scenario is always considered.
- Only current scenario required (smaller problem).

Requirement: efficient and online-adaptable verification procedure.

Impact: Reduced costs, fewer liability claims, enabling safe autonomy.

EU Project UnCoVerCPS: Main objectives

- Novel on-the-fly control and verification concepts.

EU Project UnCoVerCPS: Main objectives

- Novel on-the-fly control and verification concepts.
- Unifying control and verification to quickly react to changing environments.

EU Project UnCoVerCPS: Main objectives

- Novel on-the-fly control and verification concepts.
- Unifying control and verification to quickly react to changing environments.
- A unique tool chain that makes it possible to integrate modeling, control design, formal verification, and automatic code generation.

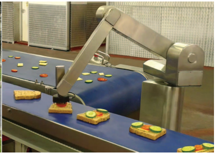
EU Project UnCoVerCPS: Main objectives

- Novel on-the-fly control and verification concepts.
- Unifying control and verification to quickly react to changing environments.
- A unique tool chain that makes it possible to integrate modeling, control design, formal verification, and automatic code generation.
- Prototypical realizations for automated vehicles, human-robot collaborative manufacturing, wind turbines and smart grids.

EU Project UnCoVerCPS: Main objectives

- Novel on-the-fly control and verification concepts.
- Unifying control and verification to quickly react to changing environments.
- A unique tool chain that makes it possible to integrate modeling, control design, formal verification, and automatic code generation.
- Prototypical realizations for automated vehicles, human-robot collaborative manufacturing, wind turbines and smart grids.
- A new development process that reduces development time and costs for critical cyber-physical systems.



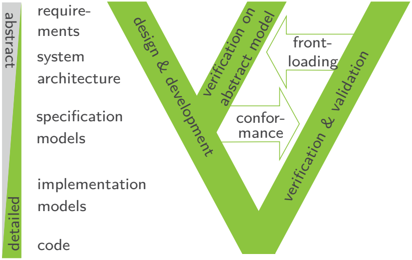


Beyond Online Verification

Unification of control and verification has also big potential for offline design:

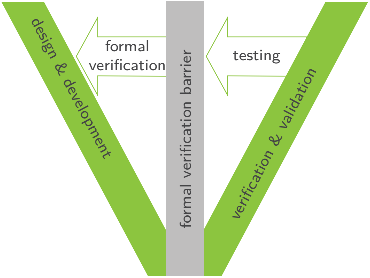
Front loading of verification

30% reduction of development time through front loading



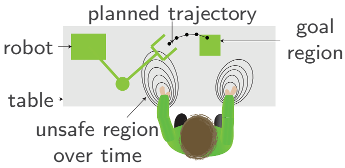
Formal verification barrier

E.g., 12.5 years of testing for autonomous vehicles

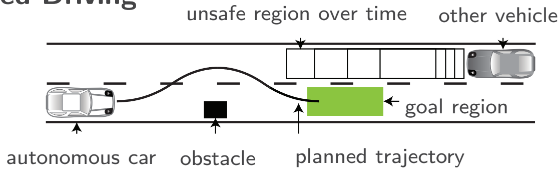


Problem Statement of Our Use Cases

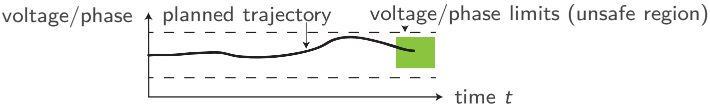
Human-Robot Co-Existence



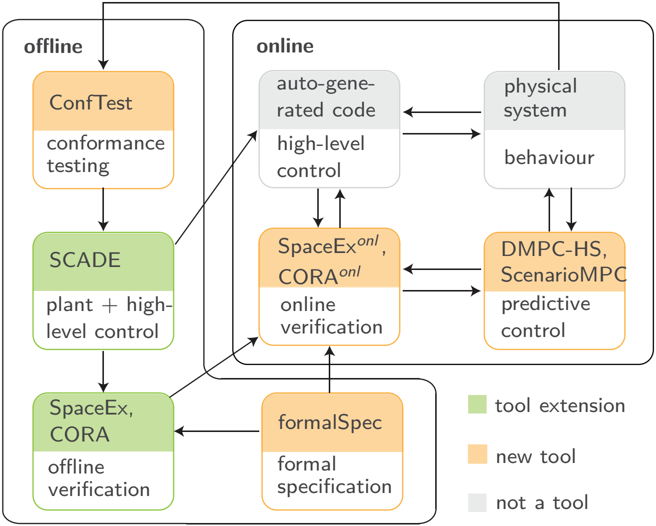
Automated Driving



Smart Grid (similar for wind turbine)

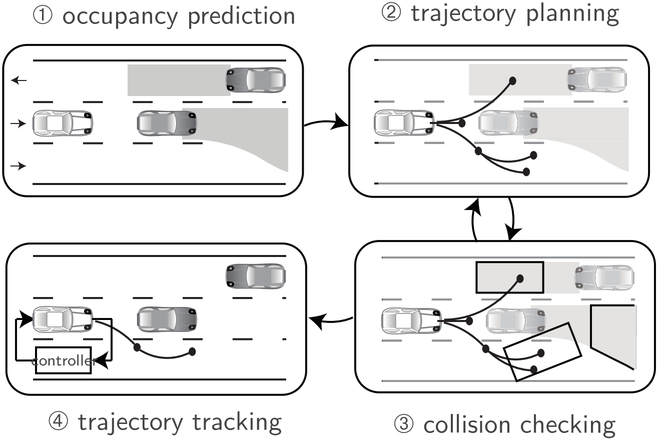


Tool chain of UnCoVerCPS



Prediction-planning-verification-control loop

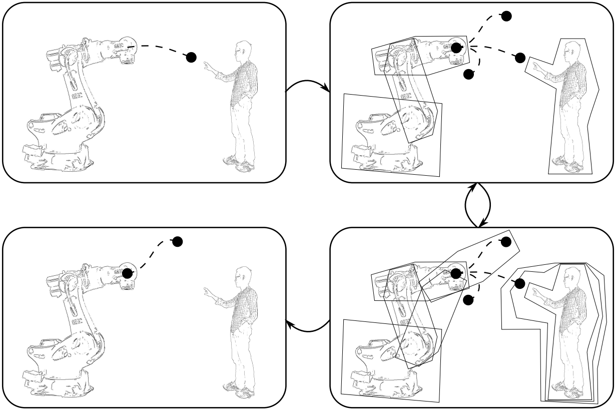
Use case: **automated driving**



Prediction-planning-verification-control loop

Use case: **human-robot co-existence**

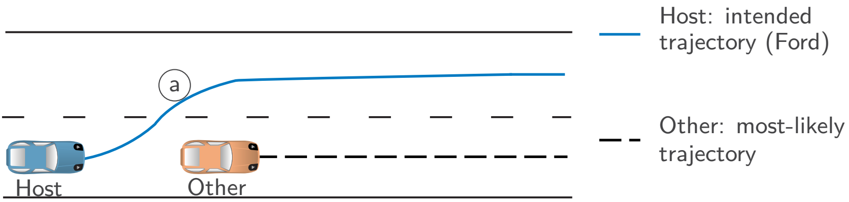
① desired trajectory ② trajectory planning



④ update of safe path ③ collision checking

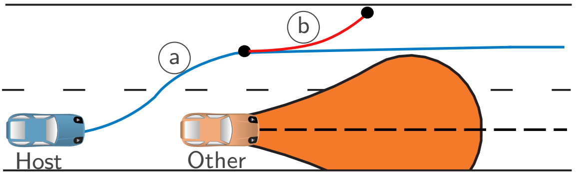
Interaction between Planning and Verification

time t_k:



Interaction between Planning and Verification

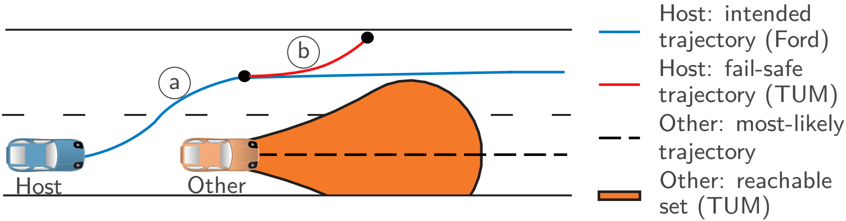
time t_k:



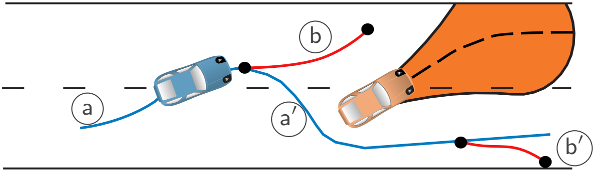
- Host: intended trajectory (Ford)
- Host: fail-safe trajectory (TUM)
- Other: most-likely trajectory
- Other: reachable set (TUM)

Interaction between Planning and Verification

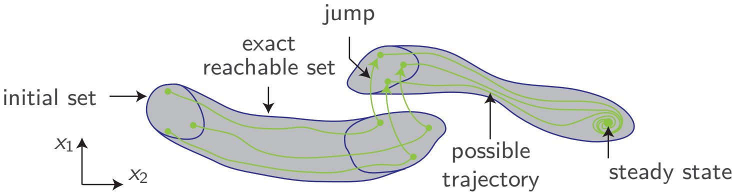
time t_k:



time t_{k+1}:



Reachable Sets

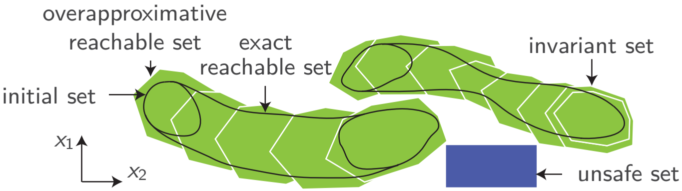


Informal Definition

A reachable set is the set of states that can be reached by a dynamical system in finite or infinite time for a

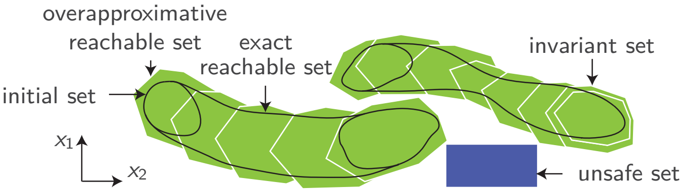
- set of initial states,
- uncertain inputs,
- and uncertain parameters.

Overapproximative Reachable Sets



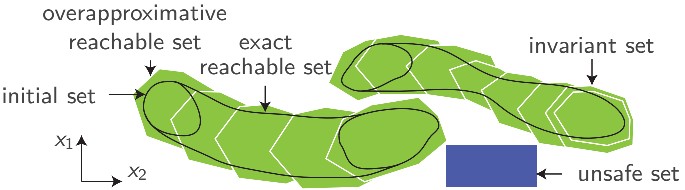
- Exact reachable set only for special classes computable
  $\rightarrow$ overapproximation computed for consecutive time intervals.

Overapproximative Reachable Sets



- Exact reachable set only for special classes computable
  $\rightarrow$ overapproximation computed for consecutive time intervals.
- Overapproximation might lead to spurious counterexamples.

Overapproximative Reachable Sets



- Exact reachable set only for special classes computable
  $\rightarrow$ overapproximation computed for consecutive time intervals.
- Overapproximation might lead to spurious counterexamples.
- Simulation cannot prove correctness.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 643921.

- Safety-critical, autonomous cyber-physical systems require on-the-fly control and verification.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 643921.

- Safety-critical, autonomous cyber-physical systems require on-the-fly control and verification.
- Changing environments require to unify control and verification to meet formal specifications.

This project has received funding from the European Union's Horizon 2020
research and innovation programme under grant agreement No 643921.

- Safety-critical, autonomous cyber-physical systems require on-the-fly control and verification.
- Changing environments require to unify control and verification to meet formal specifications.
- Advances are also beneficial to offline control and verification.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 643921.

- Safety-critical, autonomous cyber-physical systems require on-the-fly control and verification.
- Changing environments require to unify control and verification to meet formal specifications.
- Advances are also beneficial to offline control and verification.
- Our approach works across several application domains (de-verticalization).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 643921.

- Safety-critical, autonomous cyber-physical systems require on-the-fly control and verification.
- Changing environments require to unify control and verification to meet formal specifications.
- Advances are also beneficial to offline control and verification.
- Our approach works across several application domains (de-verticalization).
- We combine our expertise to establish a unique toolchain for future development of cyber-physical systems.