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

UnCoVerCPS Toolchain

Goran Frehse, *UGA*
et al.

UnCoVerCPS Review Meeting – February 7,2019

Tool Overview

- Specification
  - **formalSpec**: formalizing natural language
- Modeling and Simulation
  - **SCADE-hybrid**
  - **SpaceEx**
- Controller Synthesis
  - **DMPC-HS**: MPC for hybrid systems
  - **ScenarioMPC**: MPC for stochastic systems
- Code Generation
  - **SCADE** code generator
- Verification
  - **CORA/SPOT**: nonlinear systems
  - **SpaceEx**: piecewise linear systems
- Conformance Testing
  - **ConfTest**

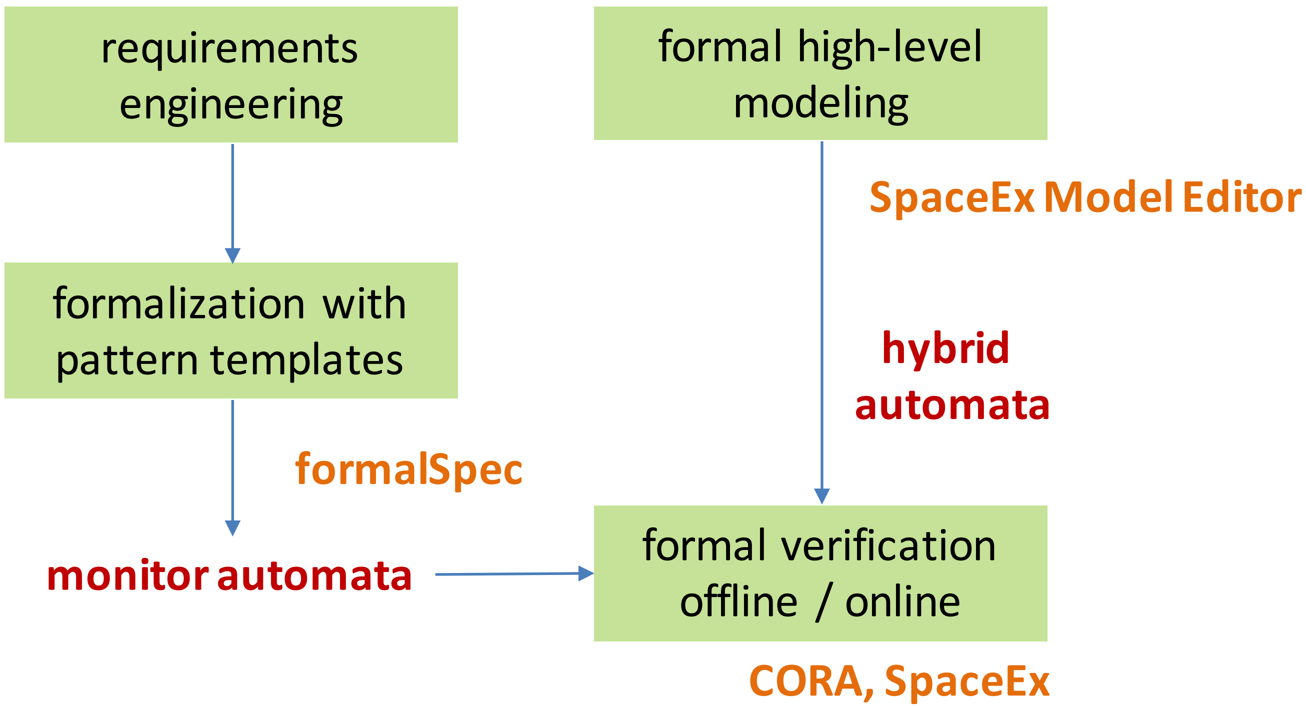
Objectives

- Goal: **Safe planning & control**
- Approach: Integrate **formal methods** in **design & operation**
- Formal specification
- Formal model & conformance
  - ensure conformance with reality
- Formal verification
  - offline: elementary plans & motion primitives
  - online: short & long-term plans

Use Case: Autonomous Driving

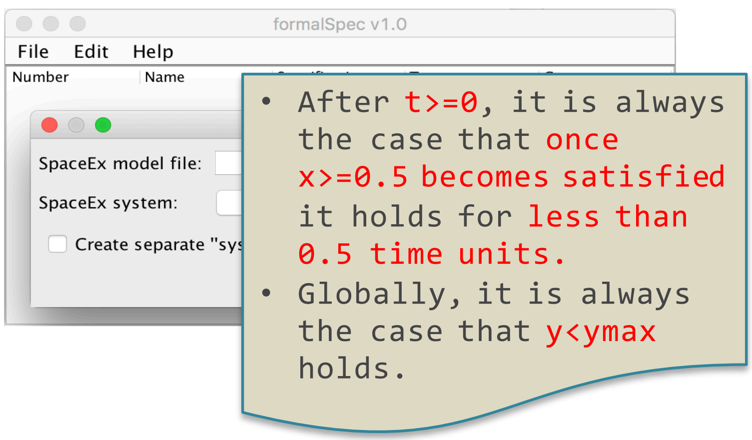
- formal specification
  - traffic rules
  - collision avoidance
- long-term planning
  - route planning, high-level maneuvers
  - performance optimization using stochastic models
- short-term planning
  - low-level maneuvers: lane changes, merging, obstacle avoidance
  - performance optimization
- fail-safe planning
  - to indefinitely safe state (standstill, safely follow)
- tracking control
  - realize current plan on vehicle

Formal Specification and Verification

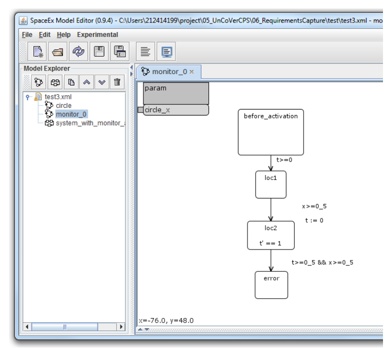


Formal Specification: formalSpec

- formalize specifications for a given model
- input: natural language edits to template,
  SX model
- output: monitor automaton
- developed by GE, contributions from UGA

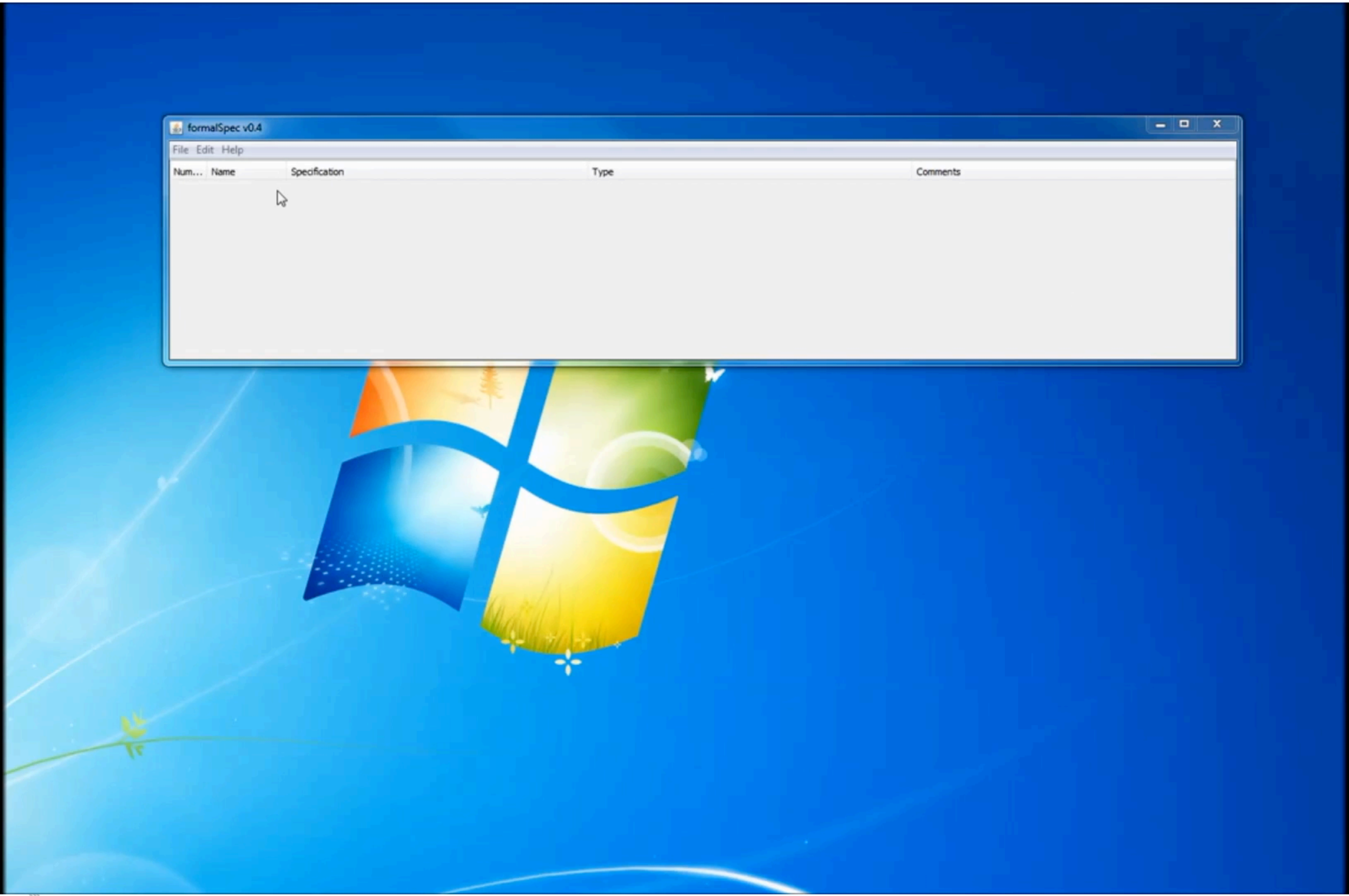


pattern template

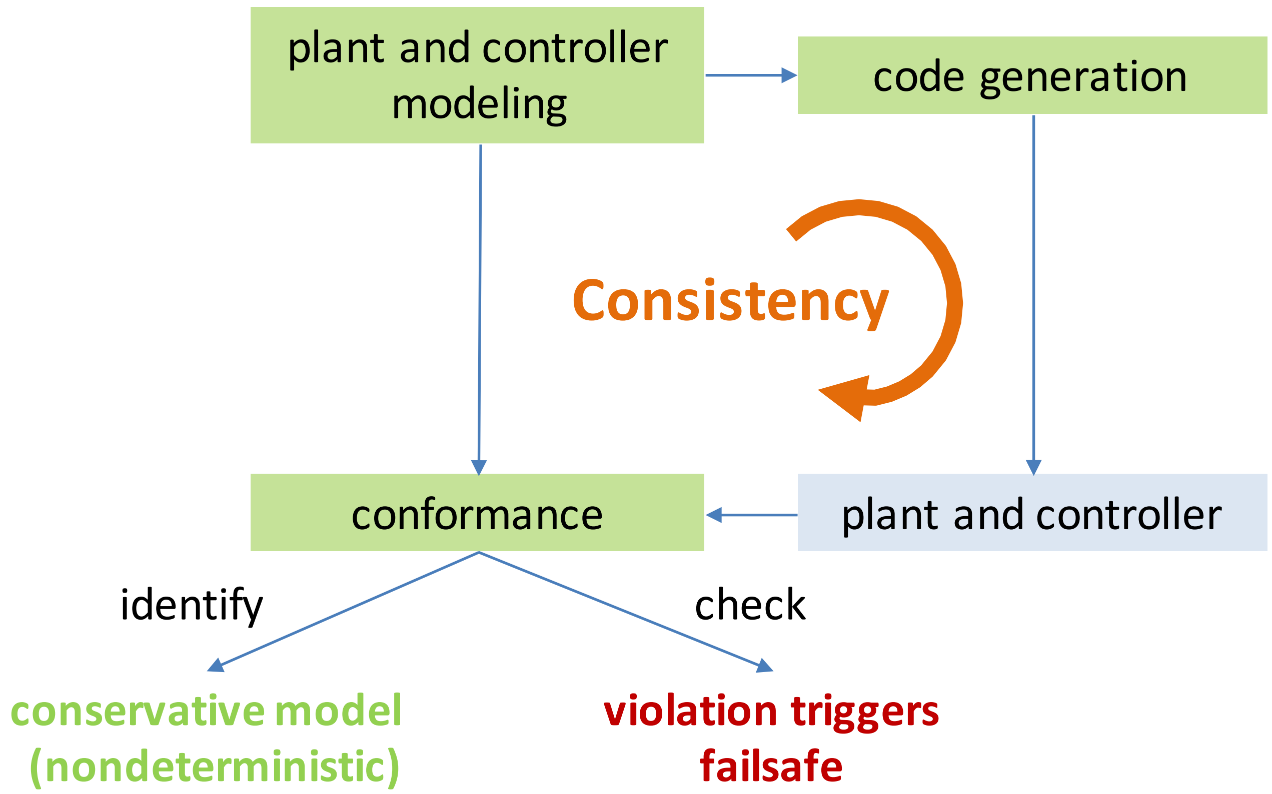


monitor automaton

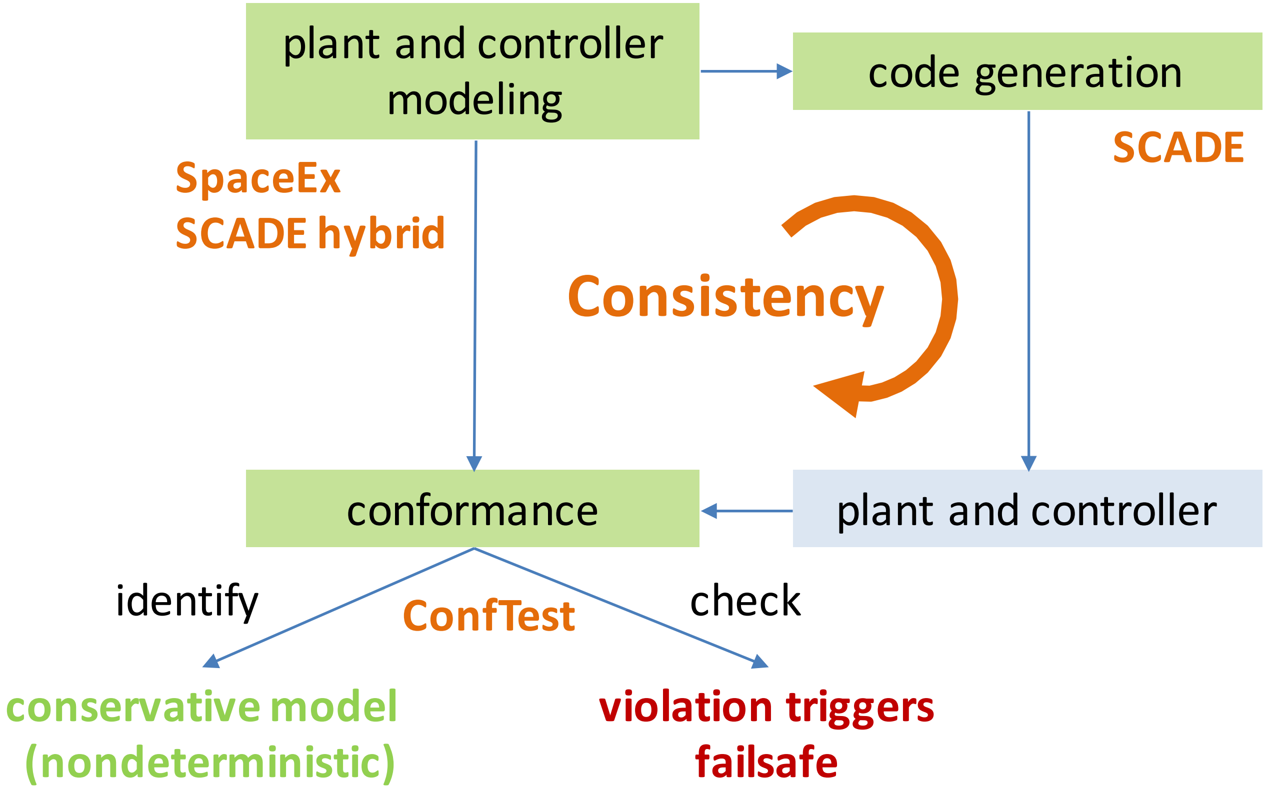
Formal Specification: Use Case



Conformance and Code Generation



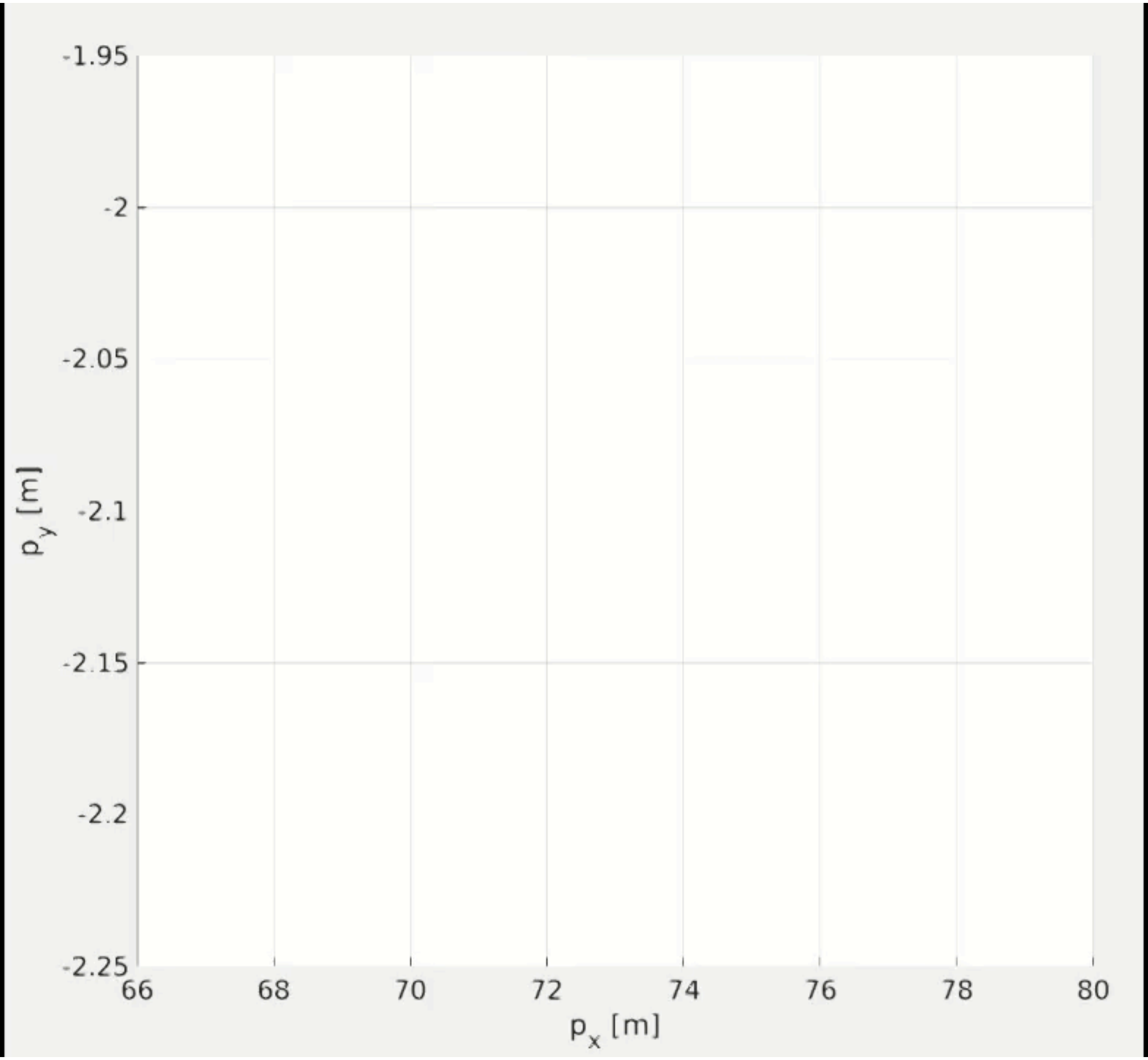
Conformance and Code Generation



Conformance: ConfTest

- Identification
  - identify abstract model that is trace and/or reachset conformant
  - input: deterministic model, reference data (e.g., measured traces)
  - output: conformant non-deterministic model
- Checking
  - check if non-deterministic abstract model is conformant
  - input: non-deterministic model, reference data (e.g., measured traces)
  - output: conformant: yes/no
- Test case generation
  - produce test cases for conformance testing
  - input: parametric input set, abstract model, reference system
  - output: test cases
- developed by Bosch, contributions from DLR & TUM

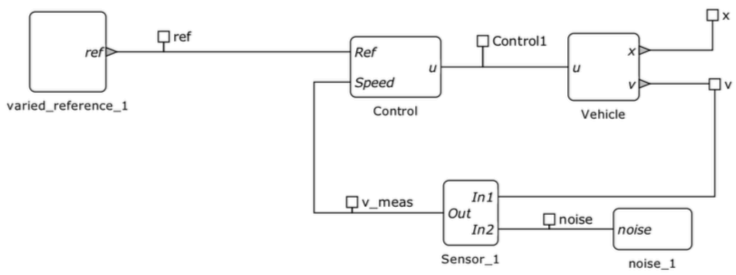
Conformance: ConfTest



Simulation: SCADE Hybrid

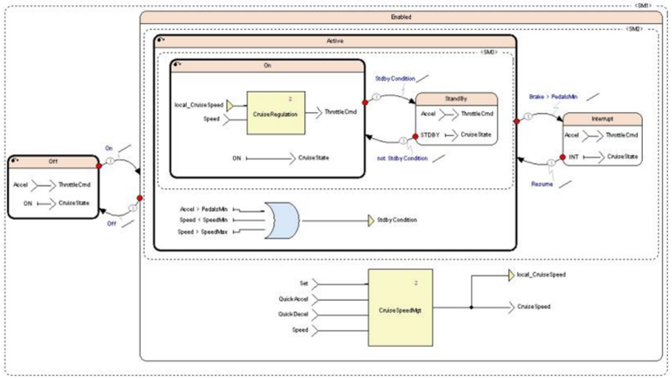
- Extension of SCADE to ODEs with well-defined semantics
  - industrial environment dedicated to high-integrity applications development
  - control-oriented input formalism
  - used in various domains: A&D, automotive, rail transport, industry, …
- input: deterministic model (SpaceEx, Simulink – Stafeflow)
- output: closed-loop simulation
- developed by Esterel

Simulation: Use Case

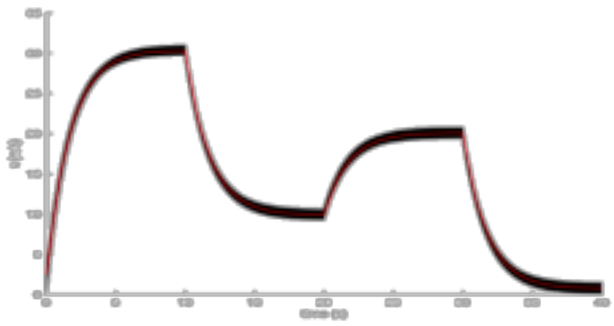


SpaceEx model

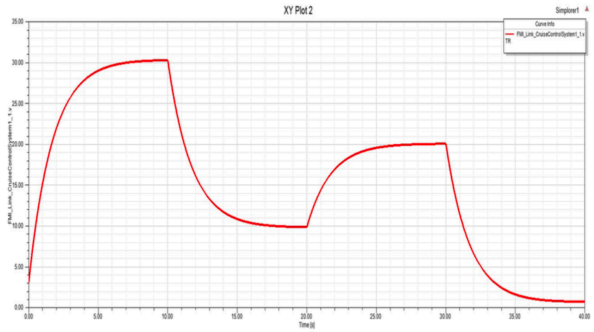
sx2sh



SCADE hybrid model



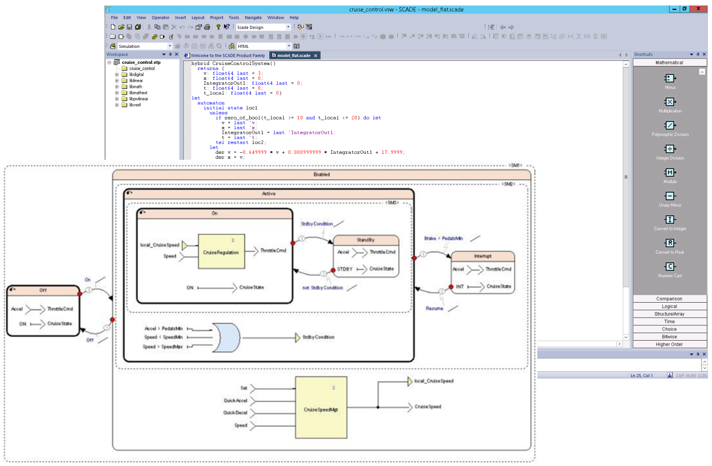
SpaceEx Verification



SCADE Hybrid Simulation

Code Generation: SCADE

- Code generation, certified ISO 26262, DO-178C, EN 50128, …
- input: controller model in SCADE hybrid
- output: certified C code
- developed by Esterel



SCADE hybrid model

SCADE code generator

```c
/* information used for corresponding FMI attribute */
#define KCG_GUID "8daf05a3-247a-11e5-aa15-2beff3ac55df"
#define MODEL_IDENTIFIER simple_ball

/* root operator functions */
#define STEP_FUN simple_ball
#define RESET_FUN simple_ball_reset
#define INIT_FUN simple_ball_init
#define CONT_FUN simple_ball_cont
#define HORIZON_FUN simple_ball_horizon

/* context and output structure */
#define SCADE_OUT_CTX outC_simple_ball
#define SCADE_IN_CTX inC_simple_ball

/* number of continuous states */
#define NB_CSTATE 2
/* number of zero-crossings */
#define NB_ZC 1

typedef struct {
    size_t offset;
} var_info;

extern const var_info var_infos[];

/* Information about a continuous state */
typedef struct {
    size_t offset;
} cstate_info;

#if NB_CSTATE > 0
extern const cstate_info cstate_infos[NB_CSTATE];
#endif

/* Information about a zero-crossing */
typedef enum { UP, DOWN, CROSS } zero_dir;

typedef struct {
    size_t offset;
    zero_dir dir;
} zero_info;

#if NB_ZC > 0
extern const zero_info zero_infos[NB_ZC];
#endif
```

certified C code

Use Case: Cruise Controller

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

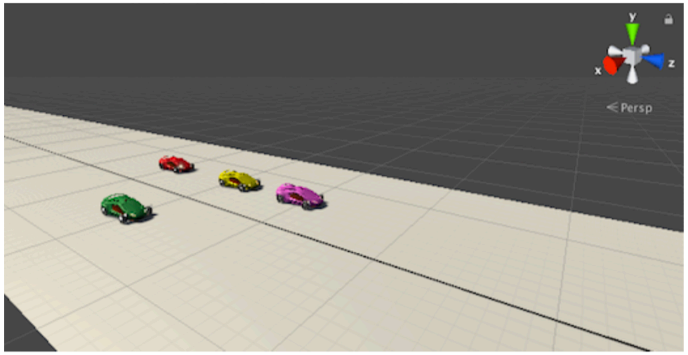
TOOLS INTEGRATION

UnCoVerCPS toolchain

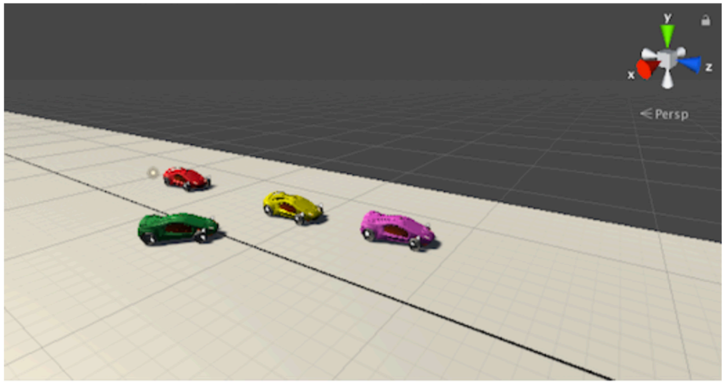
Offline Verification: SpaceEx

- modeling and verification of hybrid systems
- input: network of hybrid automata
  monitor automata (formalSpec)
- output: approximation of reachable states
  property satisfied/unknown
- developed by UGA, TUM (zonotopes)

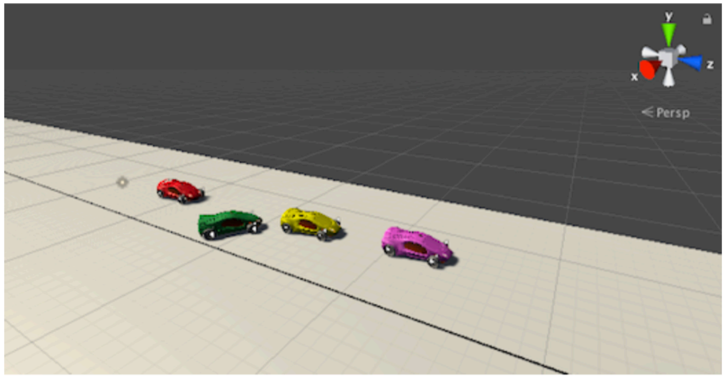
Use Case: Merging Maneuver



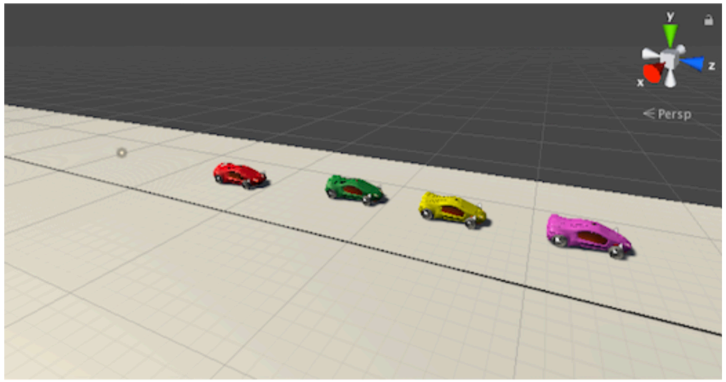
(a) Initial Phase (before maneuver)



(b) Maneuver has begun

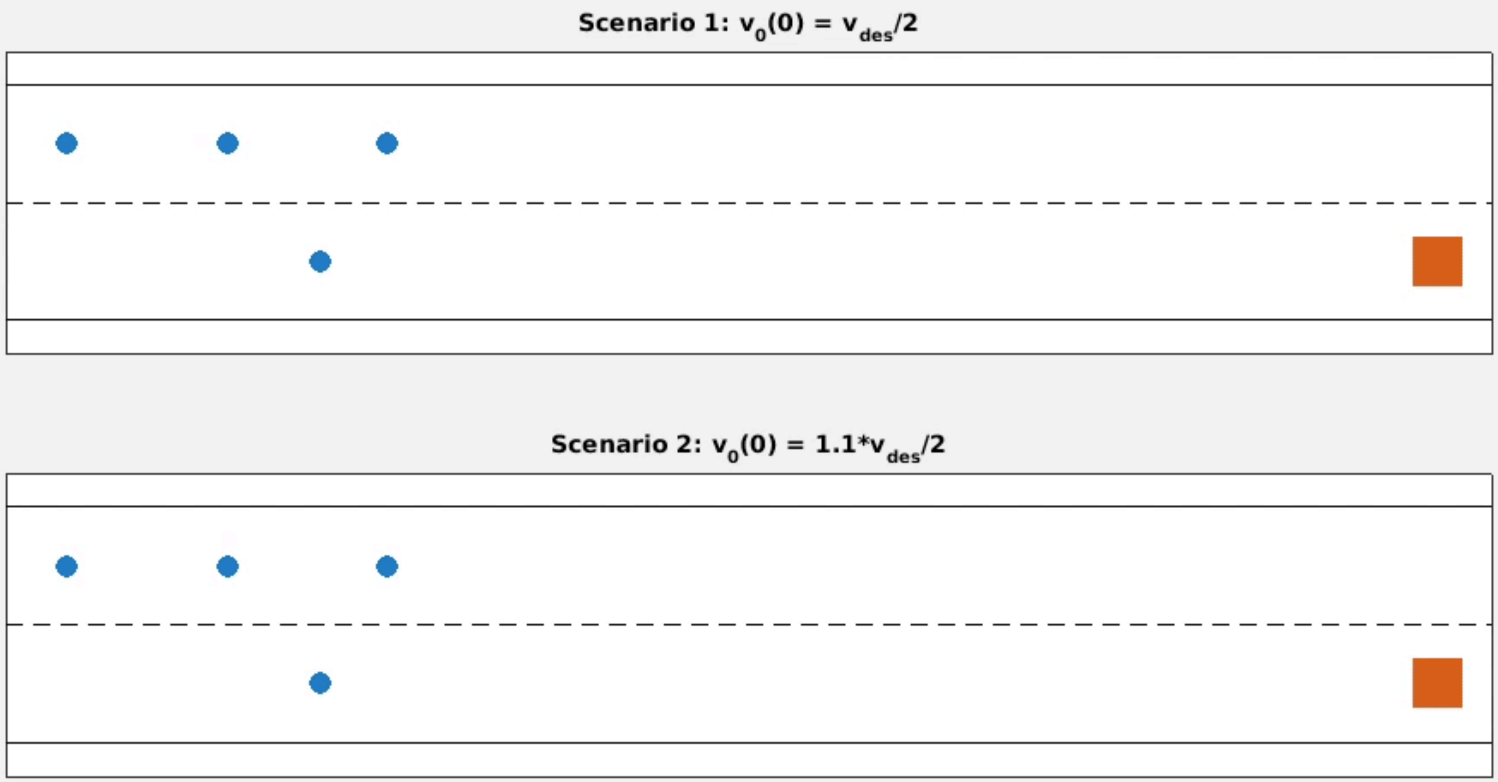


(c) Maneuver - in progress

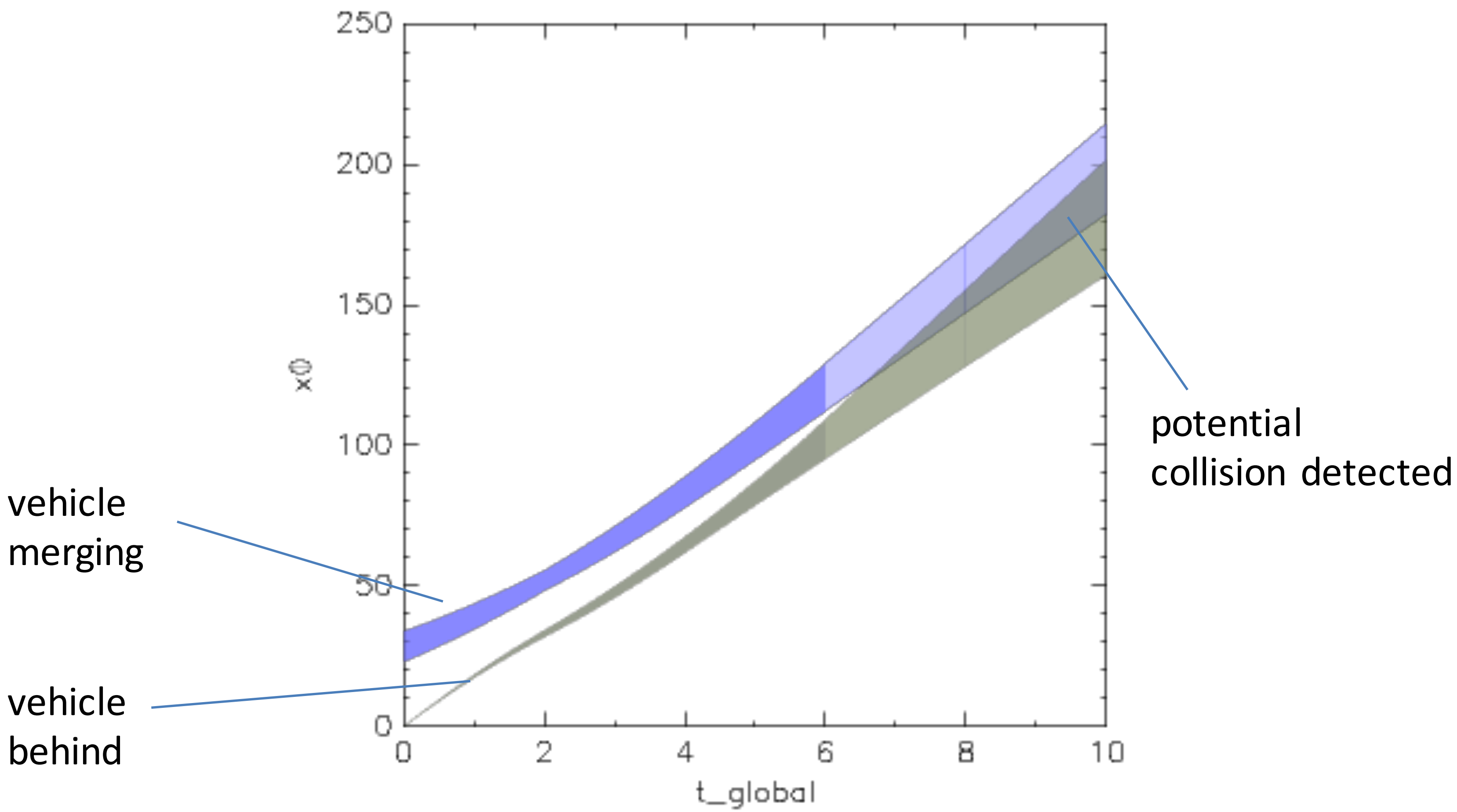


(d) Maneuver finished

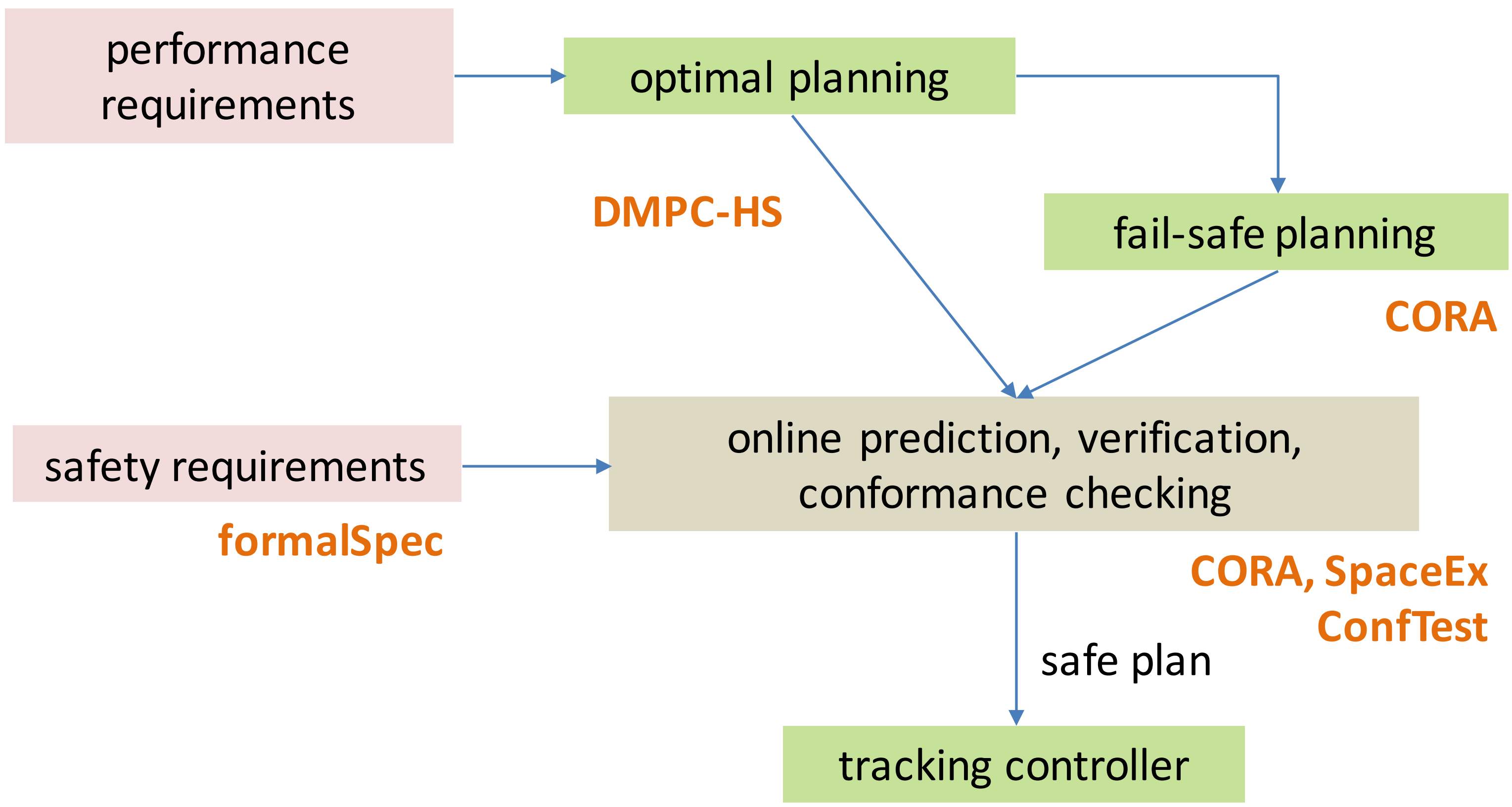
Use Case: Optimal Merging (Polimi)



Offline Verification: Use Case

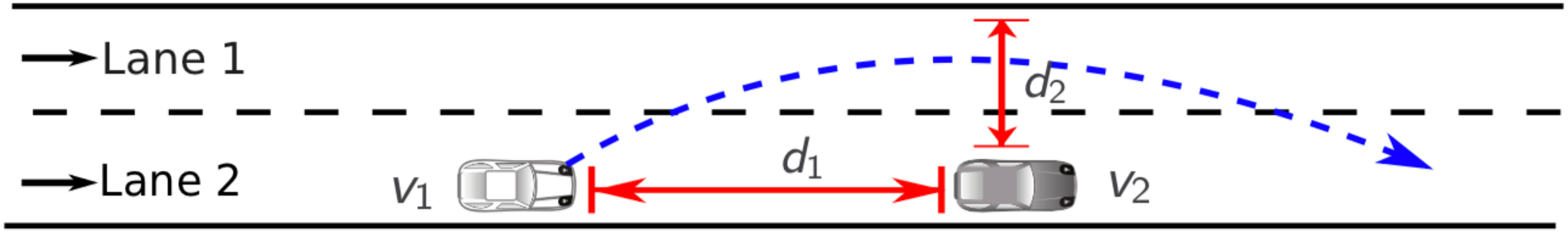


Safe Planning Architecture

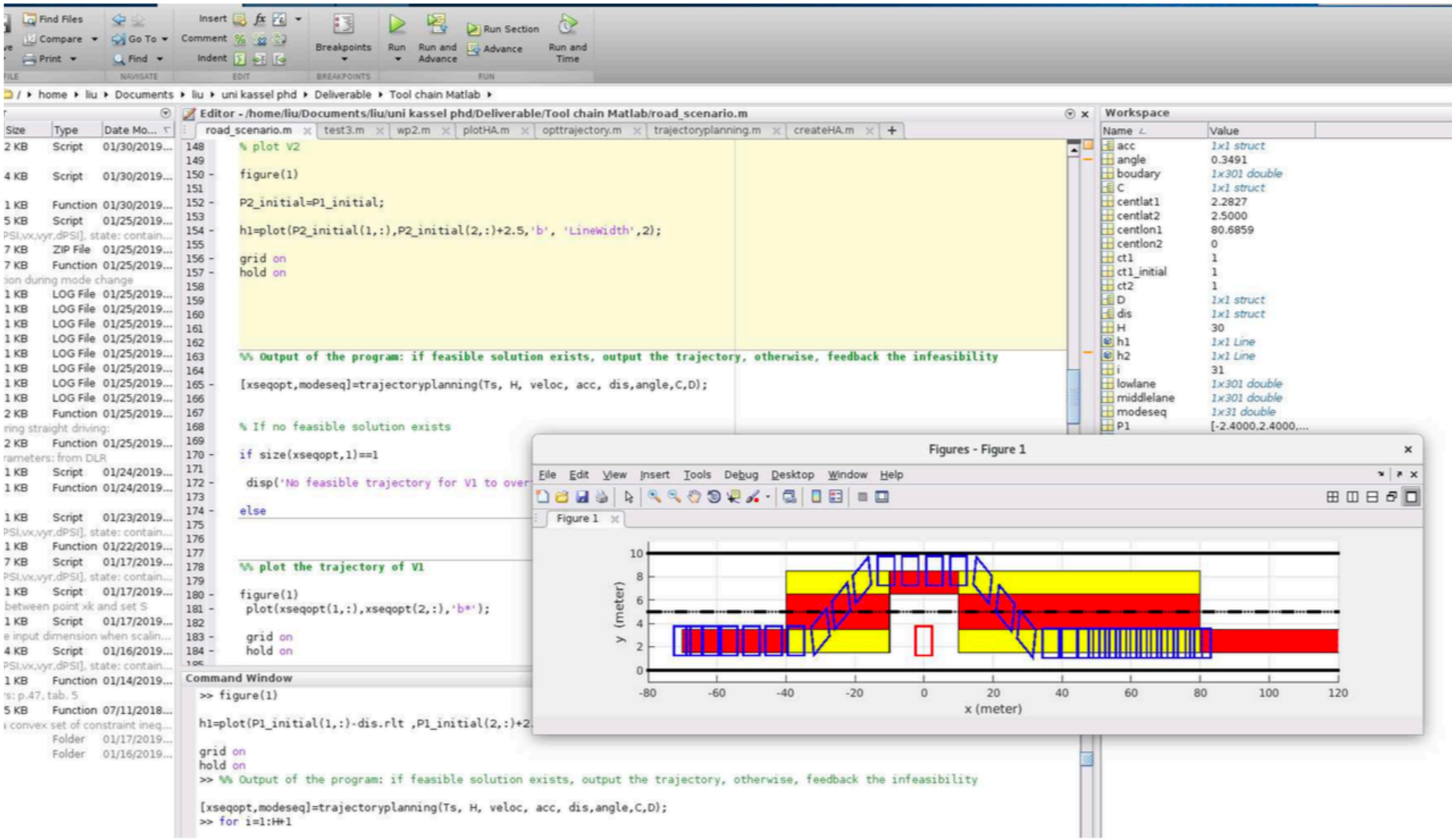


Long/Short-Term Planning: DMPC-HS

- synthesize optimal trajectory over finite time horizon
- input: nondet. model (ConfTest)
  initial and target states
- output: optimal input/state sequences
- developed by U. Kassel

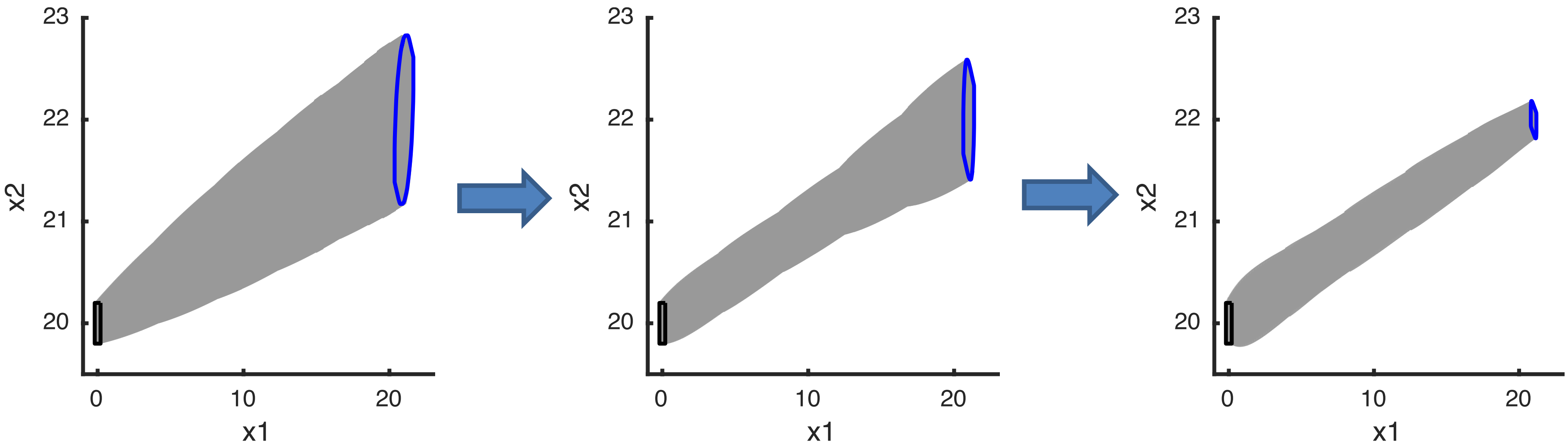


Long/Short-Term Planning: Use Case



Offline Synthesis & Verification: CORA

- Pre-computation of motion primitives by optimizing over reachable sets
- input: non-deterministic model (ConfTest), parameter range
- output: maneuver automaton
- developed by TUM



Offline Verification: CORA

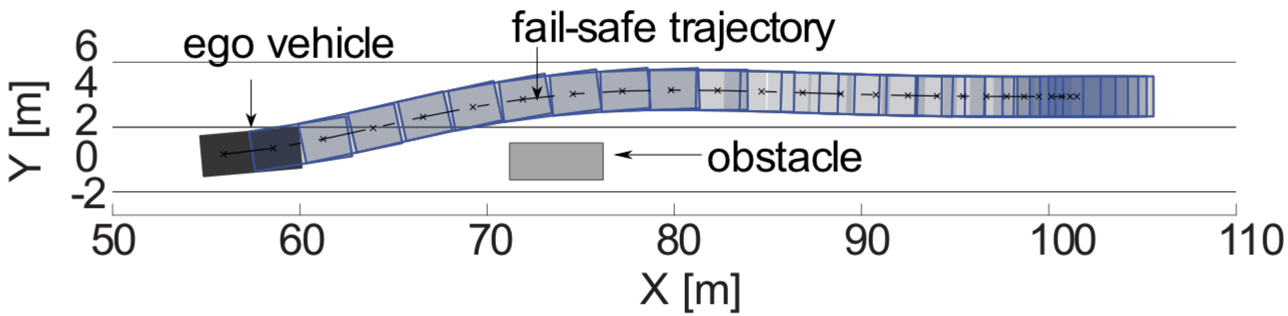
```
>> compute_motion_primitive(car_model,primitive_parameter);
```

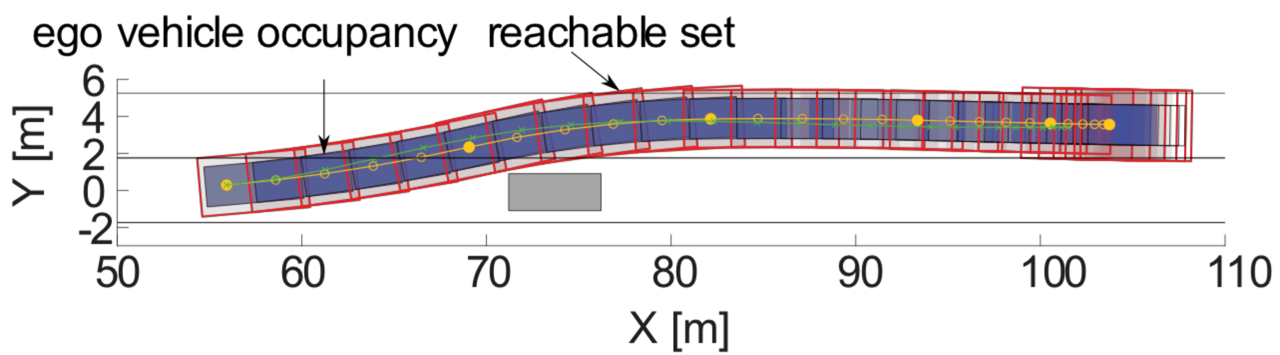
Online Verification: CORA

- Verify whether a planned trajectory can be safely executed
- input: maneuver automaton (CORA offline),
reference trajectory (DMPC-HS)
- output: safe yes/no
- developed by TUM

Online Verification: Use Case

- Online: Matching of reference trajectories to ensure drivability and safety





ScenarioMPC

- Account for stochastic uncertainty in optimal constrained control design
- input: model of the system (linear, PWA, feedback linearizable)
  constraints and control performance index
  uncertainty realizations from data or extractions
- output: controller
  probabilistic guarantees on performance
- developed by PoliMi, extended to a smart grid distributed set-up

Optimal energy management of a district

Building cooling district set-up:

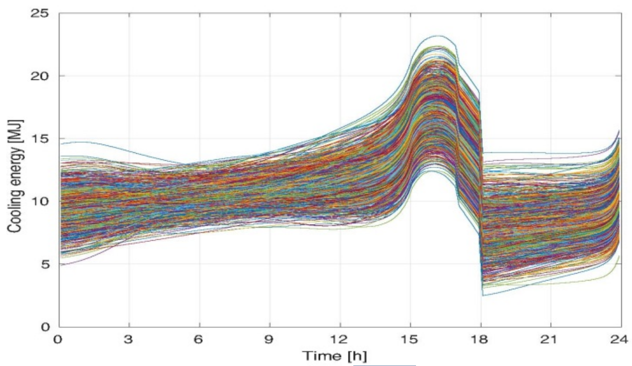
- 10 buildings, 24 hours time horizon
- a chiller per building: 5 large, 2 middle, 3 small
- a shared cooling network

Goal:

each building sets the exchange with the cooling net so as to

- satisfy its cooling load
- minimize the electrical energy consumption of its chiller over all realizations except a set of probability ≤ 0.025

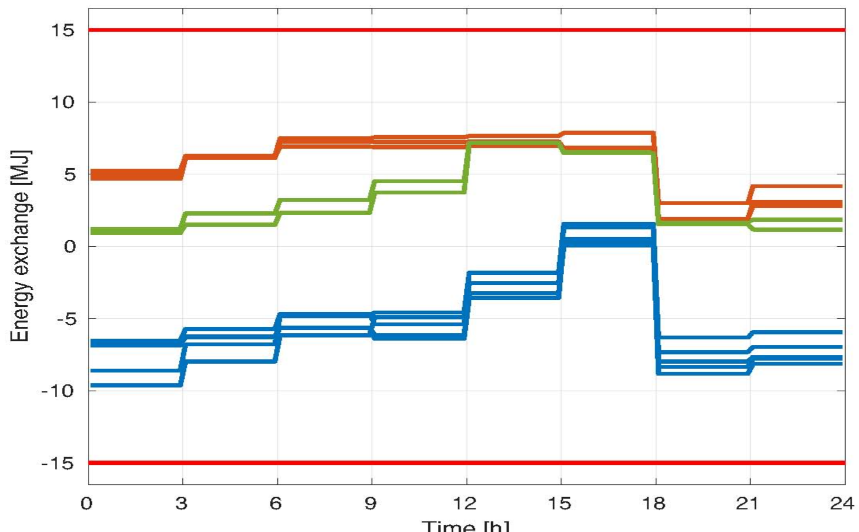
The shared net capacity couples decisions



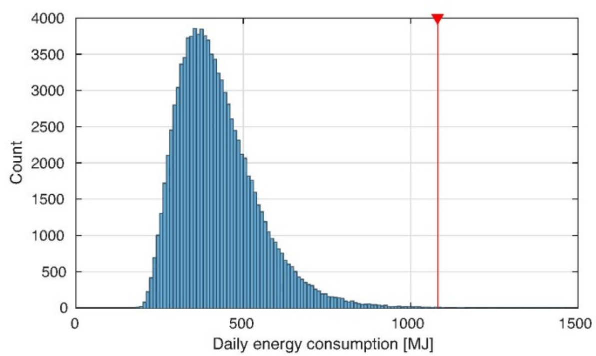
realizations of the cooling load in a building

Optimal exchange with the cooling net of all 10 buildings

- buildings with large chillers charge the net
- buildings with small chillers draw energy from the net



probabilistic performance guarantees

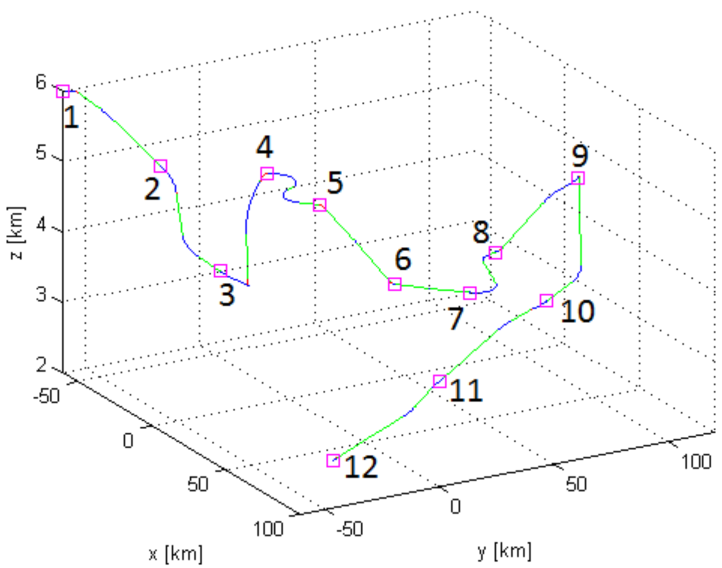


energy consumption histogram is below the red solution except for a fraction 0.9%

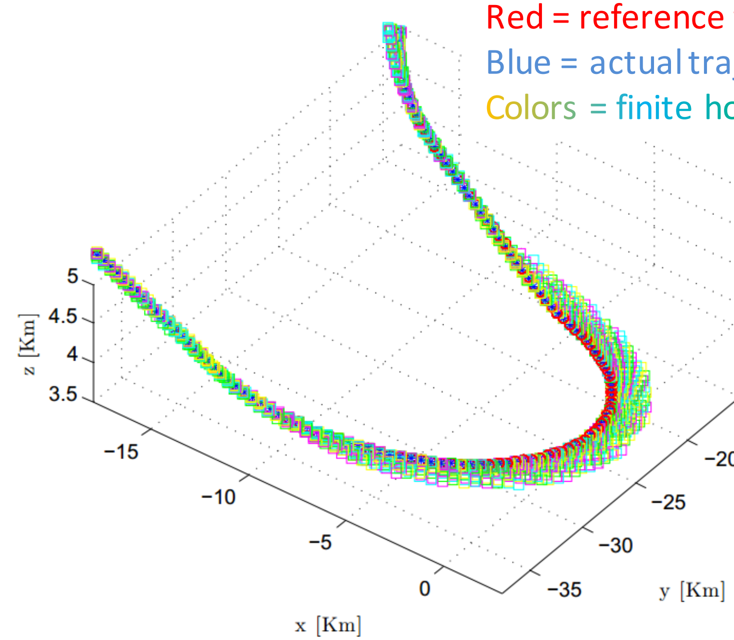
Aircraft motion control

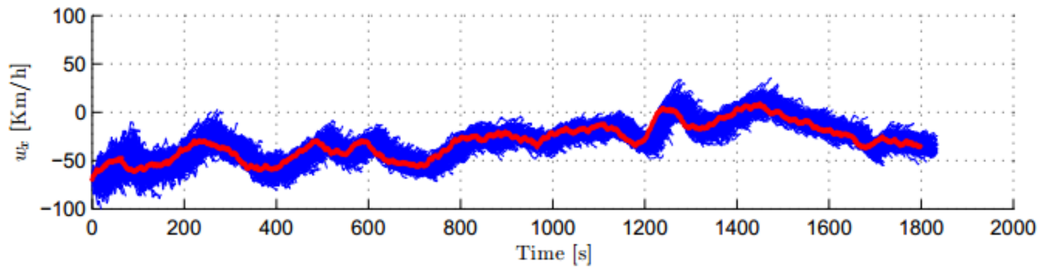
Tracking a reference trajectory via ScenarioMPC with wind compensation

Planned trajectory with target windows



Red = reference trajectory
Blue = actual trajectory
Colors = finite horizon solutions





Wind speed component x:
Red = actual wind
Blue = wind realizations from recursively identified AR processes

Conclusions

- Comprehensive toolchain for safe model-based design and **operation**
  - Specification
  - Modeling and Simulation
  - Controller Synthesis
  - Code Generation
  - Verification
  - Conformance Testing
- offline application
  - traditional MBD
- on-the-fly application
  - novel contribution of this project
- success in concrete case studies
  - automatic driving
  - human-robot-collaboration

formalSpec
SCADE-hybrid
SpaceEx
DMPC-HS
ScenarioMPC
CORA
COnfTest