Wednesday 4 July

8:30	Registration opens
9:00	**Welcome**
9:10	**Invited talk** *Lisbeth Fajstrup* Symmetries in the PV-model and of directed invariants
10:00	Break
10:20	**Invited talk** *Luc Jaulin* Distributed localization and control of underwater robots
11:10	*Hai Nguyen Van* A symbolic operational semantics for TESL
11:35	*Jérémy Dubut* Trees in partial Higher Dimensional Automata
12:00	Lunch
13:30	**Invited talk** *Emmanuel Ledinot* Towards CPS certification reformation: call for effective foundations
14:20	**Invited talk** *André Platzer* Logic of distributed hybrid systems
15:10	*Adrien Le Coënt* Guaranteed control synthesis for switched systems in Uppaal Tiga
15:35	Break
16:00	*Bernd Westphal* Code-generation for distributed real-time systems
16:25	*Paul Kröger* Reconciling hybrid-system theory with metrology
16:50	**Invited talk** *Thao Dang* Invariance and stability verification of hybrid systems
17:40	DHS ends
19:30	Informal workshop dinner *Crêperie La Belle Ronde*, 19 rue Daguerre, Paris 14

DHS 2018

Second International Workshop on

Methods and Tools for Distributed Hybrid Systems

Palaiseau, France, 4 July 2018

http://dhs.gforge.inria.fr

Program

Abstracts of invited talks

Lisbeth Fajstrup

Aalborg University, Denmark

Symmetries in the PV-model and of directed invariants

Symmetry considerations may reveal equivalences and hence possible reduction of the number of different cases to be studied for e.g. verification. The setting here is the PV-model in a geometric version, where executions are time directed paths and equivalence of executions correspond to deformation of such directed paths. In the PV-model, certainly loops provide a kind of symmetry, but the focus here is different: Copies of the same thread run in parallel with itself without control of the number N of copies gives rise to different symmetry questions and also partial results than the symmetry arising from loops, where copies of (part of) a string are run sequentially. Some results are presented in this setting - cut off for the number, N, of copies needed to ensure deadlock freedom; and also such cut offs for studying equivalence classes of executions. Another symmetry, time reversal, certainly changes some properties - for instance deadlocks become unreachable states. Other features are preserved - the execution paths from *a* to *b* correspond to execution paths from *b* to *a* under time reversal. Hence, if pairs of points are used as the basic objects, and the connections are through *(a,b)* to *(a',b')* is a pair of directed paths *a'* to *a* and *b b'* often time reversal is an equivalence. (The latter is joint work with Kathryn Hess, EPFL Lausanne.) Questions to the distributed and hybrid community may be: The space in which these directed paths run, is in most cases a cube with a set of hyper rectangles removed, and the time direction is that each coordinate to be non decreasing. How do these models and results change if e.g. paths are smooth and the time direction is defined though cones on the tangent space? if obstacles are not rectangular? if the space is a manifold?

Luc Jaulin

ENSTA Bretagne, Brest, France

Distributed localization and control of underwater robots

We consider the problem of localizing a group of underwater robots and to control the group in order to accomplish a survey. We assume here that

1. When a robot surfaces, it can use the GPS for its localization
2. The robots can communicate with a very low symbol rate
3. The robots can measure their distances with a given accuracy, but not the direction of arrival
4. Some outliers on the distances could occur, but their numbers is limited

I will propose a Lagrangian approach based on interval analysis and constraint propagation. It is based on the notion of 'tubes' which are intervals of trajectories and can easily be distributed. Some test-cases will be presented in order to illustrate the efficiency of the approach. Moreover an actual experiment involving actual underwater robots will be shown.

Thao Dang

Verimag, Grenoble, France

Invariance and stability verification of hybrid systems

Hybrid systems are widely recognized as appropriate for modelling embedded and cyber-physical systems. While reachability analysis has been used for verifying safety properties, in this work we show how reachable set computation can be used for invariance and stability properties. In particular we introduce a new set representation, called complex zonotopes, which can be seen as an extension of usual real-valued zonotopes to the complex domain and allow us to exploit eigen-structures of the dynamics in order to better capture contractive evolution. Using a number of benchmarks of hybrid systems, we also demonstrate the effectiveness of our invariance and stability algorithms.

Abstracts of invited talks

Emmanuel Ledinot

Dassault Aviation, France

Towards CPS certification reformation: call for effective foundations

Motivated by the undergoing certification reformation attempt in civil aviation, this talk will review four problems that are open from the industrial standpoint and under investigation by the hybrid system research community: contract abstraction and refinement, combinatorial structure of CPS behavioral spaces, timed-behavioral abstractions, and correctness of distributed control.

Contract-based hybrid system engineering is gaining acceptance in industry as the most promising approach to lean certification (i.e more product-oriented and safety-case oriented), and to incremental certification in particular.

Topological methods open interesting perspectives to lift structural and behavioral coverage analysis at system level. Difficult at software level where test-equivalence classes are mentioned in textbooks but hardly used in practice, behavioral coverage analysis is just inconceivable at system level, as of today in industry.

However, in addition to requirement coverage analysis which is standard through traceability, effective system behavioral coverage analysis (i.e tool-supported, scalable and qualified) would open key additional perspectives to streamline certification: it would be a pivotal enabler to depart from "the smaller, the safer" assurance principle.

This implementation minimization principle, whose soundness is not disputed here, has severe economic consequences. It conflicts with reuse of partially fit-for-purpose Components Off the Shelf (COTS). Sound timed abstraction of CPS models would be helpful for many dysfunctional combinatorial analyses, in particular for model-based safety assessment where hand-written Boolean functions or Boolean sequential processes are the industrial state of the art. Last but not least, generalized-control functions mapped on systems of systems have recently put emphasis on the need for formal verification of distributed control functions potentially disturbed by fluctuating communication delays or multi-system wide FDIR switches.

The talk will conclude on European industry-academia collaboration perspectives on these topics in the coming years.

André Platzer

Carnegie Mellon University, United States

Logic of distributed hybrid systems

This talk addresses a fundamental mismatch between the combinations of dynamics that occur in cyber-physical systems and the limited kinds of dynamics supported in analysis. Modern applications combine communication, computation, and control. They may even form dynamic distributed networks, where neither structure nor dimension stay the same while the system follows hybrid dynamics, i.e., mixed discrete and continuous dynamics. We provide the logical foundations for closing this analytic gap. We develop a formal model for distributed hybrid systems. It combines quantified differential equations with quantified assignments and dynamic dimensionality-changes. We introduce a dynamic logic for verifying distributed hybrid systems and present a proof calculus for this logic. This is the first formal verification approach for distributed hybrid systems. We prove that our calculus is a sound and complete axiomatization of the behavior of distributed hybrid systems relative to quantified differential equations. The talk will also survey the use of this logic in verifying distributed car control, robot obstacle avoidance, distributed aircraft controllers, and a surgical robot.