An Open Workshop on

Model-Based Design and Verification of Critical Systems

15/12/2016 – Sala Stringa (FBK Povo)

9:00 – 9:45

Collaborative Design for Embedded Systems - Co-modelling and Co-simulation

Speaker: Marcel Verhoef (European Space Agency)

9:45 – 10:30

Causality Checking

Speaker: Stefan Leue (University of Konstanz)

10:30 – 11:00

Coffee Break

11:00 – 11:45

Diagnosability Planning for Controllable Discrete Event Systems

Speaker: Philippe Dague (Université Paris-Sud / LRI)

Contact: Benjamin Bittner (bittner@fbk.eu)

Collaborative Design for Embedded Systems - Co-modelling and Co-simulation

Speaker: Marcel Verhoef (European Space Agency)

The talk will address the issue of cross-domain modelling of cyber-physical systems, by way of co-modelling and co-simulation, as was researched in the FP7 DESTECS project (which ran from 2010 until 2012), with follow-up in the on-going H2020 project INTO-CPS. The talk will introduce the key concepts of the approach and demonstrate its application on an aerospace challenge problem to study the early design of locomotion and safety control concepts of a Marsian rover.

Causality Checking

Speaker: Stefan Leue (University of Konstanz)

The notion of an event causing another event is essential in many areas of systems and software engineering, in particular in safety analysis, fault localization and diagnosis. The causality reasoning used during these activities is often implicit.

I will introduce into causality checking, an algorithmic method to compute ordered sequences of events causing the violation of a reachability property in system models. The approach is based on Lewis-style counterfactual reasoning and the actual cause notion proposed by Halpern and Pearl. I will extend this notion to models of concurrent computation and describe algorithmic implementations of causality checking using explicit-state as well as symbolic model checking technology. The practical applicability of this approach as implemented in the QuantUM tool will be illustrated using case studies from system safety analysis.

Diagnosability Planning for Controllable Discrete Event Systems

Speaker: Philippe Dague (Université Paris-Sud / LRI)

We propose in this talk an approach to ensure the diagnosability of a partially controllable system. Given a model of correct and faulty behaviors of a partially observable discrete event system, equipped with a set of elementary actions that do not intertwine with autonomous events, we search a diagnosability plan, i.e., a sequence of applicable actions that leads the system from an initial belief state (a set of potentially current states) to a diagnosable belief state, in which the system is then left to run freely. This helps in reducing the diagnosis interaction with running systems and can be applied, e.g., on the output of a repair plan, like in power networks. The two successive stages of this approach keep diagnosability planning, including diagnosability tests, in PSPACE in comparison to the EXPTIME test for the more complex active diagnosability used usually in such cases. For this, we propose to construct incrementally the twin plant structure of the given system and to exploit its parts already constructed while testing the candidate plans and constructing its next parts. This helps in pruning the twin plant constructions and many non-diagnosability plan tests. We have created a special benchmark and tested three proposed methods, according to the recycling level of twin plants construction, with one cost function used for plan optimality and an optional heuristics.