Contracts in Model-Based Design of Cyber-Physical Systems

"Antoine Girard" (CNRS, L2S)
Axe SciLex

Abstract

Cyber-physical systems (CPS) result from integrations of computational devices with physical processes and are to become ubiquitous in modern societies (autonomous vehicles, smart buildings, robots, etc.). The development of rigorous model based approaches to the design of CPS therefore constitutes a major challenge for the future years. Hybrid systems are natural models of CPS enabling to capture the tight interactions between ``discrete'' computing devices with the ``continuous'' physical world. Despite considerable progress in the field, current techniques apply to hybrid systems of moderate complexity. Thus, the design of complex CPS requires to divide large design problems in smaller sub-problems that can be solved using existing tools. The CODECSYS project aims at developing such approaches by decomposing a complex CPS into components which are designed independently. Each component is assigned a contract, which specifies guarantees that the component must fulfill under assumptions on the behavior of other components. For a given desired behavior of the global system, the decomposition into contracts to be satisfied by components is generally not unique: some contracts may be infeasible by components, resulting in an unsuccessful overall design; and even when all contracts can be satisfied, their choice may impact the robustness of the overall system.

The CODECSYS project will contribute to contract based design of CPS by developing novel approaches, which explore systematically the space of possible design contracts. In this talk, we will first explain our methodology using a simple example. Then, its application in embedded control systems design will be discussed. We will conclude by highlighting some of the current research directions explored within the CODECSYS project.