Abstract Thesis English

Youssef Driouich

Cyber-Physical Systems (CPSs) are integrations of computation with physical processes. Applications of CPS arguably have the potential to overshadow the 20-th century IT revolution. Nowadays, CPSs application to many sectors like Smart Grids, Transportation, and Health help us run our lives and businesses smoothly, successfully and safely.
Since malfunctions in these CPSs can have serious, expensive, sometimes fatal consequences, Simulation-based Verification (SBV) tools are vital to minimize the probability of errors occurring during the development process and beyond. Their applicability is supported by the increasingly widespread use of Model Based Design (MBD) tools. MBD enables the simulation of CPS models in order to check for their correct behaviour from the very initial design phase. The disadvantage is that SBV for complex CPSs is an extremely resources and time-consuming process, which typically requires several months of simulation. Current SBV tools are aimed at accelerating the verification process with multiple simulators working simultaneously. To this end, they compute all the scenarios in advance in such a way as to split and simulate them in parallel. Nevertheless, there are still limitations that prevent a more widespread adoption of SBV tools. To this end, we present a MBD methodology aiming the acausual modeling and verification via formal-methods, specifically the model checking techniques, the system under verification (SUV). Our approach relies basically on: Firstly, the analysis of the steady-states of the CPS and the bounding technique of the system's state in parallel with the simulation in order to identify the state space of the system simulating it only once, then represent it as a Finite State Machine (FSM). Secondly, exhaustively verify the resulted FSM using a symbolic model checker and express the desired properties in classical temporal logic. The application to a power management system is presented as a case study.