Formal verification of coupling properties for an automotive software integration across XiL

Natarajan Nagarajan*, Evren Ermis*, Andreas Thuy* and Bernd-Holger Schlingloff†

* ETAS GmbH
Borsigstraße 14, 70469 Stuttgart, Germany
e-mail: {natarajan.nagarajan, evren.ermis, andreas.thuy}@etas.com, Web page: http://www.etas.com/

† Humboldt-Universität zu Berlín
Rudower Chaussee 25, Johann von Neumann Haus, 12489 Berlin, Germany
e-mail: hs@informatik.hu-berlin.de, Web page: https://www.informatik.hu-berlin.de/en

ABSTRACT

Virtualization and desktop testing of an integrated system without inclusion of a physical hardware is a well-established concept today due to availability of abundant computing power. However, only few aspects of reality are introduced in steps into these virtual environments. The aspects of reality like hard-real time deadlines, timing events, coupling frequency and data synchronization between two subsystems in a system offer complexity without fair estimation of its consequence on the system behavior. In this paper, we describe the abovementioned complexity taking example of the coupling properties of a combustion engine along with its controller. We formally verify the timing, safety, liveness and deadlock properties of the coupling by modeling them as timed transition systems. The example is verified for idle speed control, smooth mode switching and injection cutoff control where the interaction between the subsystems is very critical. The paper highlights a very important perspective of strong and weak subsystem coupling while transiting from Model-in-the-loop simulation (MiL) to Software-in-the-Loop (SiL) and finally to Hardware-in-the-Loop (HiL). In conclusion, the input-output behavior of the coupled subsystems is also presented for a realistic observation of the control loop.