

Online-Verification of Cooperative Systems

Daniel Heß, Deutsches Zentrum für Luft- und Raumfahrt (DLR)

Control design and verification of cyber-physical systems are challenging problems, due to mixed discrete and continuous dynamics, unreliable sub-systems and complex environments. Connected, automated vehicles exemplify these properties in huge numbers of time-varying environmental variables, non-deterministic continuous dynamics, interactions with non-communicating vehicles and unreliable wireless communication with other automated vehicles. In the project UnCoVerCPS we investigate a toolchain for unification of control and verification of cyber-physical systems and apply these techniques to cooperative, automated driving. Thereby complementing classical testing with online-verification techniques. During operation of an automated vehicle, a supervisory module verifies possible actions that are proposed by high-level control processes. These actions are evaluated under the assumption of certain worst-case behaviors of other traffic participants, non-deterministic sensors and actuators, as well as past agreements with other communicating, automated vehicles. By switching between desired actions and emergency maneuvers, the supervisor guarantees invariant safety of its vehicle. Through the combination of offline and online verification steps, we can incorporate detailed models of the environment, of the vehicle and the behavior of other traffic participants. Furthermore, we make no restrictive assumptions about the control modules that propose actions to the supervisor. Thus, complex and adaptive controllers, (e.g. machine learning based techniques), can be integrated into the safety concept. We present intermediate project results, including physical test drives and real-time simulation and discuss implications and benefits of the proposed concept.