Forschungsprojekt: Towards the Verification of Safety-critical Autonomous Systems in Dynamic Environments

Daniel Arnsberger, B.Sc.

TU Clausthal

There is an increasing necessity to deploy autonomous systems in highly heterogeneous, dynamic environments, e.g. service robots in hospitals or autonomous cars on highways. Since unforeseen situations may occur in these environments, the verification results obtained with respect to the system and environment models at design-time cannot be transferred to the system behavior at runtime. For autonomous systems operating in dynamic environments, motion safety is a critical requirement. In this work, we present a two phase process in order to address the passive safety property. At the design phase, we exploit UPPAAL to formalize the autonomous system and its environment as timed automata and the safety property as TCTL formula. After verifying the correctness of these models with respect to the system’s safety requirement, we generate a monitor from these models to check whether the assumptions made at design time are also correct at run time. If the current system observations of the environment do not correspond to the initial system assumptions, then the system enters a passive safety state.