**Abstract:**

As embedded real-time systems become more and more complex and mission- or safety-critical, the traditional development process of manual coding followed by extensive and lengthy verification/testing is becoming inadequate. The model-based design utilizes the verifiable reusable components and proper architectures, to deal with the verification scalability problem caused by state-explosion. In this paper, we address verification approaches for both low-level individual component correctness and high-level system correctness, which are equally important under this scheme. Three prototype tools are developed, implementing our approaches and algorithms for verification applications accordingly.

For the component-level design-time verification, we developed a symbolic verifier, LhaVrf, for the reachability verification of concurrent linear hybrid systems (LHA). It is unique in translating a hybrid automaton into a transition system that preserves the discrete transition structure, possesses no continuous dynamics, and preserves reachability of discrete states. Afterwards, model-checking is interleaved in the counterexample fragment based specification relaxation framework.

On a run-time basis, it is critical to know whether the system under consideration will remain safe in a bounded future (reaction time). In this thesis, we present a simulation-based bounded-horizon verification framework we developed aiming for the reachability verification of systems modeled by hybrid automata (HA). This framework applies a dynamic, on-the-fly, repartition-based error propagation control method with the mild requirement of Lipschitz continuity on the continuous dynamics. The novel features allow state-triggered discrete jumps and provide eventually constant over-approximation error bound for incremental (input-to-state) stable dynamics. The above approaches are implemented in our prototype verifier called HS3V.

Once the component properties are established, the next thing is to establish the system-level properties through compositional verification. We present our work on the role and integration of quantifier elimination (QE) for property composition and verification. In our approach, we derive in a single step, the strongest system property from the given component properties for both time-independent and time-dependent scenarios. The system initial condition can also be composed, which, alongside the strongest system property, are used to verify a postulated system property through induction. The above approaches are implemented in our prototype tool called ReLIC. Additionally, we showed that certain formal verification steps can also be viewed as QE problems. Thereby, the QE tools provide options to also extend the existing verification tools. We integrated the QE tool Redlog as a back-end solver, in parallel with the existing SMT solvers, for the k-induction based model checker JKind, enhancing the capability to model check nonlinear properties of the later.