Title: **Towards theorem-grade timely execution**

Andreas Lindner

Abstract

Cyber physical systems typically describe their execution time requirements in terms of input-output response time constraints. Critical examples of such systems are car breaks, avionics, and even nuclear reactor control systems, which endanger lives in case of unspecified behavior in their implementations. To automatically and reliably determine code run-time, we implement a proof-producing symbolic execution on an intermediate language in the theorem prover HOL4. This can be used in a binary analysis framework to proof timely execution on any supported architecture. Currently and initially, we target ARM Cortex-M0 processors because their execution time is only dependent on the instruction sequence and not on the data processed or cache states. We plan to experiment with cache analysis, modeling of timer peripherals, and temporal isolation kernels in the future.