A Domain-Specific Language Approach to Hybrid CPS Modelling

The recent advent of cyber-physical systems (CPSs) in end-user applications extends the need for sophisticated model creation, simulation and system verification from classical systems engineering domains to new application areas. Since CPSs such as smart homes and office automation seamlessly integrate technology into everyday life, their safety and correctness become paramount. The intricacy of modelling these systems stems from the merging of two opposing system views: While flows of physical energy and resources are mostly described using mathematical methods such as differential equations, engineered applications are usually best expressed using automata and similar discrete formalisms. Many tools that support such hybrid models lean toward academic use, requiring extensive modelling experience, and neglect usability. Commercial platforms try to mitigate these shortcomings but involve significant financial investment. Additionally, tool creators aim to maximise their products' versatility and application areas, thereby widening the distance between software and target domain. This introduces complexity and configuration effort and increases the risk for errors not directly related to the system itself.

This thesis explores the use of domain-specific languages (DSLs) to bridge the gap between systems and models. It describes the creation of the Continuous REactive SysTems language (CREST), a DSL dedicated to the combined modelling of physical resources and engineered behaviour. The language offers architectural concepts such as hierarchical system composition and typed ports, reactive dataflow aspects that assert a synchronous model behaviour, continuous variable evolution and support for non-deterministic systems. While the language is certainly the main contribution, CREST's design considerations provide additional value to the modelling community. The findings of this project are described according to three research phases.

First, an initial analysis investigates the requirements of CPSs whose behaviour is based on the flow of resources such as heat or electricity and extracts the properties that must be provided by a modelling language or tool. These results are then used to evaluate current modelling software and formalisms.

The second part builds upon these insights to design CREST, a hybrid modelling DSL. CREST reuses well-established concepts from existing formalisms and merges them into a coherent language, whose formal semantics open the door to well-defined execution and simulation. CREST is implemented as `crestdsl`, a Python-based, internal DSL that allows efficient modelling and simulation.

The last research topic describes the application of formal verification on CREST models. This advanced use case is explored from theoretical and practical points of view. Additionally, it has been implemented in `crestdsl` proving its viability. The positive result of the approach highlights the capabilities of CREST, the practicability of the hybrid DSL modelling approach and confirms their effectiveness.

Stefan Klikovits PhD Thesis Abstract University of Geneva, 2019