Towards Modular Verification of Stabilisation in Self-Adaptive Embedded Systems*

Ina Schaefer and Arnd Poetzsch-Heffter

{inschaef|poetzsch}@informatik.uni-kl.de
Software Technology Group
Technische Universität Kaiserslautern, Germany

Abstract. We introduce a formal semantic-based modelling framework to model, specify and verify the functional and adaptive behaviour of synchronous adaptive systems.

1 Motivation

Self-adaptive embedded systems, e.g. in the automotive domain, autonomously adapt to changing environment conditions and increase their dependability by downgrading functionality in case of failures. However, adaptation in embedded systems significantly complicates system design, in particular, as adaptations trigger further adaptations in other modules potentially leading to inconsistent and unstable configurations. Hence, stabilisation of adaptation in self-adaptive systems is crucial. Formal verification as applied in safety-critical applications must therefore be able to consider not only temporal and functional properties, but also dynamic adaptation according to external and internal stimuli.

2 Modelling Synchronous Adaptive Systems

While most approaches formalizing self-adaptation [1] so far intertwine functionality and adaptation, the proposed modelling framework [3] decouples functional and adaptive behaviour providing a clear formal account of both aspects in separation. This reduces design complexity and enables explicit and uniform reasoning about functional, adaptive and combined properties. The modelling is based on state-transition systems. It describes adaptation of module behaviour in terms of an adaptation aspect on top of a set of possible predetermined configurations. Restricting adaptation to predetermined reconfiguration makes systems predictable and improves analysis results. Figure 1 depicts the intuitive notion of a module. The configurations specify local state transitions and computation of output. Before executing the actual functionality, the adaptation aspect evaluates the configuration guards and selects an applicable configuration. Furthermore, it computes adaptation signals for other system modules.

* Supported by the Rheinland-Pfalz Cluster of Excellence 'Dependable Adaptive Systems and Mathematical Modelling' (DASMOD)

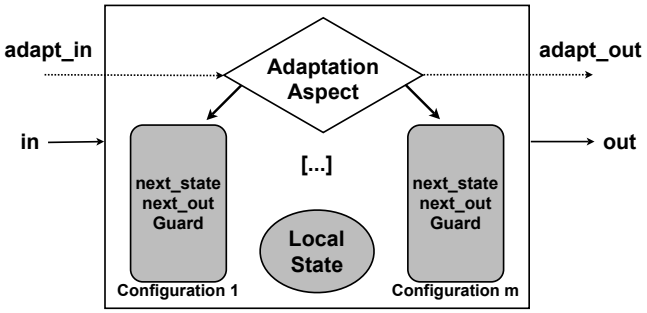

Fig. 1. Separating Functionality and Adaptation in a Module

Synchronous adaptive systems are composed from a set of modules connected via links between input and output variables where data and adaptation flow do not follow the same links. Adaptations in one module may trigger adaptations in other modules by propagation of adaptation signals. The systems are open systems with a non-deterministic environment and operate synchronously as simultaneously invoked actions are executed in true concurrency.

3 Verifying Stabilisation of Adaptation

For specification purposes, we adopt a variant of the linear time logic LTL by adding special basic predicates for functional and adaptive behaviour to standard first-order and temporal connectives. Stabilisation of adaptation with respect to a property φ is defined along the lines of [2]. It can be re-phrased in linear logic as $\mathbf{G}\ (\psi \rightarrow \mathbf{F}\,\mathbf{G}\,\varphi)$ where ψ is a formula which first becomes true in a state in which the adaptation occurs. The proposed framework enables modular reasoning exploiting the system's modular specification. A global system property can be decomposed into local properties of single modules entailing the global property. Furthermore, incorporating abstraction mechanisms, for instance to reduce unbounded data domains to finite discrete domains, facilitates the efficient integration of existing model checking techniques into the verification of self-adaptive systems for discharging certain sub-proof goals automatically.

References

1. J.S. Bradbury, J.R. Cordy, J. Dingel, and M. Wermelinger. A Survey of Self-Management in Dynamic Software Architecture Specifications. In *Proc. of Intl. Workshop on Self-Managed Systems (WOSS'04)*, 2004.
2. E.W. Dijkstra. Self-Stabilizing Systems in spite of Distributed Control. *Communications of the ACM 17(11)*, pages 643–644, 1974.
3. I. Schaefer and A. Poetzsch-Heffter. Using Abstraction in Modular Verification of Synchronous Adaptive Systems. In *Proc. of "Workshop on Trustworthy Software", Saarbrücken, Germany, May 18-19*, 2006.