Second Year Report for Project:
A tool environment for the development of embedded systems
Project no: A6-9805

Anders Wall, Christer Norström, and Wang Yi
Department of Computer Engineering
Mälardalen University
010528

1 Second year report

1.1 Original project plan

In this project, we will concentrate on questions related to code-generation, e.g. how to extend abstract models with real-time tasks, how to analyse such extended models for a given run-time scheduler by verification and schedulability analysis and how to transform such model to executable code. Main activities will be in development and integration of techniques in related areas such as compiler construction, formal verification, scheduling theories, timing analysis, and real-time operating system design. The following problems will be of particular interests in this project:

1. How to incorporate timed automata with a notion of real-time tasks, or how a timed automaton model is related to the traditional task model of a real-time system.
2. How to combine verification with schedulability analysis techniques to analyse event-driven systems modelled as extended timed automata with real-time tasks.
3. How to generate a runnable program from an extended timed automaton with tasks, and how timing analysis is incorporated in code generation.
4. How to generate a set of tests for a given timed automaton extended with tasks, to cover the behaviour of the runnable program generated from the extended automaton.

1.2 Deviations from the original plan

Item 3 was studied but no papers were written. Item 4 was never studied, instead a lot of effort was spent on combining formal methods and software architecture description and analysis.

A major deviation was that the licentiate thesis was presented almost one year ahead to plan!

1.3 Main achievements

A formal approach to software architectural analysis is proposed. A software architecture is a high-level design description of a software system. In terms of the architecture, early design decisions can be analysed to improve the quality of a real time software system, which depends very much on how it is structured rather than how it is implemented. Architectural analysis techniques vary in their degree of formality. The least formal is based on reviews and scenarios, whereas the most formal analysis methods are based on mathematics. We showed how to use networks of timed automata to model the architecture of real time systems and how to transform architectural analysis problems to reachability problems that can be checked by existing tools for timed automata. Typical properties that can be handled using this approach are schedulability and safety properties.

The first technical contribution, the classic model of timed automata was extended with a notion of real time tasks. This yields a general model for real-time systems in which tasks may be periodic and non-periodic. We show that the schedulability problem for the extended model can be transformed to a reachability problem for standard timed automata, and thus it can be checked by existing model-checking tools, e.g. UPPAAL for timed automata.

The second technical contribution is a method to check general high level temporal requirements e.g. timing constraints on data flowing in multi-rate transactions, which can not be handled by traditional approach to schedulability analysis. An algorithm was developed that given a data dependency model and a schedule for a transaction constructs a timed automaton describing the behaviour of the transaction. Thus, by using existing verification tools we can verify that a given architecture is schedulable and more importantly, it is correctly constructed with respect to the high level temporal constraints.

The main academic impact is the first technical contribution where timed automata were used to model a hybrid system. The industrial impact is mainly the basic reasoning in architecture description and analysis to establish design of real-time systems as an engineering discipline.

1.4 Results (publications)

1.4.1 Conferences

Anders Wall, Kristian Sandström, Jukka Mäki-Turja, Christer Norström, Wang Yi: Verifying Temporal Constraints on Data in Multi-Rate Transactions, proceedings of RTCSA 2000, Korea, IEEE Computer Society, December 2000.

Christer Norström, Anders Wall, Wang Yi: Timed Automata as Task Models for Event-Driven Systems, In proceedings of RTCSA'99, Hong Kong, IEEE Computer Society, December 1999.

1.4.2 Thesis

Anders Wall: A Formal Approach to Analysis of Software Architectures for Real-Time Systems, Licentiate Thesis, Dept. of Computer Systems, Uppsala University and Dept. of Computer Engineering, Mälardalen University, September 2000.

1.4.3 Technical reports

Anders Wall: Software Architectures for Real-Time systems, Technical Report 00/20, May 2000.

Henrik Thane, Anders Wall: Formal and Probabilistic Arguments for Reuse and Reverification of Components in Safety-Critical Real-Time Systems, Technical Report , January 2000.

Anders Wall: Software Architectures -An overview-, Technical Report , October 1999.

1.5 Appendix

A statement from the associated industries, Mikael Strömberg at Systemite AB: