An Application for Extending the ARTES Project:

A Tool Environment for The Development of Embedded Systems

Wang Yi
Uppsala University

Contents

1 Summary

This document is to apply for support to extend the existing ARTES project: A Tool Environment for The Development of Embedded Systems with two positions for Ph.D. projects: (1) *An Object-Oriented Language for Hierarchical Modelling and Analysis* and (2) *Test Generation: From Requirement Specifications to Executable Tests*. The original project proposal is concerning extending the Uppaal tool to cover the whole development process of embedded systems. We quote the summary of the original proposal:

> Uppaal is a tool for modelling, validation and verification of real-time systems, developed jointly by Uppsala University and Aalborg University. A Uppaal case study has been considered as one of the primary examples, in the ACM survey [2] by Ed Clarke et al on state of the art of formal methods. In recent years, it has been applied in a number of industrial case studies [1, 4, 3, 5]. However, the main application area of Uppaal has been in modelling and verification. Our vision is to further develop Uppaal to provide an integrated tool environment for the formal development of embedded real-time systems in collaboration with Uppsala University, supporting each step of the development process, from *design, simulation, verification, runnable code generation, to test generation*. This project will be one of the main activities in this joint effort. In particular, we plan to develop a code generator which transforms abstract designs written in the Uppaal description language (extended with a notion of real-time task), to executable code.

2 Background

In May, 1998, we proposed a project to ARTES: *A Tool Environment for the Development of Embedded Real Time Systems*. The project is to establish a joint effort on *tool-based system development environment* for real-time embedded systems, between Uppsala University, and Mälardalen University with Mecel AB, ABB Industrial systems AB and Volvo Technological Development Corporation being industrial partners.

The goal is to further develop the UPPAAL tool to a *coherent tool environment* for the development of embedded real-time systems, which supports each step of the system development process, from *specification, design, simulation, verification, runnable code generation, to test generation*. The vision is to *relate and unify "real–time" research results within ARTES in one framework*. This kind of projects was considered particularly important for a research network like ARTES[1].

In our first proposal (1998 May) to ARTES, we asked explicitly for funding only *one Ph.D. student* to work on *code–generation* at Mälardalen University to asset the feasibility of the project. Considering the suggestions from the ARTES advisory

[1] The project was presented at the ARTES sommer school, 1998 August in Stockholm.

board, responses to the project at the ARTES sommer school, and the current size of the project (one student), we believe that we have a strong case for extending the project.

3 Ph.D. Projects

Hierarchical Design and Analysis

Currently, the tool UPPAAL provides no support for modelling hierarchical structures, not to mention hierarchical analysis. The user can describe only a network of automata in the very flat form, which restricts the size of problems that UPPAAL can deal with. Recently we started a joint case-study project with ABB Industrial Products to model and verify a bus protocol (AF 100) developed by ABB Industrial Systems AB, which is a commercial product. It is our experience with model-checkers like UPPAAL that a large part of the total time in most of the case studies is spent on constructing the system model, i.e., modeling. This has lead to a strong demand for a modelling language as well as a graphical user interface, with features supporting abstractions, such as hierarchical descriptions of models. There have been several modelling languages e.g. State-Chart for Statemate, developed particularly for modelling and simulation. However, rather little work has been done on static analysis for such languages to provide static information, e.g. types, hierarchical structures etc to guide verification.

We plan to develop an object–oriented modelling language as well as a graphical user interface for the tool UPPAAL. With some limited short–term (6 months) grant from other funding sources (NUTEK and TFR), we have implemented the first prototype of such a language (named UL^{++}: http://www.docs.uu.se/rtmv/ul).

We hope that ARTES will support the continuation of this project, to finalize the implementation of UL^{++} in Java and integrate it with the Uppaal tool. Hopefully, in the short future, it will replace the current UPPAAL description language and user interface based on Autograph. We should point out that the UL^{++} project is naturally related to the existing *code-generation* project supported by ARTES as both address language design issues and more importantly the code-generation project is to generate runnable codes from design specifications written in UL^{++}.

The future plan with UL^{++}–project is to develop verification techniques that utilize the hierarchical information in order to guide the state–space exploration algorithm that the UPPAAL engine is based on and to introduce *abstraction* in the UPPAAL simulator and diagnostic trace–generator.

Test Generation

Testing real-time properties for embedded systems is an area where few general techniques are available. In industry, most of the techniques are ad hoc and product–oriented. There have been work on testing sequential pograms, addressed in the area of software engineering and conformance testing in the area of telecommunication, but little work on real time testing.

In addition to the difficulties in testing sequential programs such as input coverage, testing embedded real time systems must also deal with following aspects:

1. **Environment Simulation**: due to the fact that many applications are safety critical, the testing machinery for embedded systems can not be put in the target environment. Testing must be carried with a simulated model of the physical environment, which simulates the reasonable inputs, and in addition can be directed to play critical scenarios. The creation of such simulation environments is non-trivial when the environment is a complicated physical process. A related problem is to supply representative inputs.

2. **Real–Time Behaviours**: to test real-time properties, test cases must cover not only all the sequences of significant events, but also significant time points. It is a non–trivial task to cover all time points in particular working in a dense time model. One needs to find all the critical time points to represent time zones instead of points as in the case of real time model checking.

3. **Non-determinism**: for a given input, the behavior of the system may still not be predictable, especially for event-driven systems. In order to be able to replay a test execution, the testing machinery may record the sequence of significant events, sufficient to regenerate the execution.

A survey on problems and possible solutions on testing real time systems can be found in

[Sch95] *W. Schüutz. Testing distributed real-time systems: An overview. In Randel l, Laprie, Kopetz, and Littlewood, editors, Predictably Dependable Computing Systems, pages 283-298. Springer Verlag, 1995.*

[RNHW98] *P. Raymond, X. Nicollin, N. Halbwachs, and D. Weber. Automatic testing of reactive systems. In RTSS98, 1998.*

In this project, we will concentrate on *test generation*. It will be a joint project with Volvo technological development Corporation which is involved in testing control systems for cars. The company (Volvo) has built up a testing environment simulating physical components of cars, such as motor etc. In particular, we will study the following issues:

1. **Test Description Language**: To describe abstract tests which may be transformed to executable test–sequences to run together with the software/hardware components to be tested in the testing environment at Volvo.

2. **Testing Requirment Specificaitons**: To generate abstract tests (and then to executable test–sequences) from logical specifications (requirement specifications) to justify that the target implementation satisfies the original requirements.

4 Work Plan

Research Environment

The following ARTES nodes will participate in the project:

1. Uppsala University
2. Mälardalen University
3. Mecel AB in Göteborg (Mikeal Strömberg, Tel: 031 703 3200) and
4. Volvo Technological Development Corporation (Ola Lundqvist, Tel: 031 772 4407)

Complementary Activities

There have been several related activities in Uppsala and Mälardalen within the proposed project, notably the following projects:

1. Code-Generation: From High-Level Design Model to Executable Code (at Mälardalen, supported by ARTES)
2. The UPPAAL Model Checker (i.e. the UPPAAL project) (at Uppsala, supported by NUTEK)

Work Plan and Budget

We apply for funding to support 2 Ph.D. students (the Budget should be calculated according to the ARTES standard) at Uppsala University to work on (as thesis projects):

1. UL^{++}: An Object-Oriented Language for Hierarchical Design and Analysis. Currently, we have an excellent student (Alexander David) working on the project. A prototype of UL^{++} is already available, presented in Alexander's M.Sc thesis. During the next academic year, we plan to study a field bus protocol AF100 (a commercial product) developed by ABB to obtain feedback on the design of UL^{++}. In two years from now, a licentiate thesis based on the development of UL^{++} should be finished.

2. Test-Generation: From Requirement Specification to Executable Tests. This project is planned to start in the beginning of 1999. A visiting researcher working on real time testing from Twente University, Holland is currently visiting our group. A joint work on timed testing is in progress, which is to compile *determinizable* models in UPPAAL to tests. We plan to have a new Ph.D. student to join the project in the beginning of 1999 in collaboration with Volvo.

Industrial Cooperation

The success of the UPPAAL project have generated a number of industrial interests. However, we will conduct the project mainly in collaboration with ABB Industrial Products (on the verification of AF100 protocol), Mecel AB and Volvo Technological Development Corporation.

1. ABB Industrial Products AB (Ulf Hammar, Tel: 021 34 3059)

2. Mecel AB in Göteborg (Mikeal Strömberg, Tel: 031 703 3200) and

3. Volvo Technological Development Corporation (Ola Lundqvist, Tel: 031 772 4407)

References

[1] Johan Bengtsson, David Griffioen, Kåre Kristoffersen, Kim G. Larsen, Fredrik Larsson, Paul Pettersson, and Wang Yi. Verification of an Audio Protocol with Bus Collision Using Uppaal. In Rajeev Alur and Thomas A. Henzinger, editors, *Proc. of 9*th *Int. Conf. on Computer Aided Verification*, number 1102 in Lecture Notes in Computer Science, pages 244–256. Springer–Verlag, July 1996.

[2] E.M. Clarke and J.M. Wing. Formal methods: State of the art and future directions. *Computing Surveys*, 28(4):626–643, Dec. 1996.

[3] Klaus Havelund, Arne Skou, Kim G. Larsen, and Kristian Lund. Formal Modeling and Analysis of an Audio/Video Protocol: An Industrial Case Study Using Uppaal. In *Proc. of the 18*th *IEEE Real-Time Systems Symposium*, December 1997.

[4] Kim G. Larsen, Paul Pettersson, and Wang Yi. Uppaal in a Nutshell. *International Journal on Software Tools for Technology Transfer*, 1997.

[5] Magnus Lindahl, Paul Pettersson, and Wang Yi. Formal Design and Analysis of a Gear-Box Controller. In *Proc. of the 4*th *Workshop on Tools and Algorithms for the Construction and Analysis of Systems*, Lecture Notes in Computer Science, March 1998.

5 Appendix A: Short CV for Wang Yi

Personal data

Birthday: July 1, 1961.
Civil status: Married with one son born 1997.
Nationality: Swedish.
Post address: Box 325, 751 05 Uppsala, Sweden
Tel: +46 18 4713110, Fax: +46 18 550225, Email: yi@docs.uu.se

Academic Degrees

Docent in Computer Systems, Uppsala University, Sweden, 1995.
Tekn. Dr. in Computer Science, Chalmers University of Technology, Sweden, 1991.
Tekn. Lic. in Computer Science, Chalmers University of Technology, Sweden, 1988.
B.Sc. in Computer Science, North-Eastern University of Technology, China, 1982.

Employment History

1998 - Researcher/Adjunct professor (20%), Mälardalen University.
1995 - Associate Professor in Computer Systems, Uppsala University.
1994 - 1995 Assistant Professor in Computer Systems, Uppsala University.
1992 - 1994 Lecturer/Researcher, Uppsala University.
1991 - 1992 Research Fellow, Aalborg University, Denmark.
1985 - 1991 Ph.D student, Chalmers University of Technology.
1988 Oct - 1989 Mar, System Engineer, Volvo Data, Göteborg.

Research Activities and Achievements

My research interests and activities have been focused on formal design techniques and their application to the design and analysis of real-time and distributed systems, in particular, real–time systems.

I have published about 30 papers (refereed) in international journals, conferences and workshops, and held a series of grants (totally over 9 milions Swedish kronors since 1992) for research projects in the area of modelling and verification of real time systems. Currently I am leading two national projects on formal methods for real-time systems, and have been supervising a dozen Post doc, Ph.D. and M.Sc students in the area. I am also the director of graduate studies at the department of computer systems of Uppsala University.

My main scientific contributions include:

- UPPAAL, one of the leading tools for the formal development of real-time systems. I initiated the UPPAAL project in 1993 and am still one of its main developers.
- Timed CCS, one of the first formal models published in the literature for real-time systems. I developed timed CCS (A Calculus of Real–Time Systems) in my Ph.D. thesis.

Publications (Selected)

Book Contribution

1. *Probabilistic Extensions in Process Algebra.* Bengt Jonsson, Kim Larsen and Wang Yi. Invited Chapter in the Handbook of Process Algebra. To appear in 1999. Elsevier.

Journals

2. Uppaal *in a Nutshell.* Kim G. Larsen, Paul Pettersson and Wang Yi. In International Journal of Software Tools for Technology Transfer 1(1/2). 1997.
3. *Time Abstracted Bisimulation: Implicit Specification and Decidability.* Kim Larsen and Wang Yi. In the International Journal: Information and Computation, pages 75-103, Vol 134, 1997.
4. *Schedulability Analysis of Event–Driven Tasks.* Wang Yi. Presented at 10th Nordic Workshop on Programming Theory, Turku, Finland. Oct. 1998. Selected as Best Contributions for Publication in a special issue of the Nordic Journal of Computing, 1999.
5. *Clock Difference Diagrams.* Kim G. Larsen, Carsten Weise, Wang Yi and Justin Pearson. Presented at 10th Nordic Workshop on Programming Theory, Turku, Finland, Oct. 1998 (available as a DoCS technical report 98/99). Selected as Best Contributions for Publication in a special issue of the Nordic Journal of Computing, 1999.
6. *Formal Design and Analysis of a Gear Controller.* Magnus Lindahl, Paul Pettersson and Wang Yi. In Proceedings of the 4th International Workshop on Tools and Algorithms for the Construction and Analysis of Systems. Gulbenkian Foundation, Lisbon, Portugal. 1998. LNCS 1384. Selected for Publication In the Springer International Journal of Software Tools for Technology Transfer. 1998.

Conferences

7. *Partial Order Reductions for Timed Systems.* ohan Bengtsson, Bengt Jonsson, Johan Lilius and Wang Yi. In the proceedings of CONCUR98. Nice, France. September, 1998.
8. *Efficient Verification of Real-Time Systems: Compact Data Structure and State-Space Reduction.* Kim G. Larsen, Fredrik Larsson, Paul Pettersson and Wang Yi. In Proceedings of the 18th IEEE Real-Time Systems Symposium, pages 14-24. San Francisco, California, USA. 1997. IEEE RTSS'97.
9. Uppaal*: Status & Developments.* Kim G. Larsen, Paul Pettersson and Wang Yi. In Proceedings of the 9th International Conference on Computer-Aided Verification. Haifa, Israel, 1997. LNCS 1254. 1997.
10. *Compositional Proof of a Real-Time Mutual Exclusion Protocol.* Kere J. Kristoffersen, Francois Larroussinie, Kim G. Larsen, Paul Pettersson and Wang Yi. In Proceedings of (TAPSOFT'97) the 7th International Joint Conference on the Theory and Practice of Software Development, Lille, France. 1997. LNCS 1214.
11. *Verification of an Audio Protocol with Bus Collision Using* Uppaal. Johan Bengtsson, David Griffioen, Kere Kristoffersen, Kim G. Larsen, Fredrik Larsson, Paul Pettersson and Wang Yi. n Proceedings of the 8th International Conference on Computer-Aided Verification. New Brunswick, New Jersey, USA. 1996. LNCS 1102.

12. *Compositional Testing Preorders for Non-deterministic and Probabilistic Processes.* Bengt Jonsson and Wang Yi. In the proceedings of the 10th Annual IEEE Symposium on Logic in Computer Science, San Diego, California, USA, 1995. IEEE LICS'95.

13. *Compositional and Symbolic Model–Checking of Real–Time Systems.* Kim Larsen, Paul Pettersson and Wang Yi. In the proceedings of the 16th Annual IEEE Symposium on Real–Time Systems, Italy, 1995. IEEE RTSS'95.

14. *Model–Checking of Real–Time Systems.* Kim Larsen, Paul Pettersson and Wang Yi. In Proceedings of FCT95 (Fundamentals of Computation Theory), Dresden, Germany. 22-25 August 1995. LNCS 965.

15. Uppaal - *A Tool Suite for Automatic Verification of Real-Time Systems.* Johan Bengtsson, Kim G. Larsen, Fredrik Larsson, Paul Pettersson, Wang Yi. In the proceedings of the 4th DIMACS Workshop on Verification and Control of Hybrid Systems, New Brunswick, New Jersey, 22-24 October, 1995. LNCS 1066.

16. *Diagnostic Model–Checking of Real–Time Systems.* Kim Larsen, Paul Pettersson and Wang Yi. In the proceedings of the 4th DIMACS Workshop on Verification and Control of Hybrid Systems, New Brunswick, New Jersey, 22-24 October, 1995. LNCS 1066.

17. *Decidability of Timed Language–Inclusion for Networks of Real–Time Communicating Sequential Processes.* Wang Yi and Bengt Jonsson. In the proceedings of the the 14th Conference on Foundations of Software Technology and Theoretical Computer Science, Madras, India, 1994. LNCS 880.

18. *Automatic Verification of Real–Time Communicating Systems By Constraint–Solving.* Wang Yi, Paul Pettersson and Mats Daniels. In the proceedings of FORTE94 (the 7th International Conference on Formal Description Techniques), Berne, Switzerland. 1994. North Holland.

19. *Reasoning about Uncertain Information Compositionally.* Wang Yi. In the proceedings of FTRTFT94 (the 3rd International School and Symposium on Real–Time and Fault–Tolerant Systems), Kiel, Germany. 1994. LNCS 863.

20. *Testing and Refinements of Probabilistic and Nondeterministic Processes.* Bengt Jonsson, Chris Ho Stuart and Wang Yi. In the proceedings of FTRTFT94 (the 3rd International School and Symposium on Real–Time and Fault–Tolerant Systems), Kiel, Germany, 1994. LNCS 863.

21. *Testing Probabilistic and Nondeterministic Processes.* Wang Yi and Kim Larsen. In the proceedings of PSTV92 (the 12th IFIP International Symposium on Protocol Specification, Testing and Verification), Florida, USA, 1992. North Holland.

22. *CCS + Time = an Interleaving Model for Real Time Systems.* Wang Yi. In the Proceedings of ICALP91 (the 18th International Colloquium on Automata, Language and Programming), Madrid, 1991. LNCS 510.

23. *Deciding Properties of Regular Timed Processes.* Uno Holmer, Kim Larsen and Wang Yi. In the Proceedings of CAV'91 (Computer Aided Verification), Aalborg, Denmark, 1991. LNCS 575.

24. *Real Time Behaviour of Asynchronous Agents.* Wang Yi. In the Proceedings of CONCUR90 (International Conference on Concurrency Theory), Amsterdam, 1990. LNCS 458.

6 Appendix B: Support Letters from Volvo and Mecel

Volvo participation in the ARTES project:

A Tool Environment for The Development of Embedded Systems

Ola Lundkvist
Electronic Systems / Electronics and Electrotechnology
Volvo Technological Development Corporation

System development in the automotive industry is very much characterized by the fact that a lot of components are developed and manufactured by subcontractors. For the car manufacturer some of the major development activities thus is system specification and system integration and testing. For us it is important to be able to test that components delivered by a subcontractor fulfils our requirements. For efficient testing, automation and tool support is of essence. We believe that an extended tool-set based on UPPAAL, in particular, supporting the testing process is a promising tool for our needs.

How to test embedded vehicle electronics, i.e. reactive real-time systems, is not obvious. We need to gain knowledge about how to specify and what information is needed to be able to test efficiently. How to describe test cases and how to produce a set of test cases that provides good exercise for the system under test and still is of manageable size are other challenges. These are some of the issues that we want to discuss continuously during this project.

In our opinion, it is important to consider the complete testing procedure, from specification all the way to test execution and evaluation. To achieve this we will provide information needed for a realistic case study and for connecting the test generation tool with a real test system that executes the tests. This should significantly improve the impact of the evaluation of the tool and aid researchers, tool developers and tool users to find criteria a tool need to fulfil.

A Supporting Letter for the ARTES project: A Tool Environment for the Development of Embedded Systems

Mecel is a well acknowledged engineering company in the automotive industry. Our focus is on key areas such as engine management and control by means of Ion Sense as well as Multiplexed Vehicle Electronics for vehicle network communication and Mobile Multimedia.

In collaboration with Uppsala University, we have successfully applied the tool UPPAAL in a case study (for research purpose) in 1997 to develop a prototype gear box controller. It turned out that UPPAAL is a very useful tool for the design and analysis of embedded systems.

To keep our market leading position, it is of vital importance for us to corporate with academia. We want to follow and participate research activities in the further development of this type of software tools like UPPAAL, based on formal methods. In particular we are interested in research proposed in this project, i.e. generating executable code from high-level designs and specifications based on well-developed program libraries provided for different operating systems, and also test generations according to requirement specifications.

We at Mecel, have developed the concepts of BASEMENT for the development of control systems embedded in modern vehicles. We believe that research activities and results of the proposed ARTES project will be invaluable to the future development of BASEMENT. Therefore, we want to participate in research activities in this project as an industrial partner.

Mikael Strömberg
Program Manager