ARTIST 2

Network of Excellence

IST-004527 ARTIST2:
Embedded Systems Design

Activity Progress Report for Year 2

JPIA-Platform

Testing and Verification Platform for Embedded Systems

Clusters:

Testing and Verification

Activity Leader:

Professor Kim Guldstrand Larsen (Aalborg University)
http://www.cs.aau.dk/~kgl

Policy Objective (abstract)

Construction of powerful analysis tools by establishing a joint server platform providing extraordinary computational resources for conducting large-scale verification and testing efforts for embedded systems with respect to real-time requirements, quality-of-service guarantees as well as security properties.

The platform will provide a uniform, open and secure access and to all testing and verification tools of the academic as well as industrial partners of the consortium. The platform builds on existing works from the various partners and will also make available new powerful analysis tools developed within the network, in particular those from the related Joint Research Activities ("Quantitative Testing and Verification" and "Verification of Security Properties").

Table of Contents

1. Overview of the Activity

1.1 ARTIST2 Participants: Expertise and Roles

Team Leader: Ed Brinksma (University of Twente)
verification and testing of reactive and stochastic systems.

Team Leader: Pierre Wolper (Centre Fédéré de Verification)
model checking.

Team Leader: Philippe Schnoebelen (LSV)
model checking.

Team Leader: Thierry Jeron (INRIA)
testing theory and tools.

Team Leader: Yassine Lakhnech (Verimag)
infinite state model checking.

Team Leader: Wang Yi (Uppsala)
model checking for real-time systems.

Team Leader: Tom Henzinger (EPFL)
model checking of embedded software and hybrid systems.

1.2 Affiliated Participants: Expertise and Roles

Team Leader: Lubos Brim (University Brno)
distributed model checking.

Team Leader: Henrik Leerberg (IAR Systems A/S)
tool provider.

Team Leader: Tommy Ericsson (Telelogic)
tool provider.

Team Leader: Jan Tretmans (Nijmegen)
models and tools for model based testing

Team Leader: Sven H. Sørensen: (Motorola A/S)
end user.

Team Leader: Thomas Hune: (Terma A/S)
end user.

1.3 Starting Date, and Expected Ending Date

Start date September 1st, 2004 to August 31st 2008

1.4 Baseline

The teams collaborating on this activity are leading tool providers for testing and verification, with particular emphasis on real-time, hybrid and stochastic aspects.

Automatic analysis of such quantitative aspects are crucial in validating embedded systems, but are computationally significantly more difficult than validation of simple functional aspects.

Thus, to address industrial size models continued development of new algorithmic techniques and data structures should be combined with powerful computational resources. We seek to establish this by maximal use, coordination and extension of existing local resources (e.g. PC-clusters) and by exploiting on-going work on exchange between and combinations of tools.

Despite advances in algorithmic techniques verification and test case generation are computationally notoriously hard problems.

Consideration of quantitative phenomena (real-time, stochastic) adds to the complexity. Thus, to address industrial size models powerful computational resources are necessary for example by maximal coordination of existing local resources.

The computational resources of the platform will initially be provided by existing powerful stand-alone computers with the various verification and testing tools being made available via a common web-based interface. A procedure for controlling access in a flexible and secure (e.g. in accordance with the individual tools licence agreements) manner will be investigated.

Among the tools that will be made available we mention: SPIN, SMV, UPPAAL, Kronos, Blast, TorX, TGV, FAST, CADP, IF; HyTech, visualSTATE, TAU, LASH, EMTCC and Rapture where the individual consortium member will have responsibility for integrating their tools into the platform.

The emerging advances in parallel and distributed model checking also motivate the development of a generally accessible server platform consisting of local clusters of (inexpensive) PCs.

Long term vision includes an experimental GRID infrastructure targeted specifically towards verification and testing.

1.5 Problem Tackled in Year2

In order to pursue the overall goal of making the tools applied and developed by the cluster partners attractive for industrial usage, the following problems have been addressed in year 2:

- First of all, the individual tools have been further refined – both with respect to functionality and performance. This includes work on enabling the distribution of analysis techniques over a PC-cluster.
- Secondly, the work of dessimination of the tools through case study demonstrators has been initiated through the introduction of a joint web page for industrial case studies.
- Finally, in order to clarify the possibilities with respect to the establishment of an experimental Grid infrastructure, interaction with European Grid activities has been initiated.

2. Summary of Activity Progress

2.1 *Previous Work*

During the first 12 months a number of improvements have been made on the individual tools as developed by the partners:

- The Vertecs team (IRISA) supports two test generation tools: TGV and STG. During the period, a new version of TGV (based on on-the-fly enumerative algorithms) linked to the IF toolbox (Verimag) has been developed using STL libraries (in place of CADP libraries).
- Results have been implemented in the TIMES tool for automated schedulability checking.
- CFV supports the verification tool LASH and hosts powerful servers dedicated to verification tools.
- A number of improvements have been made on the Uppaal real-time model checker (www.uppaal.com). This includes the possibility to enrich the timed automaton models with C code. An extension of Uppaal (Uppaal Cora), dedicated to solving optimal scheduling and planning problems, has been introduced. Recently, a version of Uppaal (Uppaal Tron), dedicated to online testing of real time systems, has been announced.

Also, a general distributed verification environment (DiVinE, Brno) has been deployed. The environment supports the development of distributed enumerative model checking algorithms, enables unified and credible comparison of these algorithms, and makes the distributed verification available for public use in a form of a distributed verification tool.

Finally, an overview of existing tools has been made accessible via a common web portal (the Yahooda web-page maintained by Brno).

2.2 *Current Results*

2.2.1 *Technical Achievements / Outcomes / Difficulties encountered*

Development of existing and new tools

Brno has completed deployment of the distributed verification tool *"DiVinE"* (version 0.7) for enumerative model checking of LTL properties on a network of workstations. This includes the development of new algorithms for cluster-based decomposition of state spac into strongly connected components to be used in reduction of state spaces

Neijmegen has recently implemented an initial extension of the *TorX* tool (*TorXakis*) for symbolic testing – based on the formalism of Symbolic Transition Systems.

IRISA has worked on symbolic test selection for extended automata using abstract interpretation and included the results by improving test selection in their toolset *STG*.

Verimag has continued work on conformance testing for real-time systems and in particular worked on general improvements on the tool *TTG* (Timed Test Generator).

A new version of *UPPAAL* (Aalborg, Uppsala), UPPAAL 4.0, has been released with a number of new facilities and algorithms *user defined functions* (syntax follows the style of C/C++/Java, and most control-flow constructs of C are supported), *priorities and channels* may be specified and dealt with during analysis, full support for *symmetry reduction* is implemented enabled by the introduction of a *scalar* datatype and the so-called *swep-line* method may be used to reduce memory consumption.

The online testing tool *Uppaal Tron* (Aalborg) has been ported to MS windows, and a new version 1.4 has been released. This represents a significant development effort since the OS and development environments on windows are quite different from those of Linux. We have identified specific technical problems with timing under windows. We believe that the windows version will greatly extend the applicability of the tool

A new variant of Uppaal, *Uppaal Tiga*, for the analysis and synthesis of winning strategies for times games has been released. Extensive evaluation of an experimental implementation of the algorithm yields very encouraging performance results.

Evaluation of tools

The planned work on tool dissemination and evaluation through case studies has been initiated through the establishment of an open repository for Artist2 Test and Verification Case Studies (https://bugsy.grid.aau.dk/artist2). The repository can be maintained by the individual tool providers and users through the use of Wiki.

Exploiting European Grid activities

ARTIST2 partners have participated in two European meetings on parallel and distributed model checking where the issue of exploiting grid activities to build a joint infrastructure has been discussed. The meetings showed that

- There are a number of ongoing European projects with respect to the usage of high performance and Grid-based servers for model checking. Each of the projects have made contributions through new distributed algorithms, new parallel architectures and new interesting applications, and it is likely that these activities will be their main focus for the immediate future. This means that the question of mutual exploitation of resources and the provision of a common web interface will be postponed for the time being.
- The long term vision of a joint high-performance verification platform is still relevant and should be maintained.
- There are already a number of facilities (e.g.) NorduGrid available that may be exploited be the individual tool providers and users. So far, a distributed version of Uppaal (DUppaal) has been made available on the NorduGrid in a certified manner via manual certificate distribution.

2.2.2 Publications Resulting from these Achievements

J. Barnat, L. Brim, I. Cerna, M. Ceska, J. Tumova: Distributed Qualitative LTL Model Checking of Markov Decision Processes. PDMC 2006.

L. Brim: Distributed Verification: Exploring the Power of Raw Computing Power. PDMC 2006.

J. Barnat, L. Brim, I. Cerna, P. Moravec, P. Rockai, P. Simecek: DiVinE - The Distributed Verification Environment. CAV 2006.

L. Brim, I. Cerna, P. Moravec, J. Simsa: How to Order Vertices for Distributed LTL Model-Checking Based on Accepting Predecessors. Electr. Notes Theor. Comput. Sci. 135(2): 3-18 (2006)

J. Barnat, P. Moravec: Parallel Algorithms for Finding SCCs in Implicitly Given Graphs. PDMC 2006.

J. Barnat, L. Brim, I. Cerna: Distributed Analysis of Large Systems. FMCO 2005.

Elena Fersman, Leonid Mokrushin, Paul Pettersson, Wang Yi : Schedulability analysis of fixed-priority systems using timed automata. Theor. Comput. Sci. 354(2): 301-317 (2006).

B. Blanc, F. Bouquet, A. Gotlieb, B. Jeannet, T. J'8eron, B. Legeard, B. Marre, C. Michel, M. Rueher : The V3F Project. in Workshop on Constraints in Software Testing, Verification and Analysis (CSTVA'06), Sept 25-29, Nantes, 2006

L. Frantzen, J. Tretmans, T. Willemse. Test Generation based on Symbolic Specifications.In: J. Grabowski, B. Nielsen (eds.),FATES 2004 - Formal Approaches to Testing of Software.Lecture Notes in Computer Science 3395, pp. 1-15, Springer-Verlag, 2005.

L. Frantzen, J. Tretmans, T. Willemse. A Symbolic Framework for Model-Based Testing.In K. Havelund, M. Nunez, G. Rosu, B. Wolff (eds.),Formal Approaches to Testing and Runtime Verification - FATES/RV'06.Lecture Notes in Computer Science. Springer-Verlag, 2006. To appear.

Kim Guldstrand Larsen, Marius Mikucionis, Brian Nielsen, Arne Skou: Testing real-time embedded software using UPPAAL-TRON: an industrial case study. In proceedings of EMSOFT 2005.

Anders Hessel, Kim Guldstrand Larsen, Marius Mikucionis, Brian Nielsen, Paul Pettersson, Arne Skou: Automated Model-Based Conformance Testing of Real-Time Systems. Book Chapter: “Formal Methods and Testing” Editor(s): Jonathan Bowen, Mark Harman, Rob Hierons, Publishing institution: Springer Verlag 2005. Number of pages: 39. To Appear.

Gerd Behrmann: Distributed reachability analysis in timed automata. In STTT: Software Tools for Technology Transfer 7 (1): 19-30 (2005)

Gerd Behrmann, Alexandre David, Martijn Hendriks, John Håkansson, Kim G. Larsen, , Paul Pettersson, Wang Yi. UPPAAL 4.0. In Proceedings of the Third International Conference on Quantitative Evaluation of Systems, Riverside, CA, USA, September 11-14, 2006.

Franck Cassez, Alexandre David, Emmanuel Fleury, Kim Guldstrand Larsen, Didier Lime: Efficient On-the-Fly Algorithms for the Analysis of Timed Games. CONCUR 2005: 66-80

Gerd Behrmann, Agnès Cougnard, Alexandre David, Emmanuel Fleury, Kim G. Larsen, Didier Lime: UPPAAL Tiga: Timed Games for Everyone. To appear in Nordic Workshop of Programming Theory, Iceland, October 2006.

2.2.3 Keynotes, Workshops, Tutorials

Keynote: Real-time Modle Checking using UPPAAL by Kim G. Larsen. TCS Excellence in Computer Science (TECS) Week 2006, *Pune, India, January 3–7 2006,*

Workshop: SENVA Meeting on Clusters and Grids for Verification and Performance Evaluation

INRIA Rhône-Alpes - Montbonnot (Isère), France, November 16-17, 2005

The aim of this workshop was to present algorithms and tools for distributed analysis of concurrent systems. It was arranged by the SENVA project – a joint CWI, INRIA project on safety critical systems. ARTIST2 partners from Aalaborg and Brno made contributions to the presentations and discussions.

Workshop: SENVA Meeting on Parallel and Distributed Verification

CWI, Amsterdam, The Netherlands, April 3-4, 2006-09-19

The workshop was dedicated to algorithms, tools and case studies for parallel and distributed verification. It was arranged by SENVA in collaboration with a Dutch national project and with contributions from the ARTIST2 partners Aalborg and Brno.

Workshop: 5th International Workshop on Parallel and Distributed Methods in verification, PDMC 2006

August 31, 2006, Bonn, Germany

The PDMC workshop aims to provide a working forum for presenting, sharing, and discussing recent achievements in the field of parallel and distributed verification. The workshop consists of invited talks and a selection from the submitted papers. It was co-located with CONCUR 2006. ARTIST2 partners served as invited speaker, committee mebers and also presented accepted papers.

Tutorial: Tutorial on UPPAAL by Gerd Behrmann, Alexandre David, Kim G. Larsen (Aalborg U.) and Paul Pettersson, Wang Yi (Uppsala U.). The 26th IEEE Real-Time Systems Symposium, http://www.rtss.org/rtss2005, *Miami, Florida, USA, December 5-8, 2005*

Tutorial: Model-based Testing and Validation of Real-Time Systems by Kim G. Larsen and Brian Nielsen. TAROT Summerschool on Testing, http://www.info-ab.uclm.es/tarot/, *Toledo, Spain, June 26 - July 1, 2006*

Tutorial: Verification of UML models by Susane Graf (Verimag). ARTIST2 Summer School on Components & Modelling, Testing & Verification, and Static Analysis of Embedded Systems, *Nässlingen, Sweden, September 29 - October 2, 2005.*

Tutorial: On-line Testing for Real-time Systems by Brian Nielsen (Aalborg). ARTIST2 Summer School on Components & Modelling, Testing & Verification, and Static Analysis of Embedded Systems, *Nässlingen, Sweden, September 29 - October 2, 2005.*

Tutorial: Real-time Model Checking by Gerd Behrmann (Aalborg). ARTIST2 Summer School on Components & Modelling, Testing & Verification, and Static Analysis of Embedded Systems, *Nässlingen, Sweden, September 29 - October 2, 2005.*

3. Future Work and Evolution

3.1 Problem to be Tackled over the next 18 months (Sept 2006 – Feb 2008)

Based on the partner's further development of existing and new tools for quantitative testing and verification, the platform activity will focus on the following issues for the next 18 months:

- The work on tool evaluation through industrial case studies will be continued and reported in the web repository on a regular basis. Also, links to stable and mature versions of the tools will be provided and updated for download.
- As mentioned above, tackling the problems of mutual exploitation of European Grid resources for model checking and establishing a common web interface will be postponed for the time being. However, the established link to European Grid projects on verification will be maintained through regular meetings in order to pursue the overall vision of a powerful computing facility.
- Within ARTIST2, the challenge for establishing high performance resources will be pursued by exploiting resources that are immediately available, like e.g. the NorduGrid facility, which has two clusters in Aalborg that may be applied for experiments. In particular, the distributed version of Uppaal and the Devine tool will be made available on the 50-node PC cluster, and experiments will be made for exploiting the 52 Gbyte shared memory facility for analysing large models by single-CPU tools.

As for the individual tools and algorithms, the following will be worked on:

Neijmegen will continue their work on the symbolic test generation tool TorXagit, which includes results on how to test transition system swith data.

Brno will address the problem of how to extend of distributed verification methods to an inter-cluster setting with the aim to effectivelly make use large networks of heterogenous computers.

IRISA will investigate how to do symbolic test selection using coverage criteria for automata extended with variables.

Aalborg and Uppsala wil continue their further development of the Uppaal tool with focus on (among other subjects) test generation and dissemination through industrial case studies.

3.2 Current and Future Milestones

Current milestones:

- For each year: Further development of existing and new tools.
- Year 1:
  - Availability of the tools through the Yahooda database maintained by the Brno affiliated partner (achieved).
- Year 2 :
  - A server on which the main testing and verification tools developed and used by the participants will be installed and configured (not achieved). Elaboration: The various tools are developed for a variety of platforms; hence, there is no single platform, which can host all tools, and the milestone has therefore been revised (see below).

  - Links to mature model checking tools via the Yahooda homepage (not achieved). Elaboration: The tools will continued to be evaluated in more detail, in order for the existing links at Yahooda to be further characterized. The milestone is therefore maintained (see below).
  - Design of a coordination layer for parallel and distributed model chcking (not achieved); design of a GRID infrastructure (not achieved). Elaboration: As mentioned above, ARTIST2 partners have participated in two meetings with other European projects on these subjects, and the conclusion from the meetings is that more experiments have to be made within the various activities in order to mature the technology. The milestone has therefore been revised (see below).
- **Year 3:**
  - Links to the tools developed and applied by the partners will be collected at a common web entry. Also, it will be analysed whether a common web interface can be provided for tool invocation in a trusted and controlled manner. This is a revision of the above milestone on providing a single powerful server for all tools.
  - The ongoing work on tool evaluation through case studies will be continued and made accessible at the open repository. Also, links to mature version swill be provided via the Yahoda tool homepage. This is a revision of the above milestone on links to mature versions.
  - Further experiments on exploiting contemporary technologies (GRID and PC clusters) will be made. This includes experiments on establishing tool access on available sites (e.g. NorduGrid) as well as further development of distributed model checkers.
- **Year 4:**
  - Integration of results from the related Joint Research Activities

3.3 Indicators for Integration

Establishment of a common access to *all* tools. The successful integration of several of the computational resources available to the consortium in a verification grid, as this will provide an extremely powerful, yet inexpensive platform.

The leading quality of the tools available should make the web access attractive for all clusters of ARTIST2 as well as industry.

As for the tool evaluation through industrial case studies, all partners are in the process of reporting their results ito the shared repository. Also, several of the case studies involve more than one partner institution. Furthermore, the particular techniques of the individual tools are subjects for ongoing discussions at the project meetings.

The joint meetings with other European projects on exploiting PC clusters and Grid technologies, have involved the partners from both Aalborg and Brno; these two partners also collaborate on selected challenges for distributed model checking as well as the exploitation of available PC clusters and Grids.

3.4 Main Funding

Main sources of funding are

Funding from various national funding agencies and centres, such as:

- the Centre for Embedded Systems,
- CISS (http://ciss.auc.dk/),
- BRICS (http://www.brics.dk/),
- Dutch national projects STRESS, HaaST, IMPASSE, MC=MC, CASH (see http://fmt.cs.utwente.nl/),
- Swedish national projects SAVE, ASTEC,
- Czech project on distributed model checking: Paradise.
- DCGC: Danish Center for Grid Computing (http://www.dcgc.dk, in Danish).
- Funding from the IST AGEDIS project – Automatic generation of test cases.

3.5 Internal reviews for this deliverable

Contributions and internal review has been made by Bruno Bouyssounouse (UJF/Verimag), Ed Brinksma (Twente, ESI), Arne Skou (Aalborg).