



IST-004527 ARTIST2
Network of Excellence
on Embedded Systems Design

Activity Progress Report for Year 3

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	3
1.1 ARTIST Participants and Roles	3
1.2 Affiliated Participants and Roles	3
1.3 Starting Date, and Expected Ending Date	3
1.4 Baseline	4
1.5 Problem Tackled in Year 3	4
1.6 Comments From Year 2 Review	5
1.6.1 <i>Reviewers' Comments</i>	5
1.6.2 <i>How These Have Been Addressed</i>	5
2. Summary of Activity Progress	6
2.1 Previous Work in Year 1	6
2.2 Previous Work in Year 2	6
2.3 Current Results	7
2.3.1 <i>Technical Achievements</i>	8
2.3.2 <i>Individual Publications Resulting from these Achievements</i>	9
2.3.3 <i>Interaction and Building Excellence between Partners</i>	11
2.3.4 <i>Joint Publications Resulting from these Achievements</i>	11
2.3.5 <i>Keynotes, Workshops, Tutorials</i>	12
3. Future Work and Evolution	14
3.1 Problem to be Tackled over the next 12 months (Sept 2007 – Aug 2008)	14
3.2 Current and Future Milestones	14
3.3 Indicators for Integration	15
3.4 Main Funding	15
4. Internal Reviewers for this Deliverable	17

1. Overview of the Activity

1.1 ARTIST Participants 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 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 are candidates for being 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 Year 3**

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 3:

- *Development of the individual tools.* First of all, the individual tools have been further refined – both with respect to functionality and performance:
 - The open-source library of Difference-Bound Matrix datastructure (DBM) for timed automata analysis has been extended and improved substantially. This library is applied in the Uppaal tool and its variations.
 - The tool UPPALL Tiga for generation of optimal winning strategies has been fully integrated with the standard UPPAAL edition allowing for exploitation of the full modeling formalism. Also, the internal representation of strategies has been substantially improved by using CDD/BDD.
- *Dessimination and evaluation through industrial case studies.* The work of dessimination of the tools through case study demonstrators has been continued and

documented through the joint web page for industrial case studies. Apart from classical modelling efforts of protocol and controller algorithms, new application directions have been demonstrated through *automatic controller synthesis* and *biological sensor networks*. Furthermore, it has been demonstrated how the controller synthesis may be part of a full *tool chain*.

- *High performance tools server analysis*. In order to clarify the possibilities with respect to the establishment of an experimental high-performance tool server, the academic tools have been examined wrt. their ability to handle large state spaces. Unfortunately, it turns out that only a few of the tools at present can circumvent the 32 bit addressing limitation through distributed implementation or through 64 bit addressing of the state space.

1.6 Comments From Year 2 Review

1.6.1 Reviewers' Comments

There were no specific comments from the reviewers.

1.6.2 How These Have Been Addressed

There were no specific comments from the reviewers.

2. Summary of Activity Progress

2.1 Previous Work in Year 1

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 Previous Work in Year 2

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 space 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 by 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.

2.3 Current Results

The technical results below are based on joint collaboration between the partners in terms of tool sharing and evaluation (all partners) and the development of new algorithms for test generation and controller synthesis (Twente, CFV, LSV, Aalborg). Also, IRISA, Brno, Aalborg and Uppsala are contributing with further tool development – partly based on the new algorithms., and Aalborg and Brno are investigating the high performance platform issue.

Finally, the partners contribute to cross-cluster activities on tools and platform integration, and also interact with communities out ARTIST2.

2.3.1 Technical Achievements

Development of existing and new tools

IRISA has improved the STG tool (test generation for models with control and data) and it is now freely distributed (<http://www.irisa.fr/vertecs/software.html#STG>). Its integration with the NBAC analyzer and the APRON library has been improved. Also, a number of cases studies have been developed and experimented.

UPPSALA has developed a prototype tool (named CATS) for compositional timing and performance analysis using timed automata and the real time calculus developed at EPFL. It is based on an over-approximation technique in which a component of a system, modeled as a timed automaton is abstracted as a transducer of event streams described by arrival curves from the real-time calculus. This allows us to characterize the semantics of a system as a set of equations over streams. Many interesting properties such as schedulability and buffer boundedness can be checked in solving the equations. The CATS tool is implemented in the Eclipse tool platform. As the main feature of the current version, it can be used to check the schedulability of a system and to estimate the best and worst case response times of its computation tasks. The tool is available for evaluation at www.timestool.com/cats.

AALBORG has continued its work on improving *UPPAAL* (www.uppaal.com) and its variants *UPPAAL Tron* (online testing) and *UPPAAL Tiga* (analysis and synthesis of winning strategies for timed games). In particular, the basic common DBM library has been improved and several industrial cases have been carried out. Also, the performance and the presentation of winning strategies have been improved significantly.

VERIMAG has implemented new techniques for deadlock detection in DeadlockFinder - a prototype tool that generates from BIP models sufficient conditions for deadlockfreedom.

BRNO has put a major effort into the development of tools to support parallel verification of complex embedded systems. The DiVinE tool has been made publically available and extended by a Promela front-end for SPIN compatible distributed model checking. With DiVinE Multi-Core (published at SPIN'07 and released in October 2007) the world-wide first parallel model-checker for multi-core architectures has been launched. Furthermore, in the area of parallel techniques for the verification and analysis of embedded systems we focused on the development of new and enhanced algorithms for the enumerative parallel checking of reachability, safety and liveness properties, in particular taking into account stochastic aspects of embedded systems.

Evaluation and dissemination of tools

A number of industrial case studies have been carried out by OFFIS, Twente, Aalborg and Uppsala. Apart from being documented via scientific papers, they are also collected and disseminated through the open repository for Artist2 Test and Verification Case Studies

(<https://bugsy.grid.aau.dk/artist2>). Links to mature versions of the applied tools may also be found at the web page.

Investigations wrt. High-performance tool server

In most verification cases, the performance bottle neck is the state space explosion, i.e. the size of the internal memory for representing the state space. As a result of questioning the development teams and experimenting with the tools, it turns out that most academic verification tools are limited by the fact that they have been developed for a 32-bit architecture. In fact, only a few of them are considering to become upgraded to 64-bit architectures, and our investigation only identified a single 64-bit tool, namely the SPIN model checker. The SPIN team is currently working on extending the tool to exploit a multi-cpu shared memory architecture.

Hence, the available tools for a possible high performance tool server are currently SPIN (on a shared memory architecture) and UPPAAL/DiVinE (on distributed PC clusters).

Aalborg is currently installing a large (600 node) PC cluster which will be made available via NoduGrid (www.nordugrid.org). It will mainly be dedicated to scientific computing, but experiments with high-performance model checking (also parallel and distributed model checking) will be possible to a certain extent.

2.3.2 Individual Publications Resulting from these Achievements

OFFIS

Werner Damm, Alfred Mikschl, Jens Oehlerking, Ernst-Rüdiger Olderog, Jun Pang, André Platzer, Marc Segelken, and Boris Wirtz. Automating verification of cooperation, control, and design in traffic applications. LNCS. Springer, 2007. To appear.

Werner Damm, Stefan Disch, Hardi Hungar, Swen Jacobs, Jun Pang, Florian Pigorsch, Christoph Scholl, Uwe Waldmann, and Boris Wirtz: Exact state set representations in the verification of linear hybrid systems with large discrete state-space. In Proc. 5th Symposium on Automated Technology for Verification and Analysis, Lecture Notes in Computer Science 4762, pp. 425-440. Springer-Verlag, 2007.

Werner Damm, Stefan Disch, Hardi Hungar, Jun Pang, Florian Pigorsch, Christoph Scholl, Uwe Waldmann, and Boris Wirtz: Automatic verification of hybrid systems with large discrete state space. In Proc. 4th Symposium on Automated Technology for Verification and Analysis, Lecture Notes in Computer Science 4218, pp. 276-291. Springer-Verlag, 2006.

IRISA

V. Rusu: Verifying an ATM Protocol Using a Combination of Formal Techniques, Computer Journal, 49:710-730, November 2006.

C. Constant, T. Jérón, H. Marchand, V. Rusu: Integrating formal verification and conformance testing for reactive systems, IEEE Transactions on Software Engineering (To appear), 2007.

C. Constant, B. Jeannet, T. Jérón: Automatic test generation from interprocedural specifications, in TestCom/Fates07, Tallinn, Estonia, June 2007.

E. Dumitrescu, A. Girault, H. Marchand, E. Rutten: Optimal discrete controller synthesis for the modeling of fault-tolerant distributed systems, in First IFAC Workshop on Dependable Control of Discrete Systems (DCDS'07), Paris, France, June 2007.

LSV

Christel Baier, Nathalie Bertrand, Patricia Bouyer, Thomas Brihaye, Marcus Groesser, Probabilistic and Topological Semantics for Timed Automata, accepted at FSTTCS'07.

Thomas Brihaye, Francois Laroussinie, Nicolas Markey, Ghassan Oreiby, Timed Concurrent Game Structures, proceedings of the conference CONCUR 2007, Lect. Notes in Computer Science 4703, pp 445-459, Springer.

TWENTE

C. F. Daws and P. T. Kordy: Symbolic Robustness Analysis of Timed Automata. In E. Asarin and P. Bouyer, editors, Formal Modeling and Analysis of Timed Systems, Paris, France, volume 4202 of Lecture Notes in Computer Science, September 2006.

D. N. Jansen, J.P. Katoen, Marcel Oldenkamp, M.I.A. Stoelinga, and I.S. Zapreev, How fast and fat is your probabilistic model checker? an experimental performance comparison, In Proceedings of the Haifa Verification Conference, LNCS, 2007, to appear.

AALBORG

Gerd Behrmann, Agnès Cougnard, Alexandre David, Emmanuel Fleury, Kim Guldstrand Larsen, Didier Lime: UPPAAL-Tiga: Time for Playing Games! CAV 2007.

Jan Jakob Jessen, Jacob Illum Rasmussen, Kim G. Larsen, Alexandre David: Guided Controller Synthesis for Climate Controller Using Uppaal TIGA. FORMATS 2007.

Alexandre David: Pushing The Limits Of DBMs. Under submission.

Thomas Chatain, Alexandre David, Kim G. Larsen: Playing Games with Timed Games. Under submission.

UPPSALA

Pavel Krcaľ, Leonid Mokrushin and Wang Yi: A tool for compositional analysis of timed systems by abstraction, The 19th Nordic Workshop on Programming Theory Oslo, October 10-12, 2007.

Brno

J. Barnat, L. Brim, I. Cerna, S. Drazan, D. Safranek: Parallel Model Checking Large-Scale Genetic Regulatory Network with DIVINE. FBTC 2007.

J. Barnat, L. Brim, I. Cerna, M. Ceska, J. Tumova: ProbDiVinE - A Parallel Qualitative LTL Model-Checker. QEST 2007.

L. Brim, J. Barnat: Tutorial on Parallel Model-Checking. SPIN 2007.

J. Barnat, L. Brim, P. Rockai: Scalable Multi-Core LTL Model-Checking. SPIN 2007.

J. Barnat, L. Brim, M. Leucker: Parallel Model Checking and the FMICS-jETI Platform. ICECCS 2007.

J. Barnat, L. Brim, P. Simecek: I/O Efficient Accepting Cycle Detection. CAV 2007.

L. Brim, M. Kretinsky: Model Checking Large Finite-State Systems and Beyond. SOFSEM 2007.

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

L. Brim, I. Cerna, P. Moravec, J. Simsa: On Combining Partial Order Reduction with Fairness Assumptions. FMICS 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.

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

Jiri Barnat, Lubos Brim, Ivana Cerna: Distributed Analysis of Large Systems. FMCO 2005.

2.3.3 Interaction and Building Excellence between Partners

The partners developing tools meet on a regular basis with the partners that contribute to the further development of algorithms in order to evaluate and improve the tools as may be seen from list of joint publications below.

Several partners (CFV, LSV, Twente, Aalborg) have participated in a successful FP7 proposal on quantitative aspects of embedded systems (Quasimodo). A key element of this coming project is the development of tool plugins aimed to be applied in a variety of tools (commercial or academic).

Uppsala and Aalborg meet on a regular basis to coordinate the further development of the UPPPAAL tool which forms the basis of a large part of the platform activities.

At a national level, a cross cluster collaboration between the Danish ARTIST2 partners Aalborg and DTU (execution platforms) have resulted in a large national grant to an industrial project proposal (DaNES) on tools and platforms for intelligent embedded systems. Also, a grant has been given to promote industrial awareness towards the upcoming FP7 calls within the ARTEMIS JTI programme.

2.3.4 Joint Publications Resulting from these Achievements

Patricia Bouyer, Thomas Brihaye, Veronique Bruyere, Jean-Francois Raskin. On the Optimal Reachability Problem for Timed Automata. Formal Methods in Systems Design 31(2): 135-175 (2007).

Patricia Bouyer, Kim Guldstrand Larsen, Nicolas Markey, Jacob Illum Rasmussen: Almost Optimal Strategies in One Clock Priced Timed Games. FSTTCS 2006.

Patricia Bouyer, Kim Guldstrand Larsen, Nicolas Markey: Model-Checking One-Clock Priced Timed Automata. FoSSaCS 2007.

H. Dierks, S. Kupferschmid and K.G. Larsen; Automatic Abstraction Refinement for Timed Automata, FORMATS 2007, LNCS, Springer

M. Oostdijk, V. Rusu, J. Tretmans, R. de Vries, T. Willemse: Integrating verification, testing, and learning for cryptographic protocols, in Integrated Formal Methods (IFM'07), 2007.

Alexandre David, John Håkansson, Kim Guldstrand Larsen, Paul Pettersson: Model Checking Timed Automata with Priorities Using DBM Subtraction. FORMATS 2006.

Gerd Behrmann, Agnès Cougnard, Alexandre David, Emmanuel Fleury, Kim Guldstrand Larsen, Didier Lime: UPPAAL-Tiga: Time for Playing Games! CAV 2007.

Sebastian Kupferschmid, Klaus Dräger, Jörg Hoffmann, Bernd Finkbeiner, Henning Dierks, Andreas Podelski, Gerd Behrmann: Uppaal/DMC-Abstraction-Based Heuristics for Directed Model Checking. TACAS 2007.

Franck Cassez, Alexandre David, Didier Lime, Kim Larsen, Jean-Francois Raskin. Timed Control with Observation Based and Stuttering Invariant Strategies. To appear in ATVA'07, Lecture Notes in Computer Science, Springer Verlag, 25 pages, 2007.

2.3.5 Keynotes, Workshops, Tutorials

The partners have regular meetings at various Phd schools and workshops where they give invited lectures and tutorials (see below). Also, they have participated in cross-cluster workshops at conferences (CAV 2007, DATE 2007).

Keynotes :

Thierry Jéron gave a keynote speech on /Model-based test selection for infinite state reactive systems/ at the 5th International Symposium on Formal Methods for Components and Objects (FMCO'06, Amsterdam, November 2006).

<http://fmco.liacs.nl/fmco06.html>

Kim G. Larsen (invited talk): 10 Years of UPPAAL: From Theory to Industrial Impact. International Workshop on Advances in Model-Checking in honour of Gerard J. Holzmann. December 2006. University of Twente, Enschede, The Netherlands.

<http://wwwhome.cs.utwente.nl/~kuntzwm/WorkshopMCProgram.php>

Kim G. Larsen (invited talk): UPPAAL Tiga -- Controller Synthesis for Real-Time Systems. December 2006. Centre Federe on Verification. Brussels, Belgium.

Workshops:

Kim G. Larsen and Jan Madsen: Validation and Performance Analysis of Real-Time Systems in UPPAAL. Towards a Systematic Approach to Embedded System Design: Bringing Leading-Edge Embedded Systems Design Tools to Industrial Users. ARTIST2 workshop at DATE, Nice, France, April 2007.

<http://www.artist-embedded.org/artist/-ARTIST2-Workshop-at-Date-07-.html>

Kim G. Larsen and Michael R. Hansen: Validation and Performance Analysis of Real-Time Systems in UPPAAL. ARTIST WS: Tool Platforms for ES Modelling, Analysis and Validation. Computer Aided Verification, July 2007.

<http://www.artist-embedded.org/artist/-Tool-platforms-for-modelling-.html>

Kim G. Larsen: UPPAAL after ten years. Workshop on Applied Concurrency Research in Industry, (IFIP Working Group on Concurrency Theory) Affiliated with CONCUR, September 7, 2007, Lisbon, Portugal.

<http://www.ru.is/luca/ifipworkshop/>

Tutorials :

Vlad Rusu gave a talk on Model-based testing at the MOTIVES 07 Winter school in Trento (February 2007).

<http://www.artist-embedded.org/artist/Overview,577.html>

Alexandre David and Kim G. Larsen (invited mini course): Validation and Verification of Embedded and Real Time Systems. October 17, 2006, Reykjavik University, Iceland.

Brian Nielsen: Model-based Testing of Real-Time Systems. TESTCOM/FATES, June 26-29, 2007, Tallin, Estonia.

<http://testcom-fates07.ioc.ee/tutorials.html>

3. Future Work and Evolution

3.1 *Problem to be Tackled over the next 12 months (Sept 2007 – Aug 2008)*

Apart from the partner's further development of existing and new tools for testing and verification, the platform activity will focus on the following issues for the next 12 months:

- The case tool repository will be updated along with the ongoing work on tool evaluation through case studies. Links to stable and mature tool versions will be provided.
- The three candidates for high-performance verification (SPIN, DUPPAAL, DiVinE) will be tested on the new cluster in Aalborg and will be made available for experiments after special agreements with NorduGrid and the tool developers.
- The links to existing activities on high-performance verification resources will be maintained in order to be able to exploit the available technology in an optimal way.

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

- Coverage-based test generation with semantical notions of coverage using dynamic partitioning. Implementation in STG (Irisa).
- Further development and application of UPPAAL Tiga wrt. synthesis of winning strategies for timed games (Aalborg).
- Further development of the CATS tool (Uppsala)

3.2 *Current and Future Milestones*

The following milestones are recalled and commented in italics from last years deliverable report D26-TV-Y2:

Current milestones for year 3

- The work on tool evaluation through industrial case studies will be continued and reported in the web repository on a regular basis (*achieved*). Also, links to stable and mature versions of the tools will be provided and updated for download (*achieved*).
- 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 (*achieved via the close links to the NorduGrid project*).
- 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 (*partly achieved by investigating which tools that are candidates for high-performance verification, i.e. SPIN, UPPAAL, DiVine*). 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 (*not achieved because the PC cluster is in an upgrade phase which will be completed during October 2007*).

Future milestones until August 2008

- **The case tool repository will be updated along with the ongoing work on tool evaluation through case studies. This includes links to stable and mature tool versions will.**
- **The three candidates for high-performance verification (SPIN, DUPPAAL, DiVine) will be tested on the new cluster in Aalborg and will be made available for experiments after special agreements with NoduGrid and the tool developers.**
- **Links to existing activities on high performance verification resources will be maintained.**

3.3 Indicators for Integration

Establishment of a common access to *all mature* 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 regularly reporting their results into 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 close links the European Grid projects via Aalborgs participation in NorduGrid assures the access to the most recent Grid technology when it becomes available.

3.4 Main Funding

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

- the Centre for Embedded Systems,
- CISS (<http://ciss.auc.dk/>),
- MoDES (<http://www.cs.aau.dk/modes>),
- Dutch national projects STRESS, HaaST, IMPASSE, MC=MC, CASH (see <http://fmt.cs.utwente.nl/>),
- EU (CREDO project): Modeling and analysis of evolutionary structures for distributed services
- Swedish strategic research (SAVE project): Component Based Design of Safety Critical Vehicular Systems

- Swedish research council (UPPAAL/TIMES): Modeling and verification of timed systems
- DCGC: Danish Center for Grid Computing (<http://www.dcgc.dk>, in Danish).
- French RNTL project Testec (Testing of real-time embedded control-command systems) with Lurpa (Ens Cachan), Inria (Rennes), I3S (Nice) , Labri (Bordeaux), EDF R&D, TNI Software has been accepted.

4. Internal Reviewers for this Deliverable

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