ARTIST 2
Network of Excellence

IST-004527 ARTIST2:
Embedded Systems Design

Activity Progress Report for Year 2

JPRA-NoE Integration

Quantitative Testing and Verification

Clusters:

Testing and Verification

Activity Leader:

Ed Brinksma (University of Twente)
http://wwwhome.cs.utwente.nl/%7Ebrinksma/

Policy Objective (abstract)

The objective is to combine the efforts and skills of the individual leading researchers in Europe into a world-class virtual team, for advancing the state-of-the-art in verification and testing methodologies.

Achieving this objective requires development of theory, methods and tools for testing and verification of embedded systems with an emphasis on quantitative aspects (e.g. real-time and stochastic phenomena), that are of particular importance for the correctness of embedded systems.

A particular effort will be made to transfer knowledge, methods and tools to industry, including integration of the techniques developed into existing tools.

.

Table of Contents

1. Overview of the Activity

1.1 ARTIST2 Participants: Expertise and Roles

Team Leader: Kim G. Larsen (BRICS/Aalborg)
real-time and probabilistic verification and testing.

Team Leader: Ed Brinksma (University of Twente)
model-based testing, stochastic modelling and verification.

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

Team Leader: Philippe Schnoebelen (LSV)
model checking.

Team Leader: Thierry Jéron (INRIA/Rennes)
real-time testing.

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

Team Leader: Wang Yi (Uppsala)
real-time verification and schedulability.

Team Leader: Tom Henzinger (EPFL)
model checking algorithms for stochastic, real-time, and hybrid systems

Team Leader: Werner Damm (OFFIS)
modelling and validation of safety-critical systems.

1.2 Affiliated Participants: Expertise and Roles

Team Leader: Tretmans (Nijmegen)
testing

Team Leader: Bouajjani (LIAFA)
real-time and hybrid model checking

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

Team Leader: Tommy Ericsson (Telelogic)
testing tool provider.

Team Leader: Sven H. Sørensen (Motorola A/S)
Areas of his team's expertise: development of embedded systems using model-driven methodology.

Team Leader: Christer Nordstöm （ABB Automation)
Areas of his team's expertise: Modelling and validation of industrial robotics.

Team Leader: Jan Lindblad (Enea Embedded Technology)
Areas of his team's expertise: Real Time Operating Systems and Testing.

Team Leader: Alain Ourghanlian (EDF Recherche et Développement)
Areas of his team's expertise: static analysis and model checking .

1.3 Starting Date, and Expected Ending Date

Start date September 1st,2004. Expected ending date Autust 31th 2008.

1.4 Baseline

The long-term ambition of the Testing and Verification cluster is to improve current industrial practice for developing embedded systems applications by continuous dissemination and improvement of existing powerful testing and verification techniques. For embedded systems – besides functional correctness – properties concerning quantitative aspects including real-time constraints and constraints on quality of services are of utmost importance. It is therefore our aim to provide modelling formalisms, methods and tools which will allow such quantitative aspects to be dealt with at early design stages and utilized in a systematic (and ideally automatic) approach in the testing phase. Also, based on existing powerful (real-time) verification techniques new research challenges of industrial importance is taken-up including optimal scheduling, monitoring and fault diagnosis, coverage metrics, controller synthesis, analysis of hybrid models (allowing to take into account the physical environment in which an application is used) and robustness and implementability of timed models. The involved partners include leading European teams with responsibility for some of the most mature methods and tools for testing and verification of functional, timing and QoS properties.

There are several ongoing collaborations, including:

- CFV, Verimag, LIAFA and Uppsala work on integration of tools based on IF within the FST Project Advance;
- Numerous collaborations between LSV and Verimag on national projects (Eva, Prouvé, Rossignol, Action Spécifique du CNRS)
- Aalborg and Uppsala has since 95 collaborated on the development of the tool UPPAAL in parallel with the development of Kronos at Verimag;
- Aalborg and Twente collaborate with the Dutch project STRESS on developing a tool for automatic, on-the-fly test-generation and –execution for real-time systems;
- LSV and Aalborg (and recently) Twente are collaborating on compositional model checking and optimal control for real-time systems.
- Twente and INRIA have long been collaborating on testing methodologies and tools;
- INRIA and Verimag has for a long time collaborated on developing the testing tool TGV, and are currently collaborating on connecting IF and TGV within the Agedis IST project and the national project AS Testic
- Aalborg and Twente are collaborating on models and tools for real-time and stochastic systems.
- Collaboration between LSV and LIAFA on symbolic methods for quantitative verification

1.5 Problem Tackled in Year2

As mentioned above, our goal is to provide modelling formalisms, supporting methods and tools which will allow quantitative aspects (e.g. real-time, QoS) to be dealt during design, verification and testing. Also, based on existing powerful (real-time) verification techniques new research challenges of industrial importance is taken-up.

The initial technical description identified the following challenges:

> Development of a theoretical foundation for testing of real-time systems. Design of algorithms and data-structures and implemented tool support for automatic verification, test-generation and –execution. Exploitation of the complementary nature of verification and testing in development of new, easy to use and cost-efficient model-based testing techniques. This testing approach calls for application of various verification techniques (e.g. model-checking, theorem proving, controller synthesis, game theory).
>
> A main challenge will be on how to extend the successful techniques developed for the verification and testing of finite-state systems (BDDs, partial order reduction, symmetry-reduction, compositional methods) to the settings of quantitative models, in particular ones including real-time and stochastic properties.

The high level objectives for the 18 months period September 2005 until February 2007 was as follows:

> Work on test case generation will be continued and disseminated. Testing theories and analysis techniques for quantitative aspects of models and their implementation will be developed with metrics for testing coverage. Also new important areas to be studied includes robustness and implementability of timed models, stochastic model checking and controller synthesis.

During the second year all of these objectives have been addressed in quite some detail. The problems dealt with fall within the following groups:

- *Real-time verification*. Verification of real-time systems is supported by a number of tools for analysis and model-checking timed automata models. The design and careful implementation of efficient datastructures and algorithmic techniques is an ongoing research activity. During the period UPPAAL 4.0 was released introducing many new features and improvements including (among other things) symmetry reduction, user defined functions, priorities, new abstraction techniques and with a factor 3 to 5 reduction in memory usage.
- *Testing*. The work on providing a theoretical foundation for real-time (conformance) testing has been pursued by several partners and has been implemented in the tools TTG (timed test generator) and UPPAAL Tron (on-line test generator and execution). Metrics for measuring coverage based on discounting techniques has been introduced and the model based testing approach has been extended to cover probabilistic and data intensive models. A barrier in successful application of a model-based approach to development of systems which integrates existing components is the absence of models. Here the problem on how to best provide high quality estimates of models based on test results is a challenge in particular in the setting of quantities.
- *Optimal scheduling and Controller synthesis*.
    - The problem of controller synthesis from so-called timed *game* automata has been addressed by several partners of the cluster. In particular synthesis wrt general control purposes has been studied and efficient on-the-fly algorithms for reachability and safety games with implementation in UPPAAL Tiga has been undertaken. Also related problems concerning monitoring and fault-diagnosis,

decentralized observation, as well as controller synthesis under incomplete or partial information have been studied.

- The model of priced (or weighted) timed automata has become a popular and powerful extension of timed automata which permits the consumption of resources to be modelled. The model raises a the question as to computability of a number of interesting optimization problems such as optimal reachability (or optimal finite schedules) and optimal safety (or optimal infinite schedules). These problems and their efficient implementation in tools such as UPPAAL Cora has been addressed in the period. Similar optimization problems in a setting of multiple prices have also been addressed.

- *Robustness, implementability and schedulability*. The quantitative information in a given real-time model (often a timed automaton) expresses idealized assumption of the final running system. In particular clock-drifts, inaccuracy in measuring time, account of underlying scheduling principles are conveniently abstracted away. A problem is how to guarantee that properties established of the idealized timed automaton model are also true of the running system.
- *Hybrid Systems and Infinite State Systems*. For many real-life applications the environment (or plant) in which the control program is operating needs to be quite accurately modelled in order to assess correctness. Here various hybrid models, where both discrete and continuous behaviour may be taken into account are necessary. The theoretical foundation for allowing (approximate) analysis and refinements is a problem dealt with by several of the partners. For general infinite state systems (e.g. parameterized, data dependent systems or systems with communication-buffers) symbolic datastructures and (approximate) analysis techniques are required for their analysis.
- *Stochastic and Probabilistic Analysis*. The problem of taking stochastic information into account in search for optimal schedules has been addressed, as well as that of performing reliability analysis based on stochastic information.

1.6 Comments From Previous Review

1.6.1 Reviewers' Comments

The document has been modified to incorporate the changes requested in the Year 1 review report.

1.6.2 How These Have Been Addressed

No further action required.

2. Summary of Activity Progress

2.1 Previous Work

The Vertecs team of INRIA is working on test generation for models of infinite state systems with control and data. Systems are modelled with ioSTS (e.g. automata extended with data). Test generation from specification models and test purposes is based on syntactic transformations guided by approximate co-reachability analysis. The main achievements are:

- A new formalisation of symbolic test generation and the impact of approximation of analysis on the precision of test cases published in B. Jeannet, T. Jéron, V. Rusu, E. Zinovieva, “Symbolic Test Selection based on Approximate Analysis”, TACAS 2005. The formalization is more concise and general than in our previous works, reducing test selection to coreachability analysis. As coreachability is undecidable in ioSTS, test selection is then based on an approximate analysis. Compared to an exact analysis, the consequence is that test cases may delay the detection of the unsatisfiability of the test purpose (impacting on Inconclusive verdict), but remain sound for both Pass and Fail verdicts.
- A combination of verification and testing of safety properties for ioSTS published in T. Le Gall, B. Jeannet, H. Marchand, “Supervisory Control of Infinite Symbolic Systems using Abstract Interpretation”, ECC 2005. In this work, we propose a methodology and techniques where safety properties are checked on the specification, and then used to automatically generate test cases (by a generalization of our symbolic test selection techniques). In this framework, verification of safety properties is undecidable, thus relying on approximate analysis. Now, resulting test cases may detect non-conformances and violations of safety properties on the implementation. Additionaly, test cases may also detect violations on the specification, thus completing the verification phase during testing.

Uppsala has shown that the schedulability problem will be undecidable if tasks execution times may vary within an interval (representing the best and worst case execution times). They also developed an algorithm to compute the worst-case response times of non-uniformly recurring fixed-priority tasks. For systems containing only periodic tasks, the algorithm performs as well as the classic method for Rate-Monotonic Analysis. These results have been implemented in the TIMES tool for automated schedulability checking.

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. (Aalborg) This has given an important increase in the expressiveness of the modelling tool, e.g. the possibility to include advanced data types. During the period, the tool has been applied for off-line test generation on a connectivity testing framework.

An extension of UPPAAL (UPPAAL Cora, Aalborg), dedicated to solving optimal scheduling and planning problems, has been introduced. This version is based on a version of the classical timed automaton formalism extended with auxiliary cost variables and with a modified version of the UPPAAL verification engine to take the accumulation of cost into account. During the period, several new algorithms have been designed for transforming the cost optimisation problem into a max-flow problem (in stead of a linear programming problem), and they will be introduced in forthcoming versions of the tool.

Twente has carried out work on:

- Scheduling by reachability analysis: The feasibility of using search techniques from model checking to synthesize and analyse scheduling problems of industrial relevance was established.

- Integrated quantitative analysis: The usefulness of model checking techniques for Markov chain analysis was further extended by application to Markov reward modelling. An industrial case study was carried out concerning an availability monitoring algorithm for self-configuring networks, with analysis carried out using the MODEST modelling formalism and the Moebius tool.
- Modelling of hybrid systems: A process algebraic formalism for the modelling and analysis of hybrid systems has been developed.
- Real-time testing: A real-time testing theory for quiescent systems has been formulated, implemented as a TorX extension, and extended to multi-channel interfaces.

Information on formal methods relevant for industrial applications have been collected by OFFIS, and support was given to industrial partners to perform case studies on formal verification tools (commercial ones as well as academic ones). The work on case studies showed that it actually is possible to formally prove safety properties of e.g. existing car steering control software.

Uppsala has developed a sampling semantics for timed automata, and shown that the new semantics gives rise to a natural notion of digitalization for timed lnguages. A recent result shows that the language inclusion problem in this setting is decidable, which in turn implies that for any timed automaton, a digital machine can be constructed systematically, which accepts the digitalized language of the automaton.

A version of UPPAAL (UPPAAL Tron, Aalborg), dedicated to online testing of real time systems, has been announced. By using UPPAAL Tron, one can extend the testing power of traditional tools substantially, partly because one can run tests for a very long time, and also because Uppaal Tron gives the possibility to build various stochastic criteria into the test selection algorithm. During the period, further performance improvements have been made, and also a first realistic industrial case study has been made. The purpose of the study was to test the functionality of an existing electronic cooling thermostate, and several inconsistencies wrt. the product specification were revealed.

Cachan has

- Designed techniques for computing the convex hull of Presburger-definable sets of tuples of integers. These abstraction techniques are used in model-checking of complex counter systems.
- Improved techniques for verification of communicating systems: half-duplex channel systems and probabilistic lossy channel systems.
- Introduced the concept of "flat acceleration", a powerful generic algorithmic approach for the symbolic computation of reachability sets in regular model checking.
- In-depth study of the descriptive power of formalisms based on timed-automata and extensions, constrasted with verification costs.
- Model checking sets of paths: an approach that sits in between test and model checking. Also, quantitative analysis of priced timed automata, and used timed automata as a tool for fault diagnosis.
- Designed new probabilistic models supporting improved verification algorithms .
- Extensions of temporal logic formalisms, and associated verification techniques.
- Used Uppaal for the verification of a multitask automation system.

2.2 Current Results

2.2.1 Technical Achievements / Outcomes / Difficulties encountered

UPPAAL 4.0 Real Time Verification
UPPAAL 4.0 is the result of over two and half years of development and contains many neew features, additions to the modelling language, performance improvements, enhancements and polish to the easy to use graphical user interface, and libraries are available free of charge for academic, educational and evaluation purposes. In UPPAAL 4.0 the modelling language is extended with user defined functions. These are fully integrated into the modelling language, and can access and modify all state variables. The syntax follows the style of C/C++/Java, and mmost control-flow constructs of C are supported. The modelling language is also extended in order that priorities and channels may be specified and dealt with during analysis. On the performance side, 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. Main team Aalborg University.

Timed channels systems
We have studied channel systems whose behaviour (sending and receiving messages via unbounded FIFO channels) must follow given timing constraints specifying the execution speeds of the local components. We propose Communicating Timed Automata (CTA) to model such systems. The goal was to study the borderline between decidable and undecidable classes of channel systems in the timed setting. Our technical results include proof of decidability in the setting of one channel (equivalent to one-counter machines) and proof of undecidability in the setting of two or more channels. It is noted that in the untimed setting, these systems are no more expressive than finite state machines. This shows that the capability of synchronizing on time makes it substantially more difficult to verify channel systems. Main team involved: Uppsala University.
Difficulty: Undecidability occurs already in the presence of two channels. The challenge will be to identify interesting channel systems (with multiple channels) in which some timing behaviour is allowed and for which problems such as reachability is decidable.

Test-based learning of timed behaviour
We present an algorithm for inferring a timed-automaton model of a system from information obtained by observing its external behavior. Since timed automata can not in general be determinized, we restrict our attention to systems that can be described by deterministic *event-recording automata*. In previous work we have presented algorithms for event-recording automata that satisfy the restriction that there is at most one transition per alphabet symbol from each state. This restriction was lifted in subsequent work by an algorithm based on the region graph.
In this work, we extend previous work by considering the full class of event-recording automata, while still avoiding to base it on the (usually prohibitively large) region graph. Our construction deviates from previous work on inference of automata in that it first constructs a so called timed decision tree from observations of system behavior, which is thereafter folded into an automaton. Main team involved: Uppsala University.

Verification and conformance testing for reactive system.
The work studies the combination of verification and conformance testing for the formal validation of reactive systems. In particular focus has been on verification and selection of test cases that may detect both non conformance and violation of properties. Main team involved: IRISA.

Difficulty: The diffulty lies in the establishing the methodology which integrates verification and conformance testing.

Symbolic test selection for extended automata using abstract interpretation.
We continue this work line by improving test selection in our toolset STG. Main team involved: IRISA.
Difficulty: One difficult problem we attack is the refinement of test selection by the use of dynamic partitioning in abstract interpretation.

Symbolic Determinisation of Extended Automata.
In this work, we define a symbolic determinisation procedure for automata extended with symbolic data variables, which has applications in verification, testing, and diagnosis of infinite-state systems. Main team involved: IRISA.
Difficulty: The difficulty was to characterize the subclass of bounded look-ahead extended automata for which the procedure terminates.

Off-line test generation for real-time systems
We present experiences from a case study where a model-based approach to black-box testing is applied to verify that a Wireless Application Protocol (WAP) gateway conforms to its specification. The WAP gateway is developed by Ericsson and used in mobile telephone networks to connect mobile phones with the Internet. We focus on testing the software implementing the session (WSP) and transaction (WTP) layers of the WAP protocol. These layers, and their surrounding environment, are described as a network of timed automata. To model the many sequence numbers (from a large domain) used in the protocol, we introduce an abstraction technique. We believe the suggested abstraction technique will prove useful to model other similar protocols with sequence numbers, in particular in the context of model-based testing. A complete test bed is presented, which includes generation and execution of test cases. It takes as input a model and a coverage criterion expressed as an observer, and returns a verdict for each test case. The test bed includes existing tools from Ericsson for test-case execution. To generate test suites, we use UPPAAL Cover— a new test-case generation tool based on the real-time model-checker UPPAAL. Main team involved: Uppsala University and Aalborg University.

Testing of programs with floating point numbers.
Conformance testing of a program with floating point numbers with respect to its specification with real numbers. Main team involved: IRISA.
Difficulty: lies in the poor mathematical properties of floating point numbers.

Black-box testing of cryptographic protocols.
Compositional approach for checking secrecy and authenticity properties of cryptographic protocols integrating ideas from verification, conformance testing, and learning, applied to biometric passports. Main team(s) involved: IRISA.
Difficulty: black-box testing of actual implementations of cryptographic protocols is much less studied than verification of their specifications.

Verification of Communication Protocols using Abstract Interpretation of FIFO queues.
This work proposes a new approach to the verification of infinite states communicating processes based on an approximate analysis of channel contents by regular languages. Main team(s) involved: IRISA.
Difficulty: is to choose the right abstract domains and widening insuring convergence.

Supervisory Control of Infinite Symbolic Systems using Abstract Interpretation.
This work investigates the control of safety properties on infinite systems, modelled by transition system with data variables. Main team(s) involved: IRISA and on similar topics VERIMAG.
Difficulty: the main difficulty was to redefine the concept of controllability and to define synthesis algorithms based on symbolic transformations and abstract interpretation techniques so that we can ensure the convergence of the computations.

Analysis of Priced (Weighted) Timed Automata
Timed automata are a well-established formalism for the modeling and analysis of timed systems. Recently a very useful extension of timed automata has been proposed: priced (or weighted) timed automata. Priced timed automata are natural models for embedded systems where, often, resources consumptions have to be modeled. Priced timed automata extend classical timed automata with a cost function. Timed automata and priced timed automata are models for closed systems, where every transition is controlled. If we want to distinguish between actions of a controller and actions of an environment we have to consider timed games on those formalisms.
During the second year several partners have contributed with solutions to various optimization problems within this framework.

- Study of the cost-optimal reachability problem has been studied and its exact complexity settled (PSPACE-Complete).
- Optimal reachability problems (minimal and maximal costs for reaching a given goal situation) in the setting of multiple cost functions has been shown decidable using a notion of multi-priced zones.
- The open problem of model-checking timed automata augmented with costs has been shown to be undecidable in general; undecidability has been shown to hold even when restricting to priced timed automata with only three clocks.
- Similar timed games played on priced timed automata has been shown to be undecidable in general (again three clocks suffices).
- For priced timed automata with only one clock both the problem of computing optimal winning strategies as well as model checking has been shown decidable.

Main teams involved: Aalborg University, CVF and LSV-Chachan.

UPPAAL Cora: Optimal Scheduling and Planning
UPPAAL Cora is a branch of UPPAAL which allows for efficient analysis of cost-optimal reachability of priced timed automata. The original algorithm used a symbolic A* algorithm using so-called priced zones as main datastructure. It has been shown how the simple structure of the linear programs encountered during this symbolic A* algorithm can be exploited in order to substantially improve the performance of the current algorithm. The idea is rooted in duality of linear programs and we show that each encountered linear program can be reduced to the dual problem of an instance of the min-cost flow problem. Experimental results show a 70-80 percent performance gain. A framework for providing priced timed automata models scheduling problems is given as well as experimental results illustrating the potential competitiveness of our approach compared to existing approaches such as mixed integer linear programming. Main team involved Aalborg University.

Robustness issues for timed and hybrid automata
We have introduced a parametric semantics for timed controllers called the ASAP semantics. This semantics is a relaxation of the usual ASAP (ASAP stands for ``as soon as possible'') semantics (also called the maximal progress semantics) which is a mathematical idealization that can not be implemented by any physical device no matter how fast it is. On the contrary, any correct Almost ASAP controller can be implemented by a program on sufficiently fast hardware. We have studied the properties of this semantics and show how it can be analyzed

using the tool HyTech. Main team CVF, and triggered several cooperations and future work with LSV-Cachan.

Analysis of O-minimal Hybrid Systems
Recently, the control of hybrid systems has appeared as a new interesting and active field of research, and many results have already been obtained. O-minimal hybrid systems have been first proposed in as an interesting class of systems. They have very rich continuous dynamics, but limited discrete steps.
Several contribution have been made in this framework. First an encoding of trajectories with words has been proposed in order to prove the existence of finite bisimulations for o-minimal hybrid systems. We also study control of o-minimal hybrid games and prove that, under the assumption that the theory of the underlying o-minimal structure is decidable, the control problem can be solved and that winning states and winning strategies can be computed. Main team(s) involved: CVF, LSV-Cachan.

Refinement of abstraction for affine hybrid automata
In this research, we have shown how to automatically construct and refine rectangular abstractions of systems of linear differential equations. From a hybrid automaton whose dynamics are given by a system of linear differential equations, our method computes automatically a sequence of rectangular hybrid automata that are increasingly precise over-approximations of the original hybrid automaton. We have proved an optimality criterion for successive refinements. We also have shown that this method can take into account a safety property to be verified, refining only relevant parts of the state space. The practicability of the method is illustrated on a benchmark case study. Main team(s) involved: EPFL and CVF.

Development of an acceleration method suited for linear hybrid automata.
This method generalizes previous work on acceleration of integer-based systems, and provides a semi-algorithm for exploring the state-space of general linear hybrid automata, without abstracting away parts of the system or performing approximations. This method has been shown to be complete over the specific subclass of timed automata, but is also applicable to a much broader class of systems. Main team(s) involved: CVF.

UPPAAL Tiga: efficient synthesis of winning strategies for timed games
We have proposed a first efficient on-the-fly algorithm for solving games based on timed game automata with respect to reachability and safety properties. The algorithm we propose is a symbolic extension of the on-the-fly algorithm suggested by Liu & Smolka [LS98] for linear-time model-checking of finite-state systems. Being on-the-fly, the symbolic algorithm may terminate long before having explored the entire state-space. Also the individual steps of the algorithm are carried out efficiently by the use of so-called zones as the underlying data structure. Various optimizations of the basic symbolic algorithm are proposed as well as methods for obtaining time-optimal winning strategies (for reachability games). Extensive evaluation of an experimental implementation of the algorithm yields very encouraging performance results. On-going research include compact representation of winning strategies using symbolic datastructures such as BDDs and CDDs as well as their translation to executable control programs. Main team(s) involved: Aalborg with Nantes and input from LSV-Cachan.

Synthesis with incomplete information
In this research, we have proposed a fixed point theory to solve games of imperfect information. The fixed point theory is defined on the lattice of anti-chains of sets of states. Contrary to the classical solution proposed by Reif, our new solution does not involve determinization. As a consequence, it is readily applicable to classes of systems that do not admit determinization. Notable examples of such systems are timed and hybrid automata. As an application, we show that the discrete control problem for games of imperfect information

defined by rectangular automata is decidable. This result extends a result by Henzinger and Kopke.
This research has recently been extended to solve classical problems in automata theory for finite word languages. With this new method, inclusion between two nondeterministic automata can be solved much more efficiently than with previously known algorithms. The technique is currently extended to cope with Buechi automata (finite automata over infinite words). Main team(s) involved: CVF and EPFL.

Algorithms for the verification of infinite state systems
In this research, we propose an abstract interpretation based approach to solve the coverability problem of well-structured transition systems. Our approach distinguishes from other attempts in that (1) we solve this problem for the whole class of well-structured transition systems using a forward algorithm. So, our algorithm has to deal with possibly infinite downward closed sets. (2) Whereas other approaches have a non generic representation for downward closed sets of states, which turns out to be hard to devise in practice, we introduce a generic representation requiring no additional effort of implementation. Main team(s) involved: CVF and LIAFA.

Rectangular abstractions of hybrid automata
We showed how to automatically construct and refine rectangular abstractions of systems of linear differential equations. From a hybrid automaton whose dynamics are given by a system of linear differential equations, our method computes automatically a sequence of rectangular hybrid automata that are increasingly precise over-approximations of the original hybrid automaton. We proved an optimality criterion for successive refinements. We also showed that this method can take into account a safety property to be verified, refining only relevant parts of the state space. The practicability of the method was illustrated on a benchmark case study. Main team(s) involved: EPFL.

Quantitative similarity between timed systems
We defined quantitative similarity functions between timed transition systems that measure the degree of closeness of two systems as a real, in contrast to the traditional boolean yes/no approach to timed simulation and language inclusion. Two systems are close if for each timed trace of one system, there exists a corresponding timed trace in the other system with the same sequence of events and closely corresponding event timings. We showed that timed CTL is robust with respect to our quantitative version of bisimilarity, in particular, if a system satisfies a formula, then every close system satisfies a close formula. We also defined a discounted version of CTL over timed systems, which assigns to every CTL formula a real value that is obtained by discounting real time. We proved the robustness of discounted CTL by establishing that close states in the bisimilarity metric have close values for all discounted CTL formulas. Main team(s) involved: EPFL.

Logics for real-time games
We added freeze quantifiers to the game logic ATL in order to specify real-time objectives for games played on timed structures. We defined the semantics of the resulting logic TATL by restricting the players to physically meaningful strategies, which do not prevent time from diverging. We showed that TATL can be model checked over timed automaton games. We also specified timed optimization problems for physically meaningful strategies, and we showed that for timed automaton games, the optimal answers can be approximated to within any degree of precision. Main team(s) involved: EPFL.

Symbolic testing
Symbolic testing aims at the integration of action-based testing (or control-flow testing, or state-based testing) and data testing. This means that actions in a state-based model can be equipped with data-parameters, and that the sequences of allowed actions can be determined

by predicates over these data parameters. Currently these two approaches to testing are not integrated

The formalism of Symbolic Transition Systems (STS) has been defined to provide a well-defined basis for symbolic testing. A test generation algorithm for STS has been developed, and a very early prototype tool implementing this algorithm is available. Main team(s) involved: Nijmegen.

Difficulty: The main difficulty is finding finite representations of infinite objects, and lifting test generation algorithms to these representations.

Action refinement
The testing theory that was developed for testing communication protocols is message based: the test events are the sending or receiving of a message. Testing of component-based software systems is object based: the test events are method invocations, or, more precisely, method calls and method returns. This difference in granularity, or atomicity of test events hampers the application of communication protocol testing methods to component-based testing.

A theory of action refinement is being developed with particular application to testing, which should provide the theoretical foundations for comparing both approaches to testing, and which should make it possible to apply communication protocol testing methods to testing of component-based systems. Main team(s) involved: Nijmegen.

Difficulty: The general problem of action refinement and atomicity of actions was studied in the beginning of te 1990's, and turned out to be very hard. The challenge is to restrict this problem for the particular domain of model-based testing such that results can be obtained, which are applicable, among others, to testing of component-based systems.

A framework for test coverage semantics
A framework to express coverage measures that express how well a test suite covers such a specification.

Since testing is inherently incomplete, test selection has vital importance. Coverage measures evaluate the quality of a test suite and help the tester select test cases with maximal impact at minimum cost. Existing coverage criteria for test suites are usually defined in terms of syntactic characteristics of the implementation under test or its specification. Typical black-box coverage metrics are state and transition coverage of the specification. White-box testing often considers statement, condition and path coverage. A disadvantage of this syntactic approach is that different coverage figures are assigned to systems that are behaviorally equivalent, but syntactically different. Moreover, those coverage metrics do not take into account that certain failures are more severe than others, and that more testing effort should be devoted to uncover the most important bugs, while less critical system parts can be tested less thoroughly. This work introduces a semantic approach to black box test coverage. Our starting point is a weighted fault model (or WFM), which augments a specification by assigning a weight to each error that may occur in an implementation. We define a framework to express coverage measures that express how well a test suite covers such a specification, taking into account the error weight. Since our notions are semantic, they are insensitive to replacing a specification by one with equivalent behaviour. We present several algorithms that, given a certain minimality criterion, compute a minimal test suite with maximal coverage. These algorithms work on a syntactic representation of WFMs as fault automata. They are based on existing and novel optimization problems. Finally, we illustrate our approach by analyzing and comparing a number of test suites for a chat protocol. Main team(s) involved: Nijmegen.

Difficulty: The absence of semantic test coverage notions.

A testing theory for probabilistic processes
A first step in developing statistical testing techniques for systems with nondeterministic behavior.

We introduce a notion of finite testing, based on statistical hypothesis tests, via a variant of the well-known trace machine. Under this scenario, two processes are deemed observationally equivalent if they cannot be distinguished by any finite test. We consider processes modeled as image finite probabilistic automata and prove that our notion of observational equivalence coincides with the trace distribution equivalence proposed by Segala. Along the way, we give an explicit characterization of the set of probabilistic executions of an arbitrary probabilistic Automaton A and generalize the Approximation Induction Principle by defining an algebraic CPO structure on the set of trace distributions of A. We also prove limit and convex closure properties of trace distributions in an appropriate metric space. Main team(s) involved: Twente.

Difficulty: The infinite behavior of the probabilistic processes (including infinite branching and non-terminating runs), whereas the experiments on the trace distribution machine are of a finite character.

On-line testing of real-time systems
The online testing tool Uppaal-TRON 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. Future work includes tight integration with the UPPAAL graphical user interface. Main team(s) involved: Aalborg and related work at VERIMAG.

Quantitative Compositional Reasoning.
A framework for compositional reasoning about qualitative system properties.

Compositional reasoning about qualitative system properties. We present a compositional theory of system verification, where specifications assign real-numbered costs to systems. These costs can express a wide variety of quantitative system properties, such as resource consumption, price, or a measure of how well a system satisfies its specification. The theory supports the composition of systems and specifications, and the hiding of variables. Boolean refinement relations are replaced by real-numbered distances between descriptions of a system at different levels of detail. We show that the classical boolean rules for compositional reasoning have quantitative counterparts in our setting. While our general theory allows costs to be specified by arbitrary cost functions, we also consider a class of linear cost functions, which give rise to an instance of our framework where all operations are computable in polynomial time. Main team(s) involved: Twente.

Difficulty: Lack of compositionality in quantitative reasoning.

Checking robustness of timed automata.
An algorithm for robustness checking based on zones.

We propose a symbolic algorithm for the analysis of the robustness of timed automata, that is the correctness of the model in presence of small drifts on the clocks or imprecision in testing guards. This problem is known to be decidable with an algorithm based on detecting strongly

connected components on the region graph, which, for complexity reasons, is not effective in practice. Our symbolic algorithm is based on the standard algorithm for symbolic reachability analysis using zones to represent symbolic states and can then be easily integrated within tools for the verification of timed automata models. It relies on the computation of the stable zone of each cycle in a timed automaton. The stable zone is the largest set of states that can reach and be reached from itself through the cycle. To compute the robust reachable set, each stable zone that intersects the set of explored states has to be added to the set of states to be explored. Main team(s) involved: Twente.

Difficulty: The algorithm based on regions is not easily transformed to work on zones.

A Continuous-Time Bayesian Network Reliability Modeling, and Analysis Framework.
A framework for dynamic systems reliability modelling and analysis using continuous-time Bayesian networks.

We present a continuous-time Bayesian network (CTBN) framework for dynamic systems reliability modeling and analysis. Dynamic systems exhibit complex behaviors and interactions between their components; where not only the combination of failure events matters, but so does the sequence ordering of the failures. Similar to dynamic fault trees, the CTBN framework defines a set of basic BN constructs that capture well-defined system components behaviors and interactions. Combining, in a structured way, the various basic Bayesian network constructs enables the user to construct, in a modular and hierarchical fashion, the system model. Within the CTBN framework, one can perform various analyses, including reliability, sensitivity, and uncertainty analyses. All the analyses allow the user to obtain closed-form solutions. Main team(s) involved: Twente.

Difficulty: The application and contribution of temporal Bayesian Networks to the area of dependability analysis has been modest until now.

Synthesis and Stochastic Assessment of Cost-Optimal Schedules.
An alternative to the EPT approach to generate schedules that take the possible failures of resources into account.

We present a novel approach to synthesize good schedules for a class of scheduling problems that is slightly more general than certain existing scheduling problems. The idea is to prime the schedule synthesizer with stochastic information more meaningful than performance factors with the objective to minimize the expected cost caused by storage or delay. The priming information is obtained by stochastic simulation of the system environment. The generated schedules are assessed again by simulation. The approach is demonstrated by means of a non-trivial scheduling problem from lacquer production. The experimental results show that our approach achieves in all considered scenarios better results than the extended processing times approach. Main team(s) involved: Twente.

Difficulty: The interoperability of several different tools.

Reachability in priced probabilistic timed automata.
An algorithm for cost-bounded probabilistic reachability problem.

This work presents an algorithm for cost-bounded probabilistic reachability in timed automata extended with prices (on edges and locations) and discrete probabilistic branching. The algorithm determines whether the probability to reach a (set of) goal location(s) within a given price bound (and time bound) can exceed a threshold p in [0,1]. We prove that the algorithm is

partially correct and show an example for which termination cannot be guaranteed. Main team(s) involved: Twente.

Diffuclty: The symbolic state space is not guaranteed to be finite.

State identification problems for finite-state transducers
The problems of state identification have been well studied for models such as Mealy machines where inputs and outputs are synchronous, or at least have a one-to-one correspondence. Real-time models such as I/O timed automata, on the other hand, can be often abstracted by finite-state transducers, where inputs and outputs are asynchronous.
We studied state-identification problems for such models and provided initial results. Main team(s) involved: VERIMAG..

Conformance testing for real-time systems
We studied different properties of the conformance relation tioco used in the model-based testing framework for real-time systems used in the tool TTG (timed test generator). In particular under which conditions the relation is compositional (i.e., A conforms to A' and B conforms to B' implies that the parallel composition of A and B conforms to the composition of A' and B'). We also compared tioco with other real-time testing conformance relations proposed in the literature. Main team(s) involved: VERIMAG and related work at Aalborg.

Decentralized observation problems
A fundamental observation problem is, given a model of the system to be observed and a specification of the property to be observed, to check whether the property is observable (i.e., the observer can resolve potential ambiguities due to partial observation capabilities) and if so to (automatically) synthesize an observer. We studied this problem in various decentralized settings (i.e., where there are more than on observers) and provided decidability and undecidability results. Main team(s) involved: VERIMAG.

Generating Path Conditions for Timed Systems
We provide an automatic method for calculating the path condition for programs with real time constraints. This method can be used for the semiautomatic verification of a unit of code in isolation, i.e., without providing the exact values of parameters with which it is called. Our method can also be used for the automatic generation of test cases for unit testing. The current generalization of the calculation of path condition for the timed case turns out to be quite tricky, since not only the selected path contributes to the path condition, but also the timing constraints of alternative choices in the code. Main team(s) involved: VERIMAG.

Allen Linear (Interval) Temporal Logic
Translation to LTL and Monitor Synthesis: We show how Allen's logic can be translated to LTL and how to synthesize automatically monitors for specifications in this logic. Main team(s) involved: VERIMAG.

Product Lines
Families of embedded discrete finite state programs are modeled using input-enabled alternating transition systems. One model describes all functionality, while each variant is defined by an environment, describing its possible uses. The environments show both the inputs that a system can receive and indicate which of the system's responses are relevant for the environment. The latter trait, called color-blindness, creates new possibilities for system transformations in the specialization process. We demonstrate the use of the framework by applying it to two classes of realistic design languages. Main team(s) involved: Aalborg.

Compositional Verification Using I/O-Automata
We propose a new look at one of the most fundamental types of behavioral interfaces: discrete time specifications of communication—directly related to the work of de Alfaro and Henzinger. Our framework is concerned with distributed non-blocking asynchronous systems in the style of Lynch's I/O-automata, relying on a context dependent notion of refinement based on relativized language inclusion. There are two main contributions of the work. First, we explicitly separate assumptions from guarantees, increasing the modeling power of the specification language. Second, our composition operator is systematically and formally derived from the requirements stated as a system of inequalities. The derived composed interfaces are maximal in the sense of behavior, or equivalently are the weakest in the sense of assumptions. We present a method for solving systems of relativized inequalities as used in our setup. Finally we draw a formal correspondence between Interface Input/Output Automata and Interface Automata. Main team(s) involved: Aalborg.

2.2.2 Publications Resulting from these Achievements

Pavel Krcál and Wang Yi : Communicating Timed Automata: The More Synchronous, the More Difficult to Verify., CAV 2006: 249-262.

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).

C. Constant, T. Jéron, H. Marchand, V. Rusu, Combinaison entre vérification et test pour la validation de systèmes réactifs, in Traité I2C. Systèmes Temps Réel: Techniques de Description et de Vérification - Théorie et Outils, Volume 1, Chapter 2, Pages 59-88,, Hermès Science, 2006. (more)

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

T. Jéron, H. Marchand, V. Rusu, Symbolic Determinisation of Extended Automata, in 4th IFIP International Conference on Theoretical Computer Science, Stantiago, Chile, August 2006.

T. Le Gall, B. Jeannet, T. Jéron, Verification of Communication Protocols using Abstract Interpretation of FIFO queues, in 11th International Conference on Algebraic Methodology and Software Technology, AMAST '06, Kuressaare, Estonia, Michael Johnson, Varmo Vene (eds.), July 2006.

T. Le Gall, B. Jeannet, H. Marchand, Supervisory Control of Infinite Symbolic Systems using Abstract Interpretation, in 44nd IEEE Conference on Decision and Control (CDC'05) and Control and European Control Conference ECC 2005, Pages 31-35, Seville (Spain), December 2005.

Bernard Boigelot (CFV-ULg) and Frédéric Herbreteau, The Power of Hybrid Acceleration,In Proc. CAV 2006, Lecture Notes in Computer Science,volume 4144, pp. 438--451, Springer-Verlag.

B. Thomas Adler, L. de Alfaro, L. Dias Da Silva, M. Faella, A. Legay (CFV-ULg), V. Raman, P. Roy. Ticc: A Tool for Interface Compatibility and Composition. Proc. 18th International Conference on Computer-Aided Verification, volume 4144, Lecture Notes in Computer Science, pages 59-62, Seattle, August 2006, Springer-Verlag.

Alain Finkel (ENS Cachan), Gilles Geeraerts (CFV-ULB), Jean-François Raskin (CFV-ULB), Laurent Van Begin (CFV-ULB), On the omega-language expressive power of extended Petri nets. in Theoretical Computer Science, volume 356(3), pp 374-386, Elsevier. 2006.

Gilles Geeraerts (CFV-ULB), Jean-François Raskin (CFV-ULB), Laurent Van Begin (CFV-ULB), Expand, Enlarge and Check: new algorithms for the coverability problem of WSTS (extended version). Journal of Computer and System Sciences, volume 72(1), pp 180-203, Elsevier. 2005.

P. Aziz Abdulla, A. Legay, J. d'Orso, A. Rezine. Tree Regular Model Checking: A Simulation-Based Approach. Volume 69 of Journal of Logic and Algebraic Programming 2006, pages 92-121.

Véronique Bruyère (CFV-UMH), Jean-François Raskin (CFV-ULB), Real-Time Model-Checking: Parameters Everywhere (extended version). Accepted for publication in International Journal of Logical Methods in Computer Science. 2006.

Nicolas Markey (LSV), Jean-François Raskin (CFV-ULB), Model Checking Restricted Sets of Timed Paths. to appear in Theoretical Computer Science, Elsevier Sciences. 2005.

Krsihnendu Chatterjee (UCBerkeley), Laurent Doyen (CFV-ULB), Thomas Henzinger (EPFL), Jean-François Raskin (CFV-ULB), Algorithms for Omega-Regular games with Incomplete Information. in Proc. CSL06. LNCS. Springer. 2006.

Jean-François Raskin (CFV-ULB), An Introduction to Hybrid Automata. Handbook of Networked and Embedded Control System. pp 491-518, Dimitros Hristu-Varsakelis, William S. Levine (Eds.), Birkhauser, Spring. 2005.

Gilles Geeraerts (CFV-ULB), Jean-François Raskin (CFV-ULB), Laurent Van Begin (CFV-ULB), Well-structured languages. Submitted. 2006.

Martin De Wulf (CFV-ULB), Laurent Doyen (CFV-ULB), Jean-François Raskin (CFV-ULB), Antichains: a new Algorithm for Checking Universality of Finite Automata. in Proc. CAV06. LNCS 4144. Springer. 2006.

Patricia Bouyer (LSV), Thomas Brihaye (CFV-UMH), Véronique Bruyère (CFV-UMH), Jean-François Raskin (CFV-ULB), On the optimal reachability problem. Accepted in Formal Methods in System Design. 2006.

Thomas Brihaye (CFV-UMH), A note on the undecidability of the reachability problem for o-minimal dynamical systems. Mathematical Logic Quaterly, 52, no. 2, 165--170. 2006.

Patricia Bouyer (LSV), Thomas Brihaye (CFV-UMH), Fabrice Chevalier (LSV), Control in o-minimal hybrid systems. accepted in LICS'06. 2006.

Patricia Bouyer (LSV), Thomas Brihaye (CFV-UMH), Nicolas Markey (LSV), Improved Undecidability Results on Priced Timed Automata. Information Processing letters, 98, no. 5, 188--194. 2006.

Thomas Brihaye (CFV-UMH), Véronique Bruyère (CFV-UMH), Jean-François Raskin (CFV-ULB), On Model-Checking Timed Automata with Stopwatch Observers. Information and Computation 2004, no. 3, 408--433. 2006.

Alexandre Genon (CFV-ULB), Thierry Massart (CFV-ULB), Cédric Meuter (CFV-ULB), Monitoring Distributed Controllers : When an Efficient LTL Algorithm on Sequences is Needed to Model-Check Traces. In proc. FM 2006. LNCS 4085. Springer. 2006.

Martin De Wulf (CFV-ULB), Laurent Doyen (CFV-ULB), Jean-François Raskin (CFV-ULB), A Lattice Theory for Solving Games of Imperfect Information (Extended Version). In proc. HSCC 06. LNCS 3927. Spriner. 2006.

Pierre Ganty (CFV-ULB), Jean-François Raskin (CFV-ULB), Laurent Van Begin (CFV-ULB), A Complete Abstract Interpretation Framework for Coverability Properties of WSTS. In proc. VMCAI 06. LNCS 3855. Springer. 2006.

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.

Bernard Boigelot (CFV-ULg), Sébastien Jodogne (CFV-ULg), On the use of weak automata for deciding linear artihmetic with integer and real variables. In ACM transactions on Computational Logic. 2005.

Laurent Doyen, Thomas A. Henzinger, and Jean-Francois Raskin, Automatic rectangular refinement of affine hybrid systems, Proceedings of the Third International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS), Lecture Notes in Computer Science 3829, Springer, 2005, pp. 144-161.

Thomas A. Henzinger, Rupak Majumdar, and Vinayak Prabhu, Quantifying similarities between timed systems, Proceedings of the Third International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS), Lecture Notes in Computer Science 3829, Springer, 2005, pp. 226-241.

Thomas A. Henzinger and Vinayak Prabhu, Timed alternating-time temporal logic, Proceedings of the Fourth International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS), Lecture Notes in Computer Science, Springer, 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.

M. van der Bijl, A. Rensink, J. Tretmans. Action Refinement in Conformance Testing.In: F. Khendek, R. Dssouli (eds.),TestCom 2005 - Testing of Communicating Systems 17,Lecture Notes in Computer Science 3502, pp. 81-96,Springer-Verlag, 2005.

T. Willemse. Heuristics for ioco-based test-based modelling (extended abstract).In L. Brim and M. Leucker (eds.),11th Int. Workshop on Formal Methods for Industrial Critical SystemsFMICS/PDMC 2006.Lecture Notes in Computer Science. Springer-Verlag, 2006. To appear.

J. Tretmans.Model Based Testing with Labelled Transition Systems.Chapter of book on Formal testing, H. Hierons (editor). Springer, 2006. To Appear.

E. Brinksma, M.I.A. Stoelinga and L. Brandán Briones. A Semantic Framework for Test Coverage. Technical Report TR-CTIT-06-24, 2006 An extended abstract has been accepted for publication at ATVA'06.

L. Cheung and M.I.A. Stoelinga and F.W. Vaandrager. A Testing Scenario for Probabilistic Processes . Technical Report ICIS-R06002. 2006. (Submitted for publication.)

K. Chatterjee, L. de Alfaro, M. Faella, T. A. Henzinger, R. Majumdar and M.I.A. Stoelinga Quantitative Compositional Reasoning. To appear in Proceedings of QEST'06

Conrado Daws, Piotr Kordy.Symbolic Robustness Analysis of Timed Automata. To appear in FORMATS 2006.

H. Boudali, J. B. Dugan. A continuous-time Bayesian network reliability modeling and analysis framework. IEEE Transaction on Reliability, vol. 55(1):86-97, March 2006.

Mader, A.H. and Bohnenkamp, H.C. and Usenko, Y.S. and Jansen, D.N. and Hurink, J.L. and Hermanns, H. (2006) Synthesis and Stochastic Assessment of Cost-Optimal Schedules. Technical Report TR-CTIT-06-14 Centre for Telematics and Information Technology, University of Twente, Enschede. ISSN 1381-3625.

Berendsen, J. and Jansen, D.N. and Katoen, J.P. (2006) Probably on Time and within Budget: On Reachability in Priced Probabilistic Timed Automata. Technical Report TR-CTIT-06-26 Centre for Telematics and Information Technology, University of Twente, Enschede. ISSN 1381-3625.

Kim G. Larsen, Jacob I. Ramsmussen: Optimal Reachability for Multi-Priced Timed Automata. Accepted for publication in Journal of Theoretical Computer Science.

Kim Guldstrand Larsen, Ulrik Nyman, Andrzej Wasowski: Interface Input/Output Automata. In proceedings of Formal Methods 2006.

Kim Guldstrand Larsen, Ulrik Larsen, Andrzej Wasowski: Color-Blind Specifications for Transformations of Reactive Synchronous Programs. FASE 2005: 160-174

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

Henrik Schioler, Jan Jessen, Jens Dalsgaard, Kim Guldstrand Larsen: Network Calculus for Real Time Analysis of Embedded Systems with Cyclic Task Dependencies. Computers and Their Applications 2005: 326-332

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.

Kim Guldstrand Larsen, Jacob Illum Rasmussen: Optimal Conditional Reachability for Multi-priced Timed Automata. FoSSaCS 2005.

Gerd Behrmann, Kim Guldstrand Larsen, Jacob Illum Rasmussen: Beyond Liveness: Efficient Parameter Synthesis for Time Bounded Liveness. FORMATS 2005.

Patricia Bouyer, Franck Cassez, Emmanuel Fleury, Kim Guldstrand Larsen: Synthesis of Optimal Strategies Using HyTech. Proceedings of the Workshop on Games in Design and Verification. Electr. Notes Theor. Comput. Sci. 119(1): 11-31 (2005)

Gregorio Díaz, Kim Guldstrand Larsen, Juan José Pardo, Fernando Cuartero, Valentin Valero: An approach to handle real time and probabilistic behaviors in e-commerce: validating the SET protocol. SAC 2005: 815-820

Gerd Behrmann, Kim Guldstrand Larsen, Jacob Illum Rasmussen: Optimal scheduling using priced timed automata. SIGMETRICS Performance Evaluation Review 32(4): 34-40 (2005)

Sebastian Kupferschmid, Jörg Hoffmann, Henning Dierks, Gerd Behrmann: Adapting an AI Planning Heuristic for Directed Model Checking. SPIN 2006: 35-52

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

J. I. Rasmussen and K. G. Larsen a K. Subramani**:** Cost-Optimal Scheduling Using Priced Timed Automata. Accepted for publication in Formal Methods in System Design, 2006.

Alexandre David, John Håkansson, Kim G. Larsen and Paul Pettersson: Model Checking Timed Automata with Priorities using DBM Subtraction. To appear in proceedings of FORMATS 2006.

P. Bouyer, K. G. Larsen, N. Markey, J. I. Rasmussen: Almost Optimal Strategies in One Clock Priced Timed Automata. To appear in proceedings of FSTTCS 2006.

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.

Kim G. Larsen, Ulrik Nyman, Andrzej Wasowski: Modelling Software Product Lines using Color-blind Transition Systems. To appear in Software Tools for Technology Transfer.

Kim G. Larsen, Ulrik Nyman, Andrzej Wasowski. Interface Input/Output Automata: Splitting Assumptions from Guarantees. In: Foundations of Interface Technologies (FIT 2005), affiliated workshop of CONCUR 2005. San Francisco, CA, USA, August 20, 2005. Preliminary Proceedings.

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

ACM Kanellakis 2005 Theory and Practice Award G. Holzmann, R. Kurshan, M. Vardi, and P. Wolper (CFV-ULg) received the ACM Kanellakis 2005 Theory and Practice award for their work on softaware and hardware verification.

LICS 2006 "Test of time" Award M. Vardi and P. Wolper (CFV-ULg) received the LICS 2006 "Test of time" award for their 1986 paper "An automata-theoretic approach to automatic program verification.

Workshop FORMATS 2005. Paul Pettersson and Wang Yi organized and chaired FORMATS 2005. Uppsala, Sweden, September 29 - October 2, 2005.

Workshop FORMATS 2006. Patricia Bouyer and Eugene Assarine organized and chaired FORMATS 2006, Paris, September 2006.

Tutorial ARTIST2/China Spring school on Embedded Systems Design. Wang Yi lectured in Xian, China, April 4 - 17, 2006.

Summerschool ARTIST2 Summer School on Components & Modelling, Testing & Verification, and Static Analysis of Embedded Systems. T. Jéron, Test Generation using Model-Checking, Nässlingen, Sweden, September 29 - October 2, 2005. http://www.artist-embedded.org/FP6/ARTIST2Events/SummerSchools/Artist05.html

Summerschool ARTIST2 Summer School on Components & Modelling, Testing & Verification, and Static Analysis of Embedded Systems. Gerd Behrmann: Real-Time Verification using UPPAAL, Nässlingen, Sweden, September 29 - October 2, 2005. http://www.artist-embedded.org/FP6/ARTIST2Events/SummerSchools/Artist05.html

Summerschool ARTIST2 Summer School on Components & Modelling, Testing & Verification, and Static Analysis of Embedded Systems. Brian Nielsen, Off- and On-lien testing of Real-Time Systems. Nässlingen, Sweden, September 29 - October 2, 2005. http://www.artist-embedded.org/FP6/ARTIST2Events/SummerSchools/Artist05.html

Keynote in DGA (French Army) Seminar on "Operational challenges in modelling of complex software systems", Toulouse, Nov. 2006. T. Jéron, Testing and test selection

Spring School in IPA Lentedagen on Testing. V. Rusu, Combining formal verification and conformance testing, Landgoed Huize Bergen, Vught, April 19-21 2006 http://www.win.tue.nl/ipa/activities/springdays2006/index.html.

Summerschool ARTIST2 Summer School on Components & Modelling, Testing & Verification, and Static Analysis of Embedded Systems. JF Raskin (speaker), Timed Controller Synthesis: Robustness Issues, Nässlingen, Swenden, September 2005.

Summerschool MOVEP'06. JF Raskin (speaker), Timed Controller Synthesis: Robustness Issues, MOVEP'06, Bordeaux, France, June 2006.

Invited speaker at workshop "Coopreation of Decution Tools". B. Boigelot, ,Nancy, France, April 10th 2006.

Keynote at MMB: 13th GI/ITG Conference on Measurement, Modeling, and Evaluation of Computer and Communication Systems J. Tretmans: Model Based Testing: An Attempt to Combine Provable Soundness and Effective Automation and Industrial Applicability. Nurnberg (D), March 27-29 2006. http://www.mmb2006.org/programme.html.

Tutorial at the IPA Lentedagen on Testing, Vught (NL), April 19-21 2006. Jan Tretmans: Introduction to model-based testing**.** http://www.win.tue.nl/ipa/activities/springdays2006

Tutorial at "Testnet Thema Avond", June 8 2006, Nieuwegein (NL). J. Tretmans. Model-Based Testing http://www.testnet.org/Produktie/Bibliotheek/Presentaties.html.

Keynote: Invited talk at workshop on "Games in design and verification" Edinburgh, June 13 2005 (co-located with CAV05). M.I.A. Stoelinga.

Workshop: Dutch National Testing Day. E. Brinksma and M.I.A. Stoelinga (eds). Proceedings of 11th Dutch Testing Day November 11, Enschede, the Netherlands.

Workshop: Workshop on Foundations of Interface Technologies H. Hermanns and J. Rehof and M.I.A. Stoelinga (eds). Proceedings of First Workshop on Foundations of Interface Technologies August 28, San Francisco, USA.

Tutorial at RTSS2005. 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 December 5-8, 2005 Miami, Florida, USA. http://www.rtss.org/rtss2005.

Summerschool: International PhD School on Verification of Protocols for Security and Mobility, IT-University, Copenhagen, Denmark, October 9-13, 2006. Gerd Behrmann and Kim G. Larsen: Real Time Validation of Embedded Systems Using UPPAAL. http://first.dk/VPSM.

Summerschool ARTES. Kim G. Larsen *Controller Synthesis for Real Time Systems.* Nässlingen, Sweden, August 21-25 2006. http://www.artes.uu.se/events/summer06/

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

Summerschool GLOBAN: The global computing approach to analysis of systems. Kim G. Larsen: Model Checking. DTU, Lyngby, Denmark, August 21-25, 2006. http://www2.imm.dtu.dk/GLOBAN/.

3. Future Work and Evolution

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

As mentioned in the introduction the long-term ambition of the Testing and Verification cluster is to improve current industrial practice by continuous dissemination and improvement of existing powerful testing and verification techniques. Within the Quantitative Testing and Verification activity our aim to provide modelling formalisms, methods and tools which will allow *quantitative* aspects to be dealt with and utilized for verification and performance analysis at early design stages as well as for systematic approaches to the testing phase.

The planned work includes continuation of metrics for testing coverage, abstraction methods and compositional methods allowing properties of a composite system to be inferred from those of its components.

Also, based on existing powerful (real-time) verification techniques the new research challenges identified within the second year will be continued in the next period. This includes work towards maturing and further development of important topics such as optimal scheduling, monitoring and fault diagnosis, controller synthesis, robustness and implementability of quantitative models and analysis of hybrid models, stochastic and timed models.

The theoretical work will be supplemented by experimental work on tool prototypes and case studies.

In somewhat more detail we expect to tackle the following problems during the next 18 months:

Verification:

- Systematic construction of verification models for embedded systems
- Implementation of robust model-checking algorithms for real-time systems.
- Development of efficient symbolic representations for arithmetic sets.
- Study of the properties of automata-based symbolic representations of sets of integer and real vectors (Real Vector Automata, RVA).
- Development of efficient methods for iterating transducers.
- UPPAAL with asynchronous communication
- Implementation of zone-based verification engine for probabilistic timed automata.

Testing:

- Establishing a relation between (ioco) testing theory and assume/guarantee frameworks
- Symbolic test selection using coverage criteria and incorporating a technique for test-data selection.
- Application of work on coverage metrics to realistic case studies
- Testing theory and test selection for recursive programs.
- Test-based modeling, i.e. a model is inferred from test observations.
- Continued development of the test generation tools UPPAAL Tron,TTG, and TorX.

Abstraction and approximate methods:

- Approximate methods for verification of timed systems, in particular systems with buffers for asynchronous communication and resource sharing.
- Methods for automatic abstraction refinement for hybrid and probabilistic systems

Compositionality:

- Compatability checking between timed interfaces.

- Compositional backwards reachability methods for timed systems.

Robustness and implementability;

- Identification of tractable, robust models of quantitative systems, possibly based on theory of continuity and discounting.
- Code synthesis from timed models to executable code.

Controller synthesis and optimal scheduling

- Generation of compact code from winning strategies for timed games using symbolic datastructures.
- Efficient algorithms for synthesis of winning strategies for timed games with incomplete information
- Continued development of UPPAAL Tiga
- Revisit the automata theoretic approach to model-checking in the light of the research done on synthesis for incomplete information.
- Further developments on synthesis of robust controllers (incomplete information)

Priced / Weighted Timed automata

- Efficient algorithms dealing with multi-priced models
- Efficient algorithms for optimal infinite schedules.
- Continued development of UPPAAL Cora
- Optimal stategies for priced timed game automata with two clocks.

3.2 Current and Future Milestones

(achieved) Year1: Initial results for testing and verification with emphasis on quantitative aspects

(achieved) Year2: Develop theory, methods and tools for testing and verification of embedded systems with emphasis on quantitative aspects (e.g. real-time and stochastic phenomena) that are of particular importance for the correctness of embedded systems. Further work on robustness, metrics and abstraction. Also collect and classify major case studies.

Year3: **Development of algorithms and implementation of tools for optimal controller synthesis, robust model checking, coverage-based test selection and code generation.** Existing verification tools and test generation tools are more strongly connected, including stronger links between academic and industrial tools.

Year4: **Development of generic framework using abstraction and compositionality for efficient analysis of quantitative models.** Emergence of a range of new powerful debugging and analysis based on various combinations of testing and verification techniques.

3.3 Indicators for Integration

During the second year several partners (Aalborg, LSV Cachan, CVF, Twente) have been working (often in collaboration) towards completing the theoretical foundation for priced timed automata settling decidability for various decision problems.

Work on observability/monitoring, fault tolerance and controller synthesis has been conducted by several partners (Verimag, LSV Cachan, Aalborg, CVF, EPFL) often with joint publications as result.

The work on robustness has been done by several partners (Twente, Uppsala, CVF, LSV Chachan, EPFL) following different and competing approaches.

Symbolic techniques for on-and off-line testing has been considered by several partners dealing with different sources of infinite-state behaviour such as real-time (Aaalborg, Verimag, Uppsala) and data (IRISA, Nijmegen).

The UPPAAL verification tool and its variants for optimal scheduling – UPPAAL Cora – and controller synthesis – UPPAAL Tron – are widely used by several other partners.

Piotr Kordy took his MSc from Aalborg University and has been recruited as a PhD student at Twente University. Also Thomas Chatain finishes his PhD from IRISA and has been imployed as post-doc at Aalborg University.

In addition the following visits between partners has been recorded:

- From CFV (Brussels) to EPFL (Henzinger) (three visits: three months, one week-one, week, by Doyen and Raskin)
- From CFV (Brussels) to ENS Cachan (Finkel-Bouyer-Markey) by Raskin, twice one week.
- From ENS Cachan to CFV (Brussels), Bardin, three months.
- From CFV (Brussels) to LIAFA (Bouajjani), L. Van Begin was one year as an ATER in LIAFA.
- From CFV (Brussels) to Uppsala University August, 4th to August, 13th 2005: visit to Prof. Parosh Aziz Abdulla and Mr Johann Deneux.
- From CFV (Mons) to ENS-Cachan: visit by T. Brihaye.
- From CFV (Liège) to University of Twente: six week visit by A. Legay.
- From Aalborg to Cachan: Kim G. Larsen and Jacob I Rasmussen (2 times 1 week)
- From LSV Cachan to Aalborg: Nicola Marcy , Patricia Bouyer (1 week)
- From Aalborg to Brno: Gerd Behrmann (1 week)
- From Brno to Aalborg: Jiri Simsa (3 months) and Jiri Barnat (2 weeks)
- From Uppsala to Aalborg: Anders Hessel (1 day)
- Participation in Scandinavian ARTIST2 day, Stockholm (Kim G Larsen)
- Contribution to ARTES summerschool (held by Uppsala).

3.4 Main Funding

Various national funds 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: ParaDice.
- Danish national project MoDES
- French national project ACI CORTOS: Control and Observation of Real-Time Open Systems

3.5 Internal Reviewers for this Deliverable

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