IST-004527 ARTIST2
Network of Excellence
on Embedded Systems Design

Activity Progress Report for Year 3

JPRA-NoE Integration

Quantitative Testing and Verification

Cluster:

Testing and Verification

Activity Leader:

Professor Ed Brinksma (University of Twente, Embedded Systems Institute)
http://wwwhome.cs.utwente.nl/~brinksma/

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 ARTIST Participants 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 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:

- The successful application of the STREP proposal *Quasimodo* marks a significant collaboration between several partners of the cluster (Aalborg, Twente, CFV, LSV). Also a number of teams affiliated with the cluster are partners in the proposal (Aachen, Saarlandes, ESI, Nijmegen).
- 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 continuously collaborated on the development of the tool UPPAAL in parallel with the development of Kronos at Verimag. In particular the collaboration has lead to a spin-off company (preliminary named UPPAAL International).
- LSV, Aalborg and Twente are collaborating on problems related to optimal control and scheduling for real-time systems.
- CVF and Aalborg have been collaborating on controller synthesis for real-time systems under partial observability.
- 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

- Collaboration between LSV and LIAFA on symbolic methods for quantitative verification

1.5 Problems Tackled in Year 3

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 is 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 objectives for the 18 months period September 2006 until February 2008 included 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 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 has been planned.

In more detail the following problems has been dealt with during the 18 months period (following closely the milestones of the 18 months period – see seciton 3.2 for more information):

Verification

- improved state space exploration algorithms for timed automata using heuristics from AI, randomized search as well as abstraction-refinement technique.
- Deadlock detection and verification in BIP
- open-source library of Difference-Bound Matrix datastructure (DBM) for timed automata analysis
- Extending Difference-Bound Matrices with disequality constraint.

Testing

- test case generation techniques from symbolic specifications and interprocedural specifications.
- Off-line generation of testing strategies using algorithmic framework for timed games.
- Test case generation for ultimately periodic paths.
- Conformance testing framework for hybrid systems.

Compositionality

- for dynamic fault tree analysis
- An interface theory based on modal transition systems
- synthesis of interfaces from code

Abstraction and Approximate Analysis

- Event stream abstraction from timed automata models with application to schedulability analysis.
- Fixed point based abstraction refinement
- Counter Example Guided Abstraction Refinement for Timed Automata (implemented based on UPPAAL).
- acceleration method for linear hybrid systems
- convex hull and iteration techniques for infinite state systems.

Robustness and Implementability

- symbolic algorithms for efficient analysis of robustness (i.e. reachability unaffected by small perturbance).

Controller Synthesis and Optimal Scheduling

Numerous results within these areas have been achieved during the last year and from from several groups. The contributions include both several important theoretical results (settling the boundary between undecidability and decidability) as well as truly significant algorithmic advances in tool performance. For untimed systems the main results are:

- controller synthesis wrt LTL or non-deterministic Büchi conditions as winning objectives.
- synthesis of concurrent controllers
- synthesis of observations-based strategies

For timed systems important results concerning controller synthesis are:

- The tool UPPALA Tiga is now a completely integrated extension of UPPAAL allowing the full modeling formalism including discrete datastructures (arrays and records) as well as userdefined datatypes and functions. The tool support synthesisof winning strategies with respect to safety as well as liveness objectives. Strategies are represented and availiable in compact form as CDD/BDD.
- synthesis and model checking wrt TATL
- Controller synthesis for timed games under partial observability.
- Use of timed controller synthesis for testing, refinement and equivalence checking
- Industrial application (climate control) with support for automatic conversion of winning strategies produced by UPPAAL Tiga into S-functions to be used for further performance evaluation (using simulation) in Simulink.

Priced Timed Automata & Quantitative Models

- Stochastic extensions with semidecision procedure for optimal cost-bounded reachability.
- a line of undecidability results of model checking and optimal strategies in setting of more than 3 clocks.
- decidability results of model checking and optimal strategies when restricting to only one clock.
- compositional, real-valued specification framework (i.e. a system satisfies a specification to a certain quantifaible degree).

1.6 Comments From Year 2 Review

1.6.1 Reviewers' Comments

For this activity there have been no particular comments.

1.6.2 How These Have Been Addressed

Since there were no specific comments, we did not take specific measures.

2. Summary of Activity Progress

2.1 Previous Work in Year 1

Work carried out in the first months include:

- The Vertecs team of INRIA has worked 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 has been a new formalisation of symbolic test generation and a combination of verification and testing for safety properties.
- 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 including 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 Previous Work in Year 2

Short summary of work carried out in the second year:

- We hve released UPPAAL 4.0 being the result of over two and half years of development and contains many new 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
- 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 have presented an algorithm for inferring a timed-automaton model of a system from information obtained by observing its external behavior. In this work, the full class of event-recording automata has been considered.

- We have worked on symbolic test selection for extended automata using abstract interpretation.
- We have worked on symbolic Determinisation of Extended Automata.
- We have implemented tool support for off-line test generation for real-time systems in UPPAAL Cover and UPPAAL Tron and applied it to 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 have worked on conformance testing of programs with floating point numbers with respect to its specification with real numbers.
- We have worked on black-box testing of cryptographic protocols, using a compositional approach for checking secrecy and authenticity properties of cryptographic protocols integrating ideas from verification, conformance testing, and learning, with application to biometric passports.
- Work on verification of communication protocols using abstractiInterpretation of FIFO queues.
- Work on supervisory control of infinite symbolic systems using abstract interpretation.
- We have worked on analysis of priced (Weighted) timed automata, in particular settling decidability of optimal reachability in presence of multi cost functions and proved undecidability of model checking and optimal control in general (for priced timed automata with 3 or more clocks)
- We have worked on efficient implementation of cost-optimal reachability for priced timed automata using a symbolic A* algorithm in UPPAAL Cora.
- Work on robustness issues for timed and hybrid automata by introduction of a parametric semantics for timed controllers called the ASAP semantics.
- We have worked on analysis of O-minimal Hybrid Systems, refinement of abstraction for affine hybrid automata and development of an acceleration method suited for linear hybrid automata.
- We have developed and implemented an efficient on-the-fly algorithm for solving timed games wrt reachability and safety propertis. The implementation is available in the tool UPPAAL Tiga.
- For finite games we have proposed a fixed point theory of anti-chains to efficiently solve games of imperfect information.
- We have proposed algorithms for the verification of infinite state systems including rectangular abstrqctions of hybrid automata.
- We haved defined Quantitative similarity between timed systems and proposed logics for real-time games allowing to specify objectives.
- We have defined the formalism of Symbolic Transition Systems (STS) in order to support testing of systems with data. Also to support testing of communication protocls a testing theory allowing for action refinement was proposed.
- We have developed a framework for test coverage semantics as well as a testing theory for probabilistic processes.

- We have developed on-line testing of real-time systems in the tool UPPAAL Tron as well as a theory for conformance testing for real-time systems as used in the tool TTG.
- We have developed a framework for compositional reasoning about qualitatitve system properties.
- We have proposed 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.
- We have presented a novel approach to synthesize good schedules for a class of scheduling problems that is slightly more general than certain existing scheduling problems.
- We have presented an (semi-decision procedure) algorithm for cost-bounded probabilistic reachability problem.
- We have studied the state identification problems for finite-state transducers, and the fundamental observation problem of decentralized observation.'
- We have provided 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.
- We have showed how Allen's logic can be translated to LTL and how to synthesize automatically monitors for specifications in this logic.
- We have developed a framework for development and validation of product lines. In the approach 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.
- We have worked on compositional verification using I/O-Automata

2.3 Current Results

2.3.1 Technical Achievements

TWENTE

Compositional Analysis of Dynamic Fault Trees

Dynamic Fault Trees (DFT) is a common, versatile and graphical formalism to specify and analyze system reliability; a DFT specifies how the components' failures impact the system failure. We have tackled two important problems (1) we have given a formal semantics for DFTs, thus providing a rigourous basis for DFT analysis and tool development. (2) We have developed compositional analysis techniques for DFTs, which are an important means to aleviate the state spaceexplosion problem.

Metric for stochastic games

We have developed equivalence relations and metrics for concurrent, stochastic games. Stochastic games are important paradigm in computer science, eg for modeling the interactions between various agents or components. The equivalences we developed allow to combat the state space exposion problem by grouping together equivalent states. Our metrics

provide a formal definition of what is means that one game is very similar to another one and they allow us to do approximate analysis on games.

Robustness analysis for timed automa
We have proposed 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

Time and cost bounded reachability in probabilistic timed automata
We developed 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 probaility p in [0, 1]. The algorithm is partial in the sense that termination cannot be guaranteed.

Quantative reasoning frameworks
We developed a framework for quantitative reasoning about quantitative systems. More precisely, we developed quantitative logics and quantitative refinement relations and showed their connections.

Aalborg

Controller Synthesis for Timed Games
In 2005 we proposed the first efficient on-the-fly algorithm for solving games based on timed game automata with respect to reachability and safety properties. UPPAAL Tiga provides a mature and fully integrated tool with dramatic improvements both in terms of performance and the availability of the extended input language of Uppaal-4.0. UPPAAL Tiga can synthesis winning strategies for both safety and liveness control objectives and let the user play against them both from the command line and from the graphical simulator that was completely re-designed. In particular stategies can be represented as BDDs and CDDs providing an extremely compact format for control code.

Controller Synthesis with Partial Observability
In this work we consider the problem of controller synthesis for timed games under imperfect information. Novel to our approach is the requirements to strategies: they should be based on a finite collection of observations and must be stuttering invariant in the sense that repeated identical observations will not change the strategy.We provide a constructive transformation to equivalent finite games with perfect information, giving decidability as well as allowing for an efficient on-the-fly forward algorithm. We report on application of an initial experimental implementation.

Playing Games with Games
In this work we focus on property-preserving preorders between timed (game) automata. Following the example of timed (weak) simulation between timed automata, we define timed

alternating (weak) simulation as a preorder between timed game automata, which preserves controllability. We show how (weak) timed simulation and (weak) timed alternating simulation problems may be reduced to safety games. We provide two case-studies using our technique for preorder checking.

A Game-Theoretic Approach to Real-Time Testing
This work presents a game-theoretic approach to the testing of uncontrollable real-time systems. By modelling the systems with Timed I/O Game Automata and specifying the test purposes as Timed CTL formulas, we employ UPPAAL-TIGA to synthesize winning strategies, and then use these strategies to conduct on-line testing of the systems. The testing process is proved to be sound and complete with respect to the given test purposes. Case study and preliminary experimental results indicate that this is a viable approach to real-time system testing.

Guided Controller Synthesis for Climate Controller Using UPPAAL Tiga (case study)
In this work, we provide a complete tool chain for automatic controller synthesis using UPPAAL Tiga and Simulink. The tool chain is explored using an industrial case study for climate control in a pig stable. The problem is modeled as a game, and UPPAAL Tiga is used to automatically synthesize a safe strategy that is transformed for input to Simulink, ´which is used to run simulations on the controller and generate code that can be executed in the actual pig stable. The model allows for guiding the synthesis process and generate different strategies that are compared through simulations.

Modal Transition Systems
In this work we reexamine the notion of modal transition systems due to Larsen and Thomsen in two different ways. Firstly it is shown that the notion of interface automata by Alfaro and Henzinger corresponds to a subset of modal transition systems. As a consequence a more expressive interface theory may be built, by a simple generalization from interface automata to modal automata. In order to further exemplify the usefulness of modal I/O automata, we construct a behavioral variability theory for product line development. Secondly, we demonstrate deciding any refinement, complete with respect to the standard notions of implementation, is shown to be computationally hard (co-NP hard). Also, we consider four forms of consistency (existence of bimplementations) for modal specifications. We characterize each operationally, giving algorithms for deciding, and for synthesizing implementations, together with their complexities.

One-clock Priced Timed Automata
The model of priced timed automata was independently introduced by Larsen et al and Alur et al in 2001 with the first decidability results (concerning cost optimal reachability). Since then a number other decision problems have been considered including cost-optimal infinite schedules. Also model checking wrt suitable weighted logics (CTL and LTL) have been considered as well as the problem of synthezising cost-optimal strategies. For priced timed automata with 3 clocks or more both these problems have been proven undecidable. As recent results it has been proved that both problems are decidable in when restricting to the setting of a single clock.

Improved State Space Search Algorithms for Timed Automata Models
Several new contributions toward improved state space exploration algorithms have been made during the third year:

- In one approach, the traversal of the state space is guided by a heuristic function which estimates the distance of a search state to the nearest error state. The technique combines two recent approaches to design such estimation functions. Both are based on computing an abstraction of the system and using the error distance in this abstraction as the heuristic value. The abstractions, and thus the heuristic functions, are generated fully automatically and do not need any additional user input. Experiments indicate less time and memory to find shorter error paths than UPPAAL's standard search methods.
- A second approach introduces a new flexible framework for state space exploration based on cooperating agents. The idea is to let various agents with different search patterns explore the state space individually and communicate information about fruitful subpaths of the search tree to each other. That way very complex global search behavior is achieved with very simple local behavior. As an example agent behavior, a novel anytime randomized search strategy called frustration search is proposed. The effectiveness of the framework is illustrated in the setting of priced timed automata on a number of case studies.
- In the third approach a fully automatic approach for counter example guided abstraction refinement of real-time systems modelled in a subset of timed automata has been introduced. Since the abstractions are overapproximations, absence of abstract counterexamples implies a valid result for the full model. Generated abstract counterexamples are used to construct either concrete counterexamples for the full model or to identify slightly refined abstractions in which the found spurious counterexample cannot occur anymore. Nontrivial case studies demonstrate that this approach computes small abstractions fast without any user interaction.

DBM Library

This work represents several years of effort on the design and efficient implementation of the various datastructures needed for performing symbolic exploration of timed automata. The main datastructure is that of Difference Bounded Matrices (DBM), and the work has lead to an open-source library for manipulating DBMs. The library includes recent research results on subtraction and merging of DBMS: subtraction is one of the few operations that result in a non-convex set, and thus, requires splitting. Whereas subtraction can be avoided in simple state space exploration of timed automata (UPPAAL), subtraction is required when deriving and representing strategies of timed games (UPPAAL Tiga). The algorithm proposed is efficient in the sense that the number of splits is significantly reduced (compared to a naive algorithm). Also available in the library are research results on the efficient merge of difference bound matrices (DBMs) in order to avoid an explosion of the number of DBMs during operations (e.g. subtraction of DBMs).

EPFL

Algorithms for Interface Synthesis

A temporal interface for a component is a finite automaton that specifies the legal sequences of calls to functions that are provided by the component. We compared and evaluated three different algorithms for automatically extracting temporal interfaces from code: (1) a game

algorithm that computes the interface as a representation of the most general environment strategy to avoid a safety violation; (2) a learning algorithm that repeatedly queries the program to construct the minimal interface automaton; and (3) a CEGAR algorithm that iteratively refines an abstract interface hypothesis by adding relevant program variables. On the theoretical side, we provided for each of the three algorithms a family of components on which that algorithm outperforms the two alternatives. On the practical side, we evaluate the three algorithms experimentally on a variety of component libraries. [CAV 2007]

Solving Games for the Control of Reactive Systems
The control of reactive systems requires the solution of two-player games on graphs with omega-regular objectives. When the objective is specified by a linear temporal logic formula or nondeterministic Buchi automaton, then previous algorithms for solving the game require the construction of an equivalent deterministic automaton. However, determinization for automata on infinite words is extremely complicated, and current implementations fail to produce deterministic automata even for relatively small inputs. We show howed to construct, from a given nondeterministic Buchi automaton, an equivalent nondeterministic parity automaton that is good for solving games. The main insight is that a nondeterministic automaton is good for solving games if it fairly simulates the equivalent deterministic automaton. In this way, we omit the determinization step in game solving and reactive synthesis. The fact that our automata are nondeterministic makes them surprisingly simple, amenable to symbolic implementation, and allows an incremental search for winning strategies.

We introduced strategy logic, a logic that treats strategies in two-player games as explicit first-order objects. Strategy logic subsumes other logics about games and can be decided using tree automata that recognize sets of strategies
We defined and studied the assume-guarantee problem, where the goal is two synthesize several concurrent processes each satisfying a specification. The proper formulation of assume-guarantee synthesis is one where each process competes with the other processes, but not at the price of violating its own specification. We showed that the problem can be solved by computing secure-equilibrium strategies.

We studied games where the winning conditions are disjunctions (or dually, conjunctions) of parity conditions; we call them generalized parity games. These winning conditions, while omega-regular, arise naturally when considering fair simulation relations, secure equilibria, and determinization of omega automata. Considering these games as special cases of Rabin or Streett games is not optimal, and we provided improved algorithms. We also extend the subexponential algorithm for solving parity games recently introduced by Jurdzinski, Paterson, and Zwick to generalized parity games.

We designed a strategy-improvement (a.k.a. policy-iteration) algorithm for concurrent games with reachability objectives.

We study observation-based strategies for two-player turn-based games on graphs with omega-regular objectives. An observation-based strategy relies on imperfect information about the history of a play, namely, on the past sequence of observations. Such games occur in the synthesis of a controller that does not see the private state of the plant. We developed an algorithm for computing the set of states from which a player can win with a deterministic observation-based strategy for any omega-regular objective. The algorithm computes on a lattice of antichains, which has the advantages of being directed by the objective and of avoiding an explicit subset construction on the game graph. We also gave an algorithm for computing the set of states from which a player can win with probability 1 with a randomized observation-based strategy for a

Buchi objective. This set is of interest because in the absence of perfect information, randomized strategies are more powerful than deterministic ones.

Solving Timed 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 considered the minimum-time reachability problem in concurrent two-player timed automaton game structures. We showed how to compute the minimum time needed by a player to reach a target location against all possible choices of the opponent.

Algorithms for Quantitative Reasoning
We studied stochastic graph games with omega-regular winning conditions specified as Rabin or Streett objectives. These games are NP-complete and coNP-complete, respectively. The value of the game for a player at a state given an objective is the maximal probability with which the player can guarantee the satisfaction of the objective from the state. We designed a strategy-improvement algorithm to compute values in stochastic Rabin games, where an improvement step involves solving Markov decision processes (MDPs) and nonstochastic Rabin games. The algorithm also computes values for stochastic Streett games but does not directly yield an optimal strategy for Streett objectives. We showed how to obtain an optimal strategy for Streett objectives by solving certain nonstochastic Streett games.

We developed 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 showed that the classical boolean rules for compositional reasoning have quantitative counterparts in our setting.

OFFIS, Oldenborg

Automating verification of cooperation, control, and design in traffic applications
We present a verification methodology for cooperating traffic agents covering analysis of cooperation strategies, realization of strategies through control, and implementation of control. For each layer, we provide dedicated approaches to formal verification of safety and stability properties of the design. The range of employed verification techniques invoked to span this verification space includes application of pre-verified design patterns, automatic synthesis of Lyapunov functions, constraint generation for parameterized designs, model-checking in rich theories, and abstraction refinement. We illustrate this approach with a variant of the European Train Control System (ETCS), employing layer specific verification techniques to layer specific views of an ETCS design.

The flap controller (high-lift) case study
This application is derived from a case study for Airbus, a controller for the flaps of an aircraft. The flaps are extended during take-off and landing to generate more lift at low velocity. They are not robust enough for high velocity, so they must be retracted for other periods. The

controller can perform a load-relief function to correct the pilot's commands if he endangers the flaps. Additionally, there is also an extensive monitoring of the health of its sub-systems, checking for instance for hardware failures. Typically this will give rise to large discrete state spaces when model checking models derived from the flap ´controller.

Distributed Controller for Tramways
The "Single-tracked Line Segment" (SLS) case study stems from an industrial partner of the UniForM-project . It is the specification of a control system for a single-tracked line segment for tramways. It is implemented by distributed PLC automata. We took three different models of the SLS case study as examples. As the safety property to verify, we chose the mutual exclusion of drive permissions, i.e., the control system never gives permission to both directions simultaneously.

IRISA

Symbolic test generation tool
The STG tool (test generation for models with control and data) has been improved and 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. A number of cases studies have been developped and experimented.

Integrating formal verification and conformance testing for reactive systems
In this work we describe a methodology integrating verification and conformance testing for the formal validation of reactive systems. A specification of a system - an extended input-output automaton, which may be infinite-state - and a set of safety properties (``nothing bad ever happens'') and possibility properties (``something good may happen'') are assumed. The properties are first tentatively verified on the specification using automatic techniques based on approximated state-space exploration, which are sound, but, as a price to pay for automation, are not complete for the given class of properties. Because of this incompleteness and of state-space explosion, the verification may not succeed in proving or disproving the properties. However, even if verification did not succeed, the testing phase can proceed and provide useful information about the implementation. Test cases are automatically and symbolically generated from the specification and the properties, and are executed on a black-box implementation of the system. The test execution may detect violations of conformance between implementation and specification; in addition, it may detect violation/satisfaction of the properties by the implementation and by the specification. In this sense, testing completes verification.

Automatic test generation from interprocedural specifications
In this work, we aim at extending the principles and algorithms of model-based testing for recursive interprocedural specifications that can be modeled by Push-Down Systems (PDS). Such specifications may be more compact than non-recursive ones and are more expressive. The generated test cases are selected according to a test purpose, a (set of) scenario of interest that one wants to observe during test execution. The test generation method we propose is based on program transformations and a coreachability analysis, which allows to decide whether and how the test purpose can still be satisfied. However, despite the possibility to perform an exact analysis, the inability of test cases to inspect their own stack prevents it from using fully the coreachability information.

Integrating verification, testing, and learning for cryptographic protocols

The verification of cryptographic protocol specifications is an active research topic and has received much attention from the formal verification community. By contrast, the black-box testing of actual implementations of protocols, which is, arguably, as important as verification for ensuring the correct functioning of protocols is little studied. We propose an approach for checking secrecy and authenticity properties not only on protocol specifications, but also on black-box implementations. The approach is compositional and integrates ideas from verification, testing, and learning. It is illustrated on the Basic Access Control protocol implemented in biometric passports.

Analysis of Communicating Infinite State Machines using Lattice Automata

We have proposed an extension of the model of communicating automata (CFSM): Symbolic Communicating Machines (SCM), where messages carry data in infinite domains, and an approximate reachability analysis method on this model, based on lattice automata. Lattice automata are finite automata, the transitions of which are labeled with elements of an atomic lattice. We tackle the problem of the determinization as well as the definition of a widening operator for these automata. We have also shown that lattice automata are useful for the interprocedural analysis.

UPPSALA

Validation and Resource-Related Analysis (with Aalborg)

The main effort has been on validation techniques for timed systems, in particular resource-related analysis to cover a broad range of resources such as processors, buffers and memory blocks etc. A series of theoretical results have been achieved. Notably the work of [KY06] extends timed automata with FIFO channels to model asynchronous communication in timed systems. The study show that a system with two channels -- that are no more expressive than finite-state machines in the untimed setting -- is Turing-equivalent. Our recent work [FKPY07, KSY07] show that the schedulability problem in the multiprocessor setting is already undecidable for systems with two processors. To overcome these obstacles, we have been developing approximation and abstraction methods. As an abstraction for timed automata, we have adopted arrival curves from network calculus as communication and resource consumption interfaces for compositional modeling and validation. A prototype tool (named CATS) [KMY07] for compositional timing and performance analysis has been developed for systems modeled 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 Eclips 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.

To scale up the verification technique based on timed automata, a recent work has also applied the partial order method developed in our group to component-based real-time systems, with promising experimental results [HP07].

Validating QoS properties of Biomedical Sensor Networks

As a case study, we have developed a formal model for a Biomedical Sensor Network (BSN). The sensor nodes of the network are constructed based on the IEEE 802.15.4 ZigBee standard for wireless communication. The UPPAAL tool is used to tune and validate the temporal configuration parameters of the network in order to guarantee the desired QoS properties for a medical application scenario. The case study shows that even though the main feature of UPPAAL is model checking, it is also a promising and competitive tool for efficient simulation.

This is a very challenging case study for verification tools. It is easy to scale up because all nodes of a network run the same application and each node has a very simple behaviour.But as a network may contain a large number of nodes andthe nodes must cooperate to achieve the same goal e.g. to deliver a message to the sink node, the behaviour of a network may beextremely complicated. Another challenge is to formalize the QoS properties for such networks. Unfortunately, the UPPAALspecification language is not expressive enough. We needa more expressive logic.

CVF

Synthesis with incomplete information (cooperation with EPFL, U Aalborg, and EC Nantes)
We have continued our collaboration with EPFL on algorithms for the synthesis of controller with imperfect 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 antichains 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.

Those results have been extended to stuttering invariant and observation based strategy in collaboration with U Aalborg and EC Nantes. Those results should be integrated into the tool UppAal-Tiga in 2008.

Improved algorithms for the automata-based approach to model-checking (in collaboration with EPFL)
Ideas underlying our new algorithms for controller synthesis under imperfect information has recently been extended to solve classical problems in automata theory for finite word languages and infinite words. With this new method, inclusion between two nondeterministic automata can be solved much more efficiently than with previously known algorithms. Those results should lead to the development of a new model-checking tool for linear time specifications expressed in LTL or using nondeterministic Buechi automata.

Fixed point based abstraction refinement (in collaboration with ENS Paris)
We have defined an new abstract fixpoint checking algorithm with automatic refinement by backward completion in Moore closed abstract domains. We have studied the properties of our algorithm and prove it to be more precise than the counterexample guided abstract refinement algorithm (CEGAR). Contrary to several works in the literature, our algorithm does not require the abstract domains to be partitions of the state space. We have shown that our automatic refinement technique is compatible with so-called acceleration techniques. Furthermore, the use of Boolean closed domains does not improve the precision of our

algorithm.

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.

New efficient approximate verification based on symmetry markers
This new verification technique can be used in various model-checker and in particular the spin tool. It exploits state-space symmetries induced by scalarset values used in a model. The technique involves efficiently computing a marker for each state encountered during search. A complete verification method only partially exploits symmetry; an approximate verification method fully exploits symmetry. We describe how symmetry markers can be efficiently computed and integrated into the SPIN tool. An empirical evaluation of our technique shows very good performance results and a high degree of precision for the approximate method (i.e. very few non-symmetric states receive the same marker). We also identify a class of models for which the approximate technique is precise.

Testing Distributed Systems through Symbolic Model Checking
The observation of a distributed systems finite execution can be abstracted as partial order trace. We show that testing that such a distributed execution satisfies some global property amounts therefore to model check the corresponding trace. We provide an efficient symbolic Ctl mode checking algorithm for traces. This method is based on a symbolic data structure, called Interval Sharing Trees, allowing to efficiently represent and manipulate sets of k-uples of naturals. Efficient symbolic operations are defined on this data structure in order to deal with all Ctl modalities.

Study of the properties of automata-based representations of sets of real numbers
Automata-based representations of sets of real vectors are useful for manipulating the sets of configurations of infinite-state systems during state-space exploration. We have established that the sets of real vectors that can be represented by weak deterministic automata in all integer bases are exactly those thatare definable in first-order additive arithmetic. This generalizes to real numbers the well-known Cobham's theorem on the representability of sets of integers, and provides a theoretical justification to the use of weak deterministic automata as data structures for representing sets of reals in actual verification applications.

Computing convex hulls by automata iteration
A new technique for computing the convex hull of an automaton-represented finite set of integers was introduced. The technique is based on the extrapolation of a sequence of automata that approximate the convex hull and produces its result in the form of on automaton operating on the econdings of real vectors. The technique has been implemented and is useful in the context of the automata-based representation of arithmetic sets.

Verimag

Test case generation for ultimately periodic paths
Software verification is a hard yet important challenge. In general, the problem is undecidable. Nevertheless, it is still beneficial to look at solutions that either restrict the generality (e.g., model-checking for finite state systems) or are heuristic in nature, hence do not guarantee to terminate. In this work, we concentrate on a related problem, that of verifying that a cycle in the flow graph of a program (or in the combination of flow graphs of various concurrent processes)

does not terminate. We showed some exact and sufficient conditions for cycle non-termination, and provided application for program verification. This allows us to check sequential and concurrent programs against temporal properties, using a truly symbolic approach, and to use temporal logic to guide the selection of test cases in such programs.

Conformance testing framework for hybrid systems
This framework has been defined according to the international standard for formal conformance testing. It includes:

- The definition of coverage measures for hybrid systems
- Algorithms for coverage-guided test generation

Deadlock detection and verification in BIP
We developed new composability and compositionality techniques for deadlock-freedom. These are based on the separation of concerns underlying the layered BIP model. They use structural analysis techniques of the connectors of BIP models. Deadlock-freedom preservation is checked by analysis of a dependency graph relating the ports of the components. The dependency relation associates with a port the set of the ports with which synchronization is needed in some interaction. A circuit in the dependency graph characterizes a potential deadlock situation. More detailed analyses of the behaviour atomic components allow deciding deadlock-freedom. These techniques have been implemented in DeadlockFinder a prototype tool that generates from BIP models sufficient conditions for deadlockfreedom. These conditions can be checked interactively either by using model-checking tools or by using invariants provided by the user.

An abstract domain extending Difference-Bound Matrices with disequality constraints
The property that two numerical variables always hold different values, at some point of a program, can be very useful, especially for analyzing aliases: if i differs from j, then A[i] and A[j] are not aliased, and this knowledge is of great help for any other program analysis. Surprisingly, disequalities are seldom considered in abstract interpretation, most of the proposed numerical domains being restricted to convex sets. In this paper, we propose to combine simple ordering properties with disequalities. "Difference-bounds matrices" (or DBMs) is a domain proposed by David Dill, for expressing relations of the form "x-y <= constant" or `"constant1 <= x <= constant2". We define DDBMs ("disequalities DBM") as conjunctions of DBMs with simple disequalities of the form "x\neq y" or "x\neq 0". We give algorithms on DDBMs, for deciding the emptiness, computing a normal form, and performing the usual operations of an abstract domain. These algorithms have the same complexity ($O(n^3)$ where n is the number of variables) than those for classical DBMs, if the variables are considered to be valued in a dense set (reals or rationals). In the arithmetic case, the emptiness decision is NP-complete, and other operations run in $O(n^5)$.

2.3.2 Individual Publications Resulting from these Achievements

CFV

Jean-Francois Raskin. Controller Synthesis using Lattice Theory. Invited tutorial. Proceeding of the 46th conference on Decision and Control (CDC 2007), IEEE press. New-Orleans. December 2007.

Gilles Geeraerts, Jean-Francois Raskin, and Laurent Van Begin. Well-structured Languages. AcceptedÂ for publication in Acta Informatica, Springer, 2007.

Gilles Geeraerts, Jean-Francois Raskin, and Laurent Van Begin. On the efficient computation of the coverability set for Petri nets. To appear in ATVA'07,Â Lecture Notes in Computer Science, Springer Verlag, 2007.

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

Patrick Cousot, Pierre Ganty, and Jean-Francois Raskin. Fixpoint-based Abstraction Refinement. To appear in SAS07, Lecture Notes in Computer Science, Springer Verlag, 2007.

Thomas Brihaye, Thomas A. Henzinger, Vinayak S. Prabhu, and Jean-Francois Raskin. Minimum-Time Reachability in Timed Games. To appear in ICALP07, Lecture Notes in Computer Science, Springer Verlag, 2007.

Khrishnendu Charterjee, Laurent Doyen, Thomas A. Henzinger and Jean-Francois Raskin. Algorithms for Omega-regular games of Incomplete Information (extended version). Accepted for publication inÂ Logical Methods in Computer Science, 2007.

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).

Pierre Ganty, Jean-Francois Raskin, Laurent Van Begin. From Many Places to Few: Automatic Abstraction Refinement for Petri Nets. To appear in ATPN'07,Â Lecture Notes in Computer Science, Springer Verlag, 2007.

Veronique Bruyere and Jean-Francois Raskin. Real-Time Model-Checking: Parameters Everywhere (extended version). Accepted for publication in the journal Logical Methods in Computer Science, 2007. (30 pages).

Laurent Doyen and Jean-Francois Raskin. Improved Algorithms for the Automata-based Approach to Model-Checking. In TACAS'07, Lecture Notes in Computer Science, 4424,Â Springer Verlag, 2007.

Véronique Bruyère and Jean-Francois Raskin. Durations, Parametric Model-Checking in Timed Automata with Presburger Arithmetic. To appear in Transactions in Computatitonal Logic, ACM Press, 2007. (25 pages)

Michael Leuschel and Thierry Massart. Efficient approximate verification of B via symmetry markers. In Proc. of the International Symmetry Conference, Edinburgh, UK, January 2007. (15 pages).

Gabriel Kalyon , Thierry Massart , Cédric Meuter, and Laurent Van Begin.Testing Distributed Systems through Symbolic Model Checking in FORTE'07, Lecture Notes in Computer Sciences.

Dragan Bosnacki, Alastair Donaldson, Michael Leuschel, Thierry Massart: Efficient Approximate Verification of Promela Models via Symmetry Markers. To appear in ATVA'07, Lecture Notes in Computer Science, Springer Verlag, 16 pages, 2007.

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

Patricia Bouyer, Thomas Brihaye, Fabrice Chevalier, Weighted o-minimal hybrid systems are more decidable than weighted timed automata!, proceedings of the symposium LFCS 2007, Lect. Notes in Computer Science 4514, pp 69-83, Springer.

Thomas Brihaye, Words and bisimulations of dynamical systems, Discrete Mathematics and Theoretical Computer Science, 9 (2007), no.2, 11--31.

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.

B. Boigelot and J. Brusten. A Generalization of Cobham's Theorem to Automata over Real Numbers. Proc. 34th International Colloquium on Automata, Languages and Programming, volume 4596, Lecture Notes in Computer Science, pages 813-824, Wroclaw, July 2007, Springer-Verlag.

Axel Legay, Pierre Wolper: On the Use of Automata-based Techniques in Symbolic Model Checking: Invited Address. Electr. Notes Theor. Comput. Sci. 150(1): 3-8 (2006)

EPFL

Krishnendu Chatterjee, Thomas A. Henzinger, and Nir Piterman.Strategy logic. Proceedings of the 18th International Conference on Concurrency Theory (CONCUR), Lecture Notes in Computer Science, Springer, 2007.

Thomas A. Henzinger. Quantitative generalizations of languages. Proceedings of the 11th International Conference on Developments in Language Theory (DLT), Lecture Notes in Computer Science 4588, Springer, 2007, pp. 20-22.

Krishnendu Chatterjee and Thomas A. Henzinger. Assume-guarantee synthesis. Proceedings of the 13th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS),Lecture Notes in Computer Science 4424, Springer, 2007, pp. 261-275.

Krishnendu Chatterjee, Thomas A. Henzinger, and Nir Piterman. Generalized parity games. Proceedings of the Tenth International Conference on Foundations of Software Science and Computation Structures (FOSSACS), Lecture Notes in Computer Science 4423, Springer, 2007, pp. 153-167.

Thomas A. Henzinger. Games, time, and probability: Graph models for system design and analysis. Proceedings of the 33rd International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM), Lecture Notes in Computer Science 4362, Springer, 2007, pp. 103-110.

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 4202, Springer, 2006, pp. 1-17.

Thomas A. Henzinger and Nir Piterman. Solving games without determinization. Proceedings of the 15th International Conference on Computer Science Logic (CSL), Lecture Notes in Computer Science 4207, Springer, 2006, pp. 395-410.

Krishnendu Chatterjee, Luca de Alfaro, and Thomas A. Henzinger. Strategy improvement for concurrent reachability games. Proceedings of the Third Annual Conference on Quantitative Evaluation of Systems (QEST), IEEE Computer Society Press, 2006, pp. 291-300.

Krishnendu Chatterjee and Thomas A. Henzinger. Strategy improvement for stochastic Rabin and Streett games. Proceedings of the 17th International Conference on Concurrency Theory (CONCUR), Lecture Notes in Computer Science 4137, Springer, 2006, pp. 375-389.

Krishnendu Chatterjee, Laurent Doyen, Thomas A. Henzinger, and Jean-Francois Raskin. Algorithms for omega-regular games with imperfect information. Proceedings of the 15th International Conference on Computer Science Logic (CSL), Lecture Notes in Computer Science 4207, Springer, 2006, pp. 287-302.

Thomas Brihaye, Thomas A. Henzinger, Vinayak Prabhu, and Jean-Francois Raskin. Minimum-time reachability in timed games. Proceedings of the 34th International Colloquium on Automata, Languages, and Programming (ICALP), Lecture Notes in Computer Science, Springer, 2007.

Krishnendu Chatterjee, Luca de Alfaro, Marco Faella, Thomas A. Henzinger, Rupak Majumdar, and Marielle Stoelinga. Compositional quantitative reasoning. Proceedings of the Third Annual Conference on Quantitative Evaluation of Systems (QEST), IEEE Computer Society Press, 2006, pp. 179-188.

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.

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

IRISA

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

S. Pickin, C. Jard, T. Jéron, J-M Jézéquel, Y. Le Traon: Test Synthesis from UML Models of Distributed Software, IEEE Transactions on Software Engineering (to appear), 2007.

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

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.

T. Le Gall, B. Jeannet: Lattice automata: a representation of languages over an infinite alphabet, and some applications to verification, in The 14th International Static Analysis Symposium, SAS 2007,Kongens Lyngby, Denmark, August 2007.

C. Constant, B. Jeannet, T. Jéron: 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.

Thierry Jéron: Model-based test selection for infinite state reactive systems, in 5th IFIP Working Conference on Distributed and Parallel Embedded Systems, DIPES'06, Braga, Portugal, October 2006.

Twente

J. Berendsen, D. N. Jansen, and J. P. Katoen: Probably on time and within budget – On reachability in priced probabilistic timed automata. In Quantitative Evaluation of Systems (QEST), Riverside, US, pages 311-322. IEEE Computer Society Press, 2006.

Hichem Boudali, Pepijn Crouzen, and Mariëlle Stoelinga: A compositional semantics for dynamic fault tree analysis in terms of interactive markov chains, In Proceedings of the 5th International Symposium on Automated Technology for Verification and Analysis (ATVA'07), LNCS, pages 708-717. Springer, 2007, to appear.

Hichem Boudali, Pepijn Crouzen, and Mariëlle Stoelinga: Dynamic fault tree analysis using input/output interactive markov chains. In The 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2007, UK, Proceedings, pages 708-717. IEEE Computer Society, 2007.

E. Brinksma, L. Brandán Briones, and M.I.A. Stoelinga: A semantic framework for test coverage. In S. Graf and W. Zhang, editors, Proceedings of the fourth international symposium on Automated Technology for Verification and Analysis (ATVA'06), LNCS. Springer, 2006.

E. Brinksma: The Challenges of Embedded Systems Engineering. In: Alberto Bemporad, Antonio Bicchi, Giorgio C. Buttazzo (Eds.): Hybrid Systems: Computation and Control, 10th International Workshop, HSCC 2007, Pisa, Italy, April 3-5, 2007, Proceedings. Lecture Notes in Computer Science 4416 Springer 2007

L. Brandán Briones. Theories for Model-based Testing: Real-time and Coverage. PhD thesis, University of Twente, the Netherlands, March.

K. Chatterjee, L. de Alfaro, M. Faella, T. A. Henzinger, R. Majumdar, and M. I. A. Stoelinga. Quantitative compositional reasoning, pages 179-189. IEEE Computer Society Press, 2006.

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.

Luca de Alfaro, Rupak Majumdar, Vishwanath Raman, and Marielle Stoelinga: Game relations and metrics. In LICS '07: Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science, pages 99-108. IEEE Computer Society, 2007.

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.

H. Boudali and B.R.H.M. Haverkort and M. Kuntz and M.I.A. Stoelinga: Best of Three Worlds: Towards Sound Architectural Dependability Models. In Proceedings of the Eighth International Workshop on Performability Modeling of Computer and Communication Systems (PMCCS'07), 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.

Kim Guldstrand Larsen, Ulrik Nyman, Andrzej Wasowski: On Modal Refinement and Consistency. CONCUR 2007.

Kim Guldstrand Larsen, Ulrik Nyman, Andrzej Wasowski: Modal I/O Automata for Interface and Product Line Theories. ESOP 2007.

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

Jacob Illum Rasmussen, Gerd Behrmann, Kim Guldstrand Larsen: Complexity in Simplicity: Flexible Agent-Based State Space Exploration. TACAS 2007.

Kim Guldstrand Larsen, Ulrik Nyman, Andrzej Wasowski: Interface Input/Output Automata. FM 2006.

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

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

Henning Dierks, Sebastian Kupferschmid, Kim Larsen: Automatic Abstraction Refinement for Timed Automata. FORMATS 2007.

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

Partrica Bouyer, Kim G. Larsen, Nicolas Markey: Model-Checking One-Clock Priced Timed Automata. Logical Methods in Computer Science (special FoSSacS07 issue).

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.

Istvan Knoll, Yu Guo, Christo Angelov, Nicolae Marian, Anders P. Ravn, Arne Skou: SUppCom: A Toolchain for the Development of Domain Specific Embedded Software Systems. Under submission.

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

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

John Knudsen, Anders P. Ravn, Arne Skou: Design Verification Patterns. Under submission.

UPPSALA

Elena Fersman, Pavel Krcal, Paul Pettersson and Wang Yi: Task Automata: Schedulability, Decidability and Undecidability. In Information and Computation, vol 205, issue 8, pages 1149-1172, 2007.

Pavel Krcal, Martin Stigge and Wang Yi: Multi-Processor Schedulability Analysis of Preemptive Real-Time Tasks with Variable Execution Times In Proceedings of the 5th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'07), LNCS 4763. 2007.

John Hakansson and Paul Pettersson: Partial Order Reduction for Verification of Real-Time Components. In Proceedings of the 5th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'07), LNCS 4763. 2007.

John Hakansson and Paul Pettersson: Partial Order Reduction for Verification of Real-Time Components. In Proceedings of the 5th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'07), LNCS 4763. 2007.

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

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)

Pavel Krcal, 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.

Simon Tschirner and Wang Yi: Validating QoS Properties in Biomedical Sensor Networks. The 19th Nordic Workshop on Pogramming Theory Oslo, October 10-12, 2007.

Verimag

S. Bensalem, D. Peled, H. Qu, S. Tripakis and L. Zuck. Test Case Generation for Ultimately Periodic Paths: IBM Conference-HVC , October 23-25 2007.

Tarik Nahhal and Thao Dang. Guided randomized simulation. In HSCC Hybrid Systems: Computation and Control, LNCS, pages 731--735, 2007.

Tarik Nahhal and Thao Dang. Test coverage for continuous and hybrid systems. In CAV - Computer Aided Verification, LNCS, pages 454-468, 2007.

M. Péron and N. Halbwachs 8th International Conference on Verification, Model-checking, and Abstract Intepretation, VMCAI'07 B. Cook and A. Podelski, eds. Nice, France, january 2007

2.3.3 Interaction and Building Excellence between Partners

Organization and contributions to the ARTIST2 winterschool MOTIVES in Trento, February 2007.

Cluster meeting in Trento, February 2007.

Organization and contributions to the ARTIST2 workshop at DATE, Nice, April, 2007.

Organization and contributions to the ARTIST2 workshop at CAV, Berlin, July 2007.

Organization and hosting of the International Workshop FORMATS in Paris, October, 2006.

Organization and hosting of the International Workshop FORMATS in Salzburg (in connection with the ESWeek), October 2007.

Thomas Chatain has moved from a post.doc. position in Aalborg to a lecture position at LSV, Cachan.

Exchange visits:

- From Aalborg to CFV (Brussels): one week visit of Prof. Kim Larsen to the team of Prof. JF Raskin.
- From CFV (Brussels) to EPFL (Henzinger): Dr. Laurent Doyen formerly in CFV is post-doct at EPFL.
- From CFV (Brussels) to EPFL (Henzinger): several visits during 2006-2007 by Prof. JF Raskin.
- From EPFL (Henzinger) to CFV (Brussels): several visits during 2006-2007 by Dr. L Doyen.
- From CFV (Brussels) to ENS Cachan: Dr. Thomas Brihaye formerly in CFV was post-doc at LSV during 2006-2007.
- From CFV (Brussels) to LIAFA (Bouajjani), several (one week) visits of Dr. L. Van Begin to LIAFA.
- From CFV (Brussels) to INRIA-IRISA, three months visit of Prof. T. Massart to Dr T. Jeron at IRISA Rennes.
- A cooperative work with Inria Rennes and Nijmegen took place during the sabbatical year of Vlad Rusu at Nijmegen. The contribution is on a compositional approach to model-based testing which integrates ideas from verification, testing, and learning. It is illustrated on the Basic Access Control protocol implemented in biometric passports.

- Thierry Massart from ULB spent 3 months (January-March 2007) in Inria Rennes. The collaboration was on testing from interprocedural specifications and monitoring.

2.3.4 Joint Publications Resulting from these Achievements

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

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

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

Henning Dierks, Sebastian Kupferschmid, Kim Larsen: Automatic Abstraction Refinement for Timed Automata. FORMATS 2007.

Partrica Bouyer, Kim G. Larsen, Nicolas Markey: Model-Checking One-Clock Priced Timed Automata. Logical Methods in Computer Science (special FoSSacS07 issue).

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.

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

Krishnendu Chatterjee, Laurent Doyen, Thomas A. Henzinger, and Jean-Francois Raskin. Algorithms for omega-regular games with imperfect information. Proceedings of the 15th International Conference on Computer Science Logic (CSL), Lecture Notes in Computer Science 4207, Springer, 2006, pp. 287-302.

Thomas Brihaye, Thomas A. Henzinger, Vinayak Prabhu, and Jean-François Raskin. Minimum-time reachability in timed games. Proceedings of the 34th International Colloquium on Automata, Languages, and Programming (ICALP), Lecture Notes in Computer Science, Springer, 2007.

Krishnendu Chatterjee, Luca de Alfaro, Marco Faella, Thomas A. Henzinger, Rupak Majumdar, and Mariëlle Stoelinga. Compositional quantitative reasoning. Proceedings of the Third Annual Conference on Quantitative Evaluation of Systems (QEST), IEEE Computer Society Press, 2006, pp. 179-188.

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

Thomas Brihaye, Thomas A. Henzinger, Vinayak S. Prabhu, and Jean-Francois Raskin.

Minimum-Time Reachability in Timed Games. To appear in ICALP07, Lecture Notes in Computer Science, Springer Verlag, 2007. (12 pages)

Khrishnendu Charterjee, Laurent Doyen, Thomas A. Henzinger and Jean-François Raskin. Algorithms for Omega-regular games of Incomplete Information (extended version). Accepted for publication inÂ Logical Methods in Computer Science, 2007. (30 pages).

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

Laurent Doyen and Jean-François Raskin. Improved Algorithms for the Automata-based Approach to Model-Checking. In TACAS'07, Lecture Notes in Computer Science, 4424 Springer Verlag, 2007.

Patricia Bouyer, Thomas Brihaye, Fabrice Chevalier, Weighted o-minimal hybrid systems are more decidable than weighted timed automata!, proceedings of the symposium LFCS 2007, Lect. Notes in Computer Science 4514, pp 69-83, Springer.

Thomas Brihaye, François 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.

2.3.5 Keynotes, Workshops, Tutorials

Gerd Behrmann and Kim G. Larsen (invited tutorial): Real Time Validation of Embedded Systems Using UPPAAL International PhD School on Verification of Protocols for Security and Mobility, IT-University, Copenhagen, Denmark, October 9-13, 2006

Bernard Boigelot. Hybrid Acceleration. Dagstuhl Seminar on "Open Systems: Testing, Verification and Synthesis", Schloss Dagstuhl, Germany. October 2006.

Hichem Boudali, Dynamic fault tree analysis using I/O interactive Markov chains, Quantitative Aspects of Embedded Systems, Dagstuhl Seminar, Germany, 4-9 March 2007.

Hichem Boudali, A compositional semantics for Dynamic Fault Trees in terms of Interactive Markov Chains, Verification and Validation of Software Systems Symposium, LaQuSo, Eindhoven University of Technology, Eindhoven, the Netherlands, 23 March 2007.

Hichem Boudali, A Temporal Bayesian Network Reliability Framework, International Mathematical Methods in Reliability (MMR) Conference, Glasgow, Scotland, 1-4 July 2007.

Ed Brinksma, The Challenges of Embedded Systems Engineering, Invited Speaker, Hybrid Systems: Computation and Control, 10th International Workshop, HSCC 2007, Pisa, Italy, 4 April 2007.

Ed Brinksma, Models & Design, Invited Speaker, Conference on Systems Engineering Research, CSER 2007, Hoboken, NJ, USA, 15 March 2007.

Ed Brinksma, Conformance Testing & Test Coverage, Invited Lecture ARTIST2-MOTIVES Winter School, Trento, 23 February, 2007.

Ed Brinksma, A Short History of Modelling and Model Checking at Twente, International Workshop on Advances in Model-Checking in honour of Gerard J. Holzmann. December 2006. University of Twente, Enschede, The Netherlands.

P. Crouzen, CORAL - a tool for COmpositional Reliability and Availability anaLysis. Berlin, Germany, July 2, 2007.

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

Thomas A. Henzinger, Quantitative Generalizations of Languages, invited lecture, 11th International Conference on Developments in Language Theory (DLT), Turku, Finland, July 2007.

Thomas A. Henzinger, Games, Time, and Probability: Graph Models for System Design and Analysis, invited lecture, 33rd International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM), Harrachov, Czech Republic, January 2007.

Thomas A. Henzinger, Timed Alternating-Time Temporal Logic, invited lecture, Fourth International Workshop on Formal Modeling and Analysis of Timed Systems (FORMATS), Paris, France, September 2006.

Thomas A. Henzinger, Model Checking, Theorem Proving, and Abstract Interpretation: The Convergence of Formal Verification Technologies, invited lecture, Grand Challenges of Informatics Symposium, Budapest, Hungary, September 2006.

Thomas A. Henzinger, From Graph Models to Game Models, invited lecture, 25 Years of Model Checking Celebration, Seattle, Washington, August 2006.

Thomas A. Henzinger, Fine-Tuning the Dial between Model Checking and Program Analysis, invited lecture, Third Annual Alpine Verification Meeting, Aussois, France, April 2007.

Thierry Jéron, Model-based test selection for infinite state reactive systems, 5th International Symposium on Formal Methods for Components and Objects FMCO'06, Amsterdam, November 2006.

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.

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

Kim G. Larsen (invited talk): Optimal Scheduling and Controller Synthesis. ARTIST2 - MOTIVES MOdelling, TestIng, and Verification for Embedded Systems. February 2007. University of Trento.

Kim G. Larsen (invited talk): Optimal Scheduling and Controller Synthesis. Dagstuhl Seminar on Run-Time Verification, January 2007.

Kim G. Larsen (invited talk): Quantitative Analysis and Optimal Scheduling of Embedded Systems Using UPPAAL and UPPAAL Cora. Dagstuhl Seminar on Quantitative Aspects of Embedded Systems, March 2007.

Kim G. Larsen and Jan Madsen (invited talk): 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.

Kim G. Larsen and Michael R. Hansen (invited talk): 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.

Kim G. Larsen (invited tutorial): Validation of Real-Time and Embedded Systems; ARTIST/China School on Embedded Systems Design, Aug 1-11, 2007, SuZhou, China.

Kim G. Larsen (invited talk): 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.

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

Jean-Francois Raskin. Invited Talk. ``Controller Synthesis''. ARTIST2 - MOTIVES MOdelling, TestIng, and Verification for Embedded Systems. February 2007. University of Trento.

Jean-Francois Raskin. Invited Talk. ``Controller Synthesis using Lattice Theory''. IEEE CDC2007. December 2007. New-Orleans, USA.

Jean-Francois Raskin. Invited Talk. Improved Algorithms for the Automata-Based Approach to Model-Checking. International Workshop on Advances in Model-Checking in honour of Gerard J. Holzmann. December 2006. University of Twente, Endschede, The Netherlands.

Jean-Francois Raskin. A lattice theory to solve games of imperfect information. Invited talk. Summer Research Insititute. July 2006. Ecole Polytechnique Federale de Lausanne, Switzerland.

Jean-Francois Raskin. Fixpoint-based Abstraction Refinements. Concurrency seminar. Computer Science Department, Oxford, England, May, 2007.

Jean-Francois Raskin. Improved Algorithms for the Automata-based Approach to Model-Checking. Seminaires de l'IRCCyN. Unite Mixte de Recherche (UMR) 6597 du CNRS. Ecole Centrale de Nantes. France. February 2007.

Jean-Francois Raskin. A Lattice Theory to Solve Games of Imperfect Information. Dagstuhl Seminar on "Open Systems: Testing, Verification and Synthesis'', Schloss Dagstuhl, Germany. October 2006.

Vlad Rusu, Combining verification and testing for reactive systems, IPA Dutch spring school in Computer Science, Vught, Netherlands, April 2006.

Vlad Rusu, Model-based testing, invited tutorial MOTIVES 07 Winter school in Trento, February 2007.

Mariëlle Stoelinga, Time and Resource interfaces, Quantitative Aspects of Embedded Systems, Dagstuhl Seminar, Germany, 4-9 March 2007.

Pierre Wolper; Computing Closures by Automata. AFADL'07, Namur, Belgium, june 2007

Wang Yi organized and contributed to the ARTIST/China School on Embedded Systems Design, Aug 1-11, 2007, SuZhou, China.

3. Future Work and Evolution

3.1 Problem to be Tackled over the next 12 months (Sept 2007 – Aug 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 work on combining testing and verification approaches, further development and tool implementation of important topics such as optimal scheduling, fault diagnosis and controller synthesis. For finite state systems very efficient methods have been developed and for timed models UPPAAL Cora and UPPAAL Tiga provides efficient platforms on which new aspects (e.g. partial observability and robustness) may be integrated and made available. Also, continued work on quantitative models involving hybrid and stochastic phenomenas will be dealt with. Finally, work on interface specifications taking resources and quantitative aspects into account will be considered. We expect that the work within this activity will take place in close interaction with the Quasimodo STREP project.

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 12 months:

Verification

- Build a new, efficient tool for linear time model-checking using the new results obtained on the automata theoretic approach to model-checking in the light of the research done on synthesis for incomplete information.
- Extension of the antichain methods to branching time formalisms.
- Further developments of abstraction refinement methods
- Further developments of efficient symbolic representations for arithmetic sets.
- Further study of the properties of automata-based symbolic representations of sets of integer and real vectors (Real Vector Automata, RVA).
- Further development of efficient methods for iterating transducers.
- Analysis and synthesis of distributed monitors and controllers.

Testing

- A disadvantage is of dynamic fault trees (DFTs) is that is requires some extra modeling effort: an engineer has to specify a DFT, whereas many pieces of information needed for reliability is already present in the system architecture. Hence, we would like to generate DFTs or other reliability models automatically from the architecture. Furthermore, we plan to develop Monte Carlo simulation techniques for DFTs. Whereas simulation only provides approximate answers to reliability questions (ie the precision lies within the given confidence interval), it is usually much faster than exact techniques.
- We plan to implement the semantic framework test coverage in a tool called secco. We will do several case studies, comparing semantic coverage with other coverage measure, in particular with mutation coverage.
- Improvement of the STG tool and more case studies.

- Coverage-based test generation with semantical notions of coverage using dynamic partitioning. Implementation in STG.
- Continue the activity on the combination of testing and learning.
- Methodological combination of verification and test selection for safety properties.

Abstraction and Approximate Analysis

- Define suitable abstractions between (priced) timed game guaranteeing that winning strategies synthesized on a more abstract game are also winning for more concrete games. In particular, user-supplied abstract games may lead to efficient treatment og timed games under partial observatility (where the lack of full observability adds with an exponential increase in complexity).

Robustness and Quantitative Analysis

- Further study of metrics on stochastic games. In particular game metrics enable approxmat reasoning on games replacing boolean (yes/no) answers with quantitative verdicts. In this way the verification process robust to small pertubations.
- Qualitative and quantitative verification on probabilistic models for the reliability of embedded systems.

Controller Synthesis and Optimal Scheduling

- Further developments on synthesis of robust controllers (incomplete information) for timed automata and implementation in the tool UPPAALA Tiga.
- Implementation of on-the-fly algorithms for synthesis for priced timed games. This requires substantial work on extending the underlying datastructures and algorithsm from zones to polyhedra.
- Settle decidability issues for priced timed games under partial observability.

3.2 Current and Future Milestones

We call from last years deliverable (D24-TV-Y2) the current milestones:

> **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.

As is clear from Section 1.5 a significant amount of research has been carried out with respect to development of efficient algorithms for controller synthesis. In particular the work using the lattice-theoretic approach points to truly significant gains in performance for model-checking of finite state systems compared with existing implementations. For priced games the division between decidability and undecidability is now made more clear leaving only the case of models with 2 clocks open. For pure timed games efficient implementations of on-the-fly synthesis has been obtained.

Robust model checking (replacing simple boolean answers with quantitative verdicts) has been developed as well as methods for coverage-based test selection. The anticipated work on code generation has not been pursued, the main reason being that the STREPS proposal that would have funded this work for many cluster partners was not granted in the last FP6 Call. In the mean time, an improved project proposal has been submitted and accepted for the first Call of FP7 (Quasimodo), so that this work can now be commenced. Work on improving

(academic) tools for test generation by using verification tools has been conducted as foreseen, including using timed games for synthesizing test strategies for given test purposes.

Link between academic and industrial tools has been demonstrated (in particular linking UPPAAL Tiga with Simulink.

The milestones for Year 4 are as follows:

Year4: **Completion of efficient tool components for controller synthesis. Initiation of work on property-preserving code generation and industrial applications. Development of generic framework using abstraction and compositionality for efficient analysis of quantitative models.** Emergence of a range of new powerful debugging and analysis techniques based on various combinations of testing and verification techniques.

3.3 Indicators for Integration

A significant sign of integration is the succesful STREP proposal Quasimodo in which several partners of the cluster take part and will will pursue several of the challenges identified by the activity.

Also, as indicated by the concrete list of interations reported in section 2.3.3 and the numerous joint publications listed in section 2.3.4 the partners have established long-term and extensive collaborations on all the topics covered by the activity.

3.4 Main Funding

- Centre for Embedded Systems, CISS (http://ciss.auc.dk/),
- BRICS (http://www.brics.dk/).
- The project MoDES under the ICT programme NABIIT under the Danish Strategic Research Council.
- The HighTech Platform DaNES sponsored by the Danish Advanced Technology Foundation.
- Dutch national projects STRESS, HaaST, IMPASSE, MC=MC, CASH (see http://fmt.cs.utwente.nl/),
- Czech project on distributed model checking: ParaDice.
- Danish national project MoDES
- French national project ACI CORTOS: Control and Observation of Real-Time Open Systems
- 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.

4. Internal Reviewers for this Deliverable

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