IST-214373 ArtistDesign

Network of Excellence

on Design for Embedded Systems

Activity Progress Report for Year 2

Validation

Cluster:

Modeling and Validation

Activity Leader:

Professor Kim G. Larsen (CISS, Aalborg University)

http://www.cs.aau.dk/~kgl

Policy Objective (abstract)

The objective is to address the growth in complexity of future embedded products while reducing time and cost to market requires methods allowing for early exploration and assessment of alternative design solutions as well as efficient methods for verifying final implementations. This calls for a range of model-based validation techniques ranging from simulation, testing, model-checking, compositional techniques, refinement as well as abstract interpretation. The challenge will be in designing scalable techniques allowing for efficient and accurate analysis of performance and dependability issues with respect to the various types of (quantitative) models considered. The activity brings together the leading teams in Europe in the area of model-based validation.

Versions

number	comment	date
1.0	First version delivered to the reviewers	December 18th 2009

Table of Contents

1. Overview of the Activity

1.1 ArtistDesign participants and their role within the Activity

Jan Tretmans (ESI - Netherlands);
Testing, performance analysis, predictability..

Werner Damm (OFFIS - Germany);
formal analysis techniques, mainly on compositional techniques regarding safety and real, and deployment synthesis.

Tom Henzinger (EPFL - Switzerland);
Rich interface theory for component-based design. Algorithms for checking quantitative reliability measures of implementations. Compositional code generation for time-triggered architectures. Algorithms for stochastic and timed games.

Thierry Jéron, Bertrand Jeannet (INRIA - France);
Models with data and time for model-based test selection and coverage criteri. qualitative *and quantitative verification, control synthesis.*

Christoph Kirsch (Salzburg - Austria)*;*
Compositional Compositional timing and reliability validation in Giotto-inspired languages and systems

Kim Larsen (Aalborg - Denmark);
Quantitative verification, synthesis, performance evaluation and model-based testing for timed automata and games with priced and probabilitistic extensions.

Prof. Alberto Sangiovanni-Vincentelli, Scientific Director, PARADES, Italy.
Platform-Based Design, the Metropolis and COSI frameworks, industrial applications and international activities.

Prof. Roberto Passerone, University of Trento (Italy)
Formal analysis of heterogeneous composition, abstract algebra, and metamodeling.

Joseph Sifakis – VERIMAG (France)
Contributions of his team: component-based design, the BIP framework, platform-aware implementation of embedded systems, structural verification

Saddek Bensalem – VERIMAG (France)
Contributions of her team: structural analysis.

Oded Maler – VERIMAG (France)
Contribution *of his team: timing analysis, scheduling and hybrid systems*

Prof. Martin Törngren, Prof. Axel Jantsch, KTH, Stockholm, Sweden
Integrated models supporting cross-layer validation. Methods for validation of self-configuring systems.Compositional validation of integrated models/components..

Wang Yi (Uppsala - Sweden);
Scheduling and Verification (UPPAAL and TIMES), Combination of State-Based and Analytical Analysis Techniques (CATS tool)

Christophe Gaston
compositional validation, CEA symbolic execution of models of heterogeneous systems as a basis for testing or model checking activities

-- Changes wrt Y1 deliverable --

Contact person for ESI has been changed due to the leave of Ed Brinksma; roles of INRIA, Uppsala and Salzburg have been updated. Oded Maler and Saddek Bensalem have been added to the persons contributing from VERIMAG. .Alberto Sangiovanni Vincentelli transitioned from PARADES to University of Trento and University of Trento became a partner.

1.2 Affiliated participants and their role within the Activity

Prof. Yiannis Papadopolis, Univ. Of Hull (UK)
Compositional safety analysis and design optimization w.r.t. safety.

Ahmed Bouajjani - LIAFA (France)
Real-time and hybrid model checking

Stavros Tripakis – Cadence Research lab (USA)
Monitoring and test of real-time properties

Pierre Wolper and Jean-Francois Raskin (CVF – Belgium);
Efficient Model-checking of linear-time properties.
Verification and synthesis for reactive systems. Timed and hybrid automata.

Joost-Pieter Katoen (Aachen – Germany)
Model checking of quantitative system properties. Verification of (continuous-time) probabilistic and stochastic systems.

Prof. Dr. Holger Hermanns (Saarland U – Germany);
Probabilistic and stochastic model checking.

Christel Baier (Dresden – Germany);
Probabilistic and stochastic model checking

Patricia Bouyer, Nicola Markey and Phillippe Schnoebelen (LSV Cachan – France),
Decidability and algorithms for priced timed automata and games.
Algorithms for solving games of imperfect information

Prof. Roderick Bloem (TU Graz)
Algorithms for controller synthesis

Prof. dr. ir. Wil van der Aalst, professor at Eindhoven University of Technology, The Netherlands.

Information System. Affiliated participant in the ESI Octopus project.

Prof. dr. Mehmet Aksit, professor at Twente University, The Netherlands.

Software Engineering. Affiliated participant in the ESI Darwin project.

Prof. dr. Sandro Etalle, professor at Eindhoven University of Technology, The Netherlands.

Security. Affiliated participant in the ESI Darwin project.

Prof. dr. Arjen van Gemund, professor at Delft University of Technology, The Netherlands. Embedded Software Laboratory.

Affiliated participant in the ESI projects Trader and Octopus.

Prof. dr. Frits Vaandrager, professor at Radboud University, The Netherlands.

Formal methods. Affiliated participant in the ESI Octopus project.

Prof. dr. Hans van Vliet, professor at Vrije Universiteit Amsterdam, Software Engineering.

Affiliated participant in the ESI Darwin project.

Prof. dr. Jack van Wijk. professor at Eindhoven University of Technology, The Netherlands.

Visualization. Affiliated participant in the ESI Poseidon project.

Peter Habermehl – LIAFA (France)

verification of programs with arrays and dynamic data structures

-- Changes wrt Y1 deliverable --

Peter Habermehl has been added as new affiliate partner.

1.3 Starting Date, and Expected Ending Date

Starting date: January 1st 2008

Expected ending date: the activity is intended to continue beyond the end of the project (December 2011). The needs for new techniques (algorithms and data structures) for verifying and analysing system models that incorporate both functional and quantitative aspects (such as safety requirements, timing, resource constraints, reliability, etc.) are expected to continue increase in the next decade. Moreover, the feedback from the concrete applications should give to this activity new directions to investigate for researchers, most likely beyond the duration of the project.

-- Changes wrt Y1 deliverable --

No changes with respect to Year 1.

1.4 Policy Objective

The objective is to address the growth in complexity of future embedded products while reducing time and cost to market requires methods allowing for early exploration and assessment of alternative design solutions as well as efficient methods for verifying final implementations. This calls for a range of model-based validation techniques ranging from simulation, testing, model-checking, compositional techniques, refinement as well as abstract interpretation. The challenge will be in designing scalable techniques allowing for efficient and accurate analysis of performance and dependability issues with respect to the various types of (quantitative) models considered. The activity brings together the leading teams in Europe in the area of model-based validation.

-- Changes wrt Y1 deliverable --

No changes with respect to Year 1.

1.5 Background

By far the most common validation technique applied in embedded industrial today is based on rather ad-hoc and manual (hence quite error-prone) testing. Given that some 30-50% of the overall development time and cost are related to testing activities it is clear that the impact of improved validation technologies is substantial. Given this current industrial practice the academic state-of-the-art has a lot to offer. In particular the cluster combines the efforts and skills on of the individual leading researchers in Europe into a world-class virtual team for advancing the state-of-the-art and industrial take-up of model-based validation techniques.

Whereas validation techniques for assessing functional correctness have reached a certain level of maturity and industrial acceptance, there is a need for mature validation techniques addressing quantitative aspects (e.g. real-time, stochastic and hybrid phenomena) being accessible from within industrial tool-chains. Thus, particular effort should be made to transfer of validation methods and tools to industry, including integration of the techniques developed into existing tools.

-- Changes wrt Y1 deliverable --

No changes with respect to Year 1.

1.6 Technical Description: Joint Research

The joint research falls into the following three sub-activities:

A Compositional validation:
The complexity of a given analysis method is not only determined by its accuracy (and issues addressed) but mainly by the sheer size of the model analysed measure in number of components, tasks, variables, etc. In order to achieve methods which scale to the need of industry *compositionality* is paramount. That is, it should be possible for composite models to be interrelated and properties to be inferred only by consideration of the components of the models and their interfaces. In the presence of composite models with heterogeneous components – in particular involving components where quantitative aspects are considered – this is a challenge that has not yet been dealt with satisfactory.

B Quantitative validation:

Whereas functional validation addresses issues concerning logical correctness with respect to stated temporal specifications, quantitative validation takes the quantitative aspects into account. For embedded systems applied in safety-critical applications hard real-time guarantees are often imperative. For embedded systems in less critical applications performance and QoS are often more important properties: in this case the quantitative validation should return a value as to the "quality" of the model with respect to a given relevant metric, e.g. expected energy consumption pr time-unit. The quantitative aspects to be dealt with involve real-time, stochastic and hybrid phenomena. Also joint work on software verification, and more particularly on modelling and verification of quantitative properties of programs using integer arrays has been made, as well as work joint work on the evaluation of performance properties by connecting the DOL performance analysis and BIP

C Cross-layer validation

During the design trajectory, the software engineer will create, refine and make use of several models of the same system focusing on different aspects and varying in terms of particular to transfer properties established of one (early) model to properties guaranteed to hold of other (later) models without any additional effort.

Techniques for validating the conformance between design models and executing code (on particular platforms) are particular important. This includes considerations of (robust) methods for automatic code generation as well as methods for synthesizing controllers from plant models and control objectives.

In order for validation methods to be industrial applicable it is essential that existing (or thirdparty) code may be dealt with. Here software verification techniques (combining static analysis and model checking) need to be extended to involve quantitative aspects.

-- Changes wrt Y1 deliverable --

No changes with respect to Year 1.

1.7 Work achieved in Year 1

The following provide a high-level description of the work achieved in Year 1:

Within the sub–activity A "Compositional Validation", we focused on methods for deriving functional as well as non-functional properties of composite systems from properties of their components. In particular compositional approaches dealing with timing properties as well as safety, failure and reliability was addressed. Also, validation methods based on abstractions and refinements were developed.

Within the sub-activity B "Quantitative Validation", we provided (un)decidability results as well as efficient datastructures and algorithms supporting the validation of a number of non-functional models (e.g. Markov chains, timed automata, priced timed automata, memory models involving stacks and queues, linear hybrid systems) as well as their interrelation.

Within the sub-acitivity C "Cross-layer Validation", main effort was made towards controller synthesis from rich game models as well as conformance testing of non-functional propeties.

-- No changes wrt Y1 deliverable --

The above text was already presented in the Y1 deliverable, as part of the sections 1.7 and 3.1.

1.8 Problem Tackled in Year 2

Within the sub–activity A "Compositional Validation", we have worked on combining state-based and analytical methods to develop scalable compositional techniques for performance analysis and verification of timed systems. Also a number of compositional development and verification frameworks for timed and stochastic systems have been put forward allowing to infer in a compositional manner that programs exhibit predictable behaviour. Development of symbolic execution of heterogeneous systems and a symbolic execution framework devoted to system models defined recursively by interconnecting heterogeneous component models has been made. Finally work has continued its work on deadlock detection/verification and its implementation in the D-Finder tool by checking incrementally deadlock-freedom of component-based systems described as the composition of interacting components is proposed.

Within the sub-activity B "Quantitative Validation", a substantial amount of work from different partners has been made on schedulability and execution time analysis for multiprocessor platforms with pipelines and shared caches. New tools supporting verification of quantitative models combining both timing and stochastic properties have been developed. We have applied three-valued abstraction techniques for probabilistic systems showing that certain abstractions provide rather tight bounds. We have developed methods for verification of programs with arrays and dynamic data structures, investigated improved widening techniques for the abstract interpretation of numerical programs with polyhedra with the purpose of analysing Linear Hybrid Systems, and developed extendable tools for verification of hybrid systems.

Within the sub-acitivity C "Cross-layer Validation", we have continued the effort on controller synthesis from rich game models and from models with partial observability. Work conformance testing of non-functional properties has also been continued. New effort has been made on model learnability from experimentation. Also tools for establishing refinement between specification at different abstraction levels have been developed. Work on translations from real-time temporal logics to deterministic timed automata in the context of synthesis of real-time controllers as well as work on verifying real-time models with respect to scenario-based specifications constitutes contributions to cross-layer validation.

-- The above is new material, not present in the Y1 deliverable --

2. Summary of Activity Progress in Year 2

2.1 Technical Achievements

Sub-activity A: Compositional Validation

Compositional timing analysis (Verimag):

VERIMAG developed a compositional approach for timing analysis intended to avoid the state- and clock-explosion in the analysis of timed automata. The essence of this technique is to augment a timed component with auxiliary input clocks that are rest upon event occurrence. Then the reachability graph is computed for this model, followed by a projection on the input clocks, hiding and minimization. As a result we obtain a timed automaton, much smaller than the original, which over-approximates the timed I/O behavior of the component. This technique has been implemented within the IF framework and has been applied to a case study involving a wave-pipelining circuit subject to input with jitter [BBM09].

Compositional Verification for Component-based Systems (Verimag):

Verimag continued working on the *BIP verification engine* (http://www-verimag.imag.fr/~async/BIP/bip.html) which realizes compositional deadlock detection / verification. The methods that we started to develop have been significantly improved and implemented in the Deadlock Finder tool by combining structural analysis for component behaviours with structural analysis of connectors.

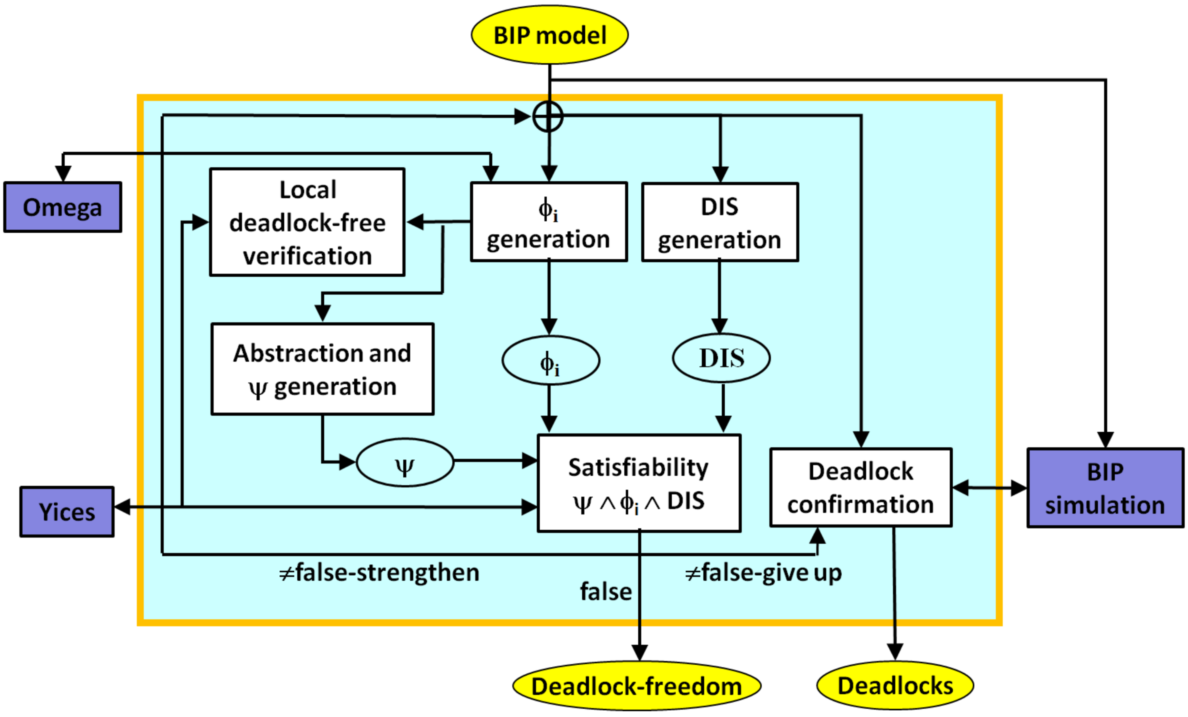


Figure 1 Functional view of the D-finder tool

In a previous work we presented a different work. It allows deadlock verification using structural analysis. It takes as input a BIP model and computes component invariants φ_i. This step may require quantifier elimination using the tool Omega. Then, it checks for deadlock-freedom based on the set of computed component invariants: it computes an abstraction of the model derived from the invariants φ, and it then computes interaction invariants ψ for this abstraction.

Then, it checks the satisfiability of the conjunction of ψ and φ_i and the predicate DIS (characterizing the set of the states in which no interaction is enabled) using the satisfiability checker Yices. If this conjunction is unsatisfiable, then there is no deadlock. Else, D-finder either generates stronger component and interaction invariants, or tries to confirm the detected deadlocks by using reachability analysis techniques.

In [BBNS09], we propose a new method for checking incrementally deadlock-freedom of component-based systems described as the composition of interacting components is proposed. It improves the method applied by the D-Finder tool based on the computation of global invariants of composite components as solutions of a set of boolean behavioral constraints. These are induced by interactions on transition relations of the composed components.

Compositional and modular analysis tool for timed systems (Uppsala)

To combine UPPAAL (state-based tool) with the RTC (Real-Time Calculus) a tool named CATS (http://www.timestool.com/cats) has been developed at Uppsala. CATS is a tool for compositional timing and performance analysis of timed systems modeled using timed automata and the real-time calculus. It is based on an approximation technique in which a timed automaton is abstracted as a transducer of abstract streams described by arrival curves from network calculus. The tool is implemented as a set of plugins for Eclipse Integrated Development Environment.

Timed Modal Specifications (INRIA)

In the application domain of component-based system design, developing theories which support compositional reasoning is notoriously challenging. In [BPR09] and [BLPR09] we define timed modal specifications, an automata-based formalism combining modal and timed aspects. As a stepping stone to compositional approaches of timed systems, we define the notions of refinement and consistency, and establish their decidability.

Abstractions and Model checking of Markovian Models (Aachen)

We have applied three-valued abstraction techniques for probabilistic systems, in particular interval MDPs and their continuous-time variants, to case studies from systems biology and queuing networks. It has been shown that certain abstractions provide rather tight bounds. For tree-based queuing networks (that are strongly related to probabilistic pushdown automata), excessive state-space reductions have been achieved while preserving very good accuracy. In addition, we have considered compositional abstraction techniques
for interactive Markov chains.

Finally, we have shown that model checking of continuous-time Markov chains against linear real-time specifications given as deterministic timed automata can be reduced to computing reachability probabilities in piecewise deterministic Markov processes. We also developed an algorithm to determine the (time-dependent) policy that maximises (or, dually minimises) the probability to reach a set of target states within a deadline in continuous-time MDPs.

Distributed and Modular HTL (Salzburg + Uni. Porto + IST Austria + Uni. Trento)

The Hierarchical Timing Language (HTL) is a real-time coordination language for distributed control systems. The desired key property of HTL programs is time-determinism, meaning that their functional and temporal behavior is repeatable (for every timed sequence of inputs, there is a unique timed sequence of outputs). HTL compilation proceeds in the following steps; (1) it checks whether an HTL program is time-deterministic on a given, possibly distributed target platform and (2) it generates code that runs of that particular platform. The time-determinism of an HTL program is ensured by checking well-formedness of its syntax, race-freedom of communicator updates, transmission-safety (schedulability of cross-host communication) and time-safety (schedulability of host computation). It follows that race-free, transmission-safe and time-safe execution of well-formed programs is time-deterministic, that is, the computed values and update times of communicators are input-determined and therefore predictable.

In this work, we proposed a modular abstract syntax and semantics for HTL. We also developed modular checks for well-formedness, race-freedom, transmission-safety and modular code distribution. The last point is based on the modular transmission safety check, ensuring that each communicator value can be communicated within a single communicator period. Our contributions complete the distributed and modular design of HTL, except for time safety checking of top-level programs, which remains non-modular. Modularity in HTL is important for design scalability but also enables efficient program modifications at runtime, called runtime patches, while maintaining predictable behavior [HKMS09].

Compositional Safety Analysis (KTH with University of Hull and Volvo)

The automotive industry has a growing demand for the seamless integration of safety analysis tools into the model-based development tool-chain for embedded systems. This requires translating concepts of the automotive domain to the safety domain. We automate such a translation between the automotive architecture description language EAST-ADL2 and the safety analysis tool HiP-HOPS by using model transformations and by leveraging the advantages of different model transformation techniques.

In this work we have shown how we integrated the safety analysis tool HiP-HOPS into the automotive model-based development based on EAST-ADL2. We used different model transformation techniques to translate the relevant information from the automotive domain to the safety analysis domain. This link enables early safety analysis. Through this integration, the analysis can be conducted early in the development process, when the system can be redesigned to fulfil safety goals with relatively low effort and cost. The safety analysis techniques relies on so called error models which are specified for each component (and which may be used for components at different levels of abstraction). An error model constitutes a so called interface failure mode and effects analysis (FMEA) model.
Based on such component models, fault-trees for an entire system considering different system failure modes can be automatically generated. Based on the fault-models in turn, cut-set analysis and other types of assessments can be performed.

The work is still ongoing, and publications are under way. The resulting tool plugin is used in further work within the ATESST2 project. Further work will also explore back-annotating results from the safety analysis into the EAST-ADL2 models.

Compositional verification of probabilistic systems (CISS)

A specification theory combines notions of specification and implementation with a satisfaction relation, a refinement relation and a set of operators that together support stepwise design. We propose a new abstraction, Constraint Markov Chains, and use it to construct a specification theory for Markov Chains. Constraint Markov Chains generalize previously known abstractions by allowing arbitrary constraints on probability distributions. Our theory is the first specification theory for Markov Chains closed under conjunction, parallel composition and synchronization. Moreover, all the operators and relations introduced are computable.

Heterogeneous Composition
(TRENTO + IST + Chennai Mathematical Institute, + UC Berkeley)

In the area of heterogeneous composition, TRENTO and IST have been collaborating with Praskash Chandrasekaran, a Research Scholar at the Chennai Mathematical Institute, Chennai, India. The activities have been centered around the development of a formal model for specifying heterogeneous systems, based on the Coordinated Concurrent System (CCS) notation. In this activity, which is reported in more details in deliverable D1.1-Y2, we have extended our previous examples of heterogeneous interaction. In particular, we have addressed the definition of an interface process between an untimed model of computation and a timed one. Here, we have used Khan Process Networks (KPN) as an example for an untimed data flow model, and Finite State Machines (FSM) as a model for synchronous timed communication based on signals. In this work we have developed techniques to synthesize an interface between KPNs and FSMs, with some restrictions on the language of the FSMs. This work extends our previous investigation by identifying a common semantic domain, the CCS, which we use to develop our interface process between the incompatible models. We take this a step further, and use the model to specify global properties that we want the system to exhibit, with particular attention to end-to-end communication and interaction properties. This way, we take advantage of the existing connection to the Uppaal model checker from CCS to provide means to verify the correctness of the heterogeneous system composition.

Sub-activity B: Quantitative Validation

Automatic verification of programs with integer arrays (Verimag, LIAFA)

Arrays are an important data structure in all common programming languages. Automatic verification of programs using arrays is a difficult task since they are of a finite, but often not a priori fixed length, and, moreover, their contents may be unbounded too.

We have developed a verification technique for a class of programs working on integer arrays of finite, but not a priori bounded length [BIH*09]. We use the logic of integer arrays SIL (Single-Index Array Logic) to specify pre- and post-conditions of programs and their parts. Effects of non-looping parts of code are computed syntactically on the level of SIL. Loop pre-conditions derived during the computation in SIL are converted into counter automata (CA). Loops are automatically translated purely on the syntactical level to transducers. Pre-condition CA and transducers are composed, and the composition over-approximated by flat automata with difference bound constraints, which are next converted back into SIL formulae, thus inferring post-conditions of the loops. Finally, validity of post-conditions specified by the user in SIL may be checked as entailment is decidable for SIL [BIH*09].

Analysis of Energy related properties of sensor Networks (VERIMAG + FT)

VERIMAG worked on analysis techniques to estimate the energy consumption of embedded systems. We applied these techniques in the context of Wireless Sensor Networks (WSN). Indeed, large scale industrial deployment of a WSN still requires to lowering the energy consumption in order to achieve long-term network lifetimes (typically more than 10 years). Hence, every layer of a WSN application (node hardware, communication protocols, auto-organization mechanisms) should be specifically designed to run in an utmost energy efficient manner.

We addressed this problem by developing accurate prototypes of WSNs, that can be formally analyzed, and that can be transformed by dedicated abstraction mechanisms, able to simplify the model complexity while preserving (or at least over-approximating) the energy consumption. During the past year, we have improved the ***Glonemo*** simulator (http://www-verimag.imag.fr/~samper/Glonemo/). This simulator can handle networks of up to several hundred thousands nodes, on typical monitoring application, running models of existing communication protocols (for the MAC and routing levels), while precisely evaluating the energy consumption of each node. We enhanced the simulator to allow modelling and simulation of more complex protocols. The whole simulation framework could be validated on a real WSN application deployed by France-Telecom consisting on about 100 sensor nodes communicating through a pseudo-geographic Mac/routing combined protocol (based on virtual coordinates). We also developed a theoretical framework to perform component-based abstractions of a WSN while preserving (over-)approximations of energy consumptions and we defined an efficient decision procedure for checking the energy-preserving abstraction relation we proposed.

This work, carried out within the RNTL ARESA project will be continued in ARESA-2 with a special emphasis on security for WSN. Our intention here is to evaluate the energy overhead induced by classical security solutions, and to adapt them to the specific context of WSN. We intend to use the ARESA techniques, to explore new event-driven and asynchronous software and hardware architectures, tailored to extremely low power consumptions; propose new communication and organization protocols, optimized in terms of energy consumption and robustness and study new network structures which facilitate auto-organization.

http://www-verimag.imag.fr/SYNCHRONE/index.php?page=fiche-aresa

Improved widening techniques for the abstract interpretation of numerical programs with polyhedra (Verimag)

Verification of numerical code is an important problem in embedded systems since computational artifacts such as overflow and error accumulation are not present in the idealized models used for algorithm design, can lead to unexpected and possibly catastrophic consequences in many applications. We apply a static analysis technique for polyhedral domains to compute bounds on the variables in numerical code with linear arithmetic, and developed a new widening operator that can be more precise than standard widening for iterative computations. Some minor but effective heuristics are used to reduce the size of the model and speed up the analysis. The results have been published in [MFK09]

Development of an extendable verification tool for hybrid systems (VERIMAG)

The verification of continuous and hybrid systems is known to be hard, and today tools are limited to relatively small problems. Several novel approaches are currently under investigation that exploit various kinds of set representations (polyhedra, zonotopes), improved algorithms (avoiding the wrapping effect) and strategies (such as abstraction refinement). We developed a tool framework that is able to integrate and combine different elements from these approaches. The framework includes implementations for common functionality (hybrid automata, graphical output, basic set operations, etc.) and interfaces that allow us to plug in different implementations, such as a particular kind of set representation or a particular optimization algorithm. This allows us to experimentally evaluate competing ideas, combine promising elements and explore new approaches with relatively little development effort. The tool architecture and preliminary results have been published in [FR09]

New Response Time Bounds for Fixed Priority Multiprocessor Scheduling (Uppsala)

This work will be presented at RTSS 2009. We have developed a new technique for the estimation of worst-case response times on multiprocessor systems using fixed priority scheduling. The technique is proven to dominate theoretically state-of-the-art techniques for multiprocessor systems. Our experiments also show that the technique results in significant performance improvement compared with several existing techniques for multiprocessor schedulability analysis. The technique can also deal with task systems with arbitrary deadlines. This is a non-trivial extension even for single-processor systems. To our best knowledge,this is the first work for multiprocessor systems in this setting, which involves sophisticated techniques for the characterization and computation of response time bounds.

Partitioning the shared caches on multicores for timing predictability (Uppsala)

This work is presented at EMSOFT 2009. The major obstacle to use multicores for real-time applications is that we may not predict and provide any guarantee on real-time properties due to the on-chip shared resources such as L2 cache. In this work, we propose to use cache space isolation techniques to avoid cache contention for hard realtime tasks running on multicores with shared caches. We have presented a scheduling strategy for real-time tasks with both timing and cache space constraints, which allows each task to use a fixed number of cache partitions, and makes sure that at any time a cache partition is occupied by at most one running task. In this way, the cache spaces of tasks are isolated at run-time. We have developed a sufficient schedulability test for non-preemptive fixed-priority scheduling for multicores with shared L2 cache, encoded as a linear programming problem. Our experiments show that the test which employs an LP solver can easily handle task sets with thousands of tasks in minutes using a desktop computer.

Fixed-Priority Multiprocessor Scheduling with Liu & Layland's Utilization Bound (Uppsala)

This work is submitted to RTAS 2010. Liu and Layland discovered the famous utilization bound for fixed-priority scheduling on single-processor systems in the 1970s. Since then, it has been a long standing open problem to find fixed-priority scheduling algorithms with the same bound for multiprocessor systems. In this work, we have developed a partitioning-based fixed-priority multiprocessor scheduling algorithm with Liu and Layland's bound.

Probabilistic acceptors on infinite words (INRIA)

In [BBG09] we define Probabilistic omega-automata which are variants of nondeterministic automata for infinite words where all choices are resolved by probabilistic distributions. Acceptance of an infinite input word requires that the probability for the accepting runs is positive. We provide a summary of the fundamental properties of probabilistic omega-automata concerning expressiveness, efficiency, compositionality and decision problems

Qualitative Determinacy and Decidability of Stochastic Games with Signals (INRIA)

In [BBG09] we consider the standard model of finite two-person zero-sum stochastic games with signals. We are interested in the existence of almost-surely winning or positively winning strategies, under reachability, safety, Büchi or co-Büchi winning objectives. We prove two qualitative determinacy results. First, in a reachability game either player 1 can achieve almost-surely the reachability objective, or player 2 can ensure surely the complementary safety objective, or both players have positively winning strategies. Second, in a Büchi game if player 1 cannot achieve almost-surely the Büchi objective, then player 2 can ensure positively the complementary co-Büchi objective. We prove that players only need strategies with finite-memory, whose sizes range from no memory at all to doubly-exponential number of states, with matching lower bounds. Together with the qualitative determinacy results, we also provide fix-point algorithms for deciding which player has an almost-surely winning or a positively winning strategy and for computing the finite memory strategy. Complexity ranges from EXPTIME to 2-EXPTIME with matching lower bounds, and better complexity can be achieved for some special cases where one of the players is better informed than her opponent.

Determinization of timed automata (INRIA)

In [BBBB09], we propose an abstract procedure which, given a timed automaton, produces a language-equivalent deterministic infinite timed tree. We prove that under a certain boundedness condition, the infinite timed tree can be reduced into a classical deterministic timed automaton. The boundedness condition is satisfied by several subclasses of timed automata, some of them were known to be determinizable (event-clock timed automata, automata with integer resets), but some others were not. We prove for instance that strongly non-Zeno timed automata can be determinized. As a corollary of those constructions, we get for those classes the decidability of the universality and of the inclusion problems, and compute their complexities (the inclusion problem is for instance EXPSPACE-complete for strongly non-Zeno timed automata).

Representation of infinite state systems (INRIA)

In [M09] we study external characterisations of infinite state systems, which avoid explicit naming of the vertices. Such characterisation are mostly defined via graph transformations. We present two kinds of external characterisations: deterministic graph rewriting, which in turn characterise regular graphs, deterministic context-free languages, and rational graphs. Inverse substitution from a generator (like the complete binary tree) provides characterisation for prefixrecognizable graphs, the Caucal Hierarchy and rational graphs. We illustrate how these characterisations provide an efficient tool for the representation of infinite state systems.

Logical reliability validation (Salzburg)

Existing logical reliability validation works with a previous version of HTL with a non compositional semantics. Salzburg is continuing to work, now with the University of Porto and IST Austria, on reliability validation in modular HTL, which has a fully compositional semantics.

Programmable temporal isolation (Salzburgh)

A software process is temporally isolated if its timing behavior does not depend on any other concurrently running processes. Temporal isolation is programmable if the timing behavior of processes can be changed at runtime. Salzburg has recently worked on a real-time scheduling system called variable-bandwidth servers (VBS) consisting of a scheduling algorithm and a schedulability test for programmable temporal isolation of software processes. VBS can also be used to implement workload-oriented programming, which has been developed as part of the modeling activity. There is also preliminary work on how to integrate VBS into virtual execution environments in order to enable programmable temporal isolation in virtualized process execution. The work on programmable temporal isolation is a new activity.

Program Analysis: Invariant and Type Inference for Matrices (Salzburg)

We developed a loop property generation method for loops iterating over multi-dimensional arrays. When used on matrices, our method is able to infer their shapes (also called types), such as upper-triangular, diagonal, etc. To generate loop properties, we first transform a nested loop iterating over a multidimensional array into an equivalent collection of unnested loops. Then, we infer quantified loop invariants for each unnested loop using a generalization of a recurrence-based invariant generation technique. These loop invariants give us conditions on matrices from which we can derive matrix types automatically using theorem provers. Invariant generation is implemented in the software package Aligator and types are derived by theorem provers and SMT solvers, including Vampire and Z3. When run on the Java matrix package JAMA, our tool was able to infer automatically all matrix types describing the matrix shapes guaranteed by JAMA's API [HHKV10].

Property-based Validation of Mixed-Signal Systems (IST Austria)

In this work, we applied a property-based validation framework to a real-world industrial analogue design. This framework proposes a formal high-level specification language, *signal temporal logic* (STL), a high-level specification language that allows expressing temporal properties of continuous and timed (Boolean) signals. STL is an extension of the real-time *metric interval temporal logic* MITL, where continuous signals are transformed into Boolean ones using numerical predicates, and the temporal relations between them are expressed using standard real-time temporal operators whose atomic propositions correspond to those predicates. Arbitrary STL properties are then automatically translated into property monitors that, given a set of simulation traces, check whether the traces satisfy the property. This framework narrows the gap between formal verification and standard simulation analysis of mixed-signal systems by providing a formal and mathematically precise language for the specification of system properties and automating the validation process.

The subject of this case study was a DDR2 memory interface developed at Rambus. The memory interface acts as a bus that interconnects the memory to other components in the design and exhibits the communication of digital data implemented at the analogue level. We identified two important properties that are part of the official DDR2 specification document. These properties were translated from their informal English description into STL specifications. The STL properties were automatically translated into monitors and checked against a set of simulation traces provided by the DDR2 designers.

The experimental evaluation of the case study showed that the property-based validation framework is applicable to analogue and mixed-signal designs, in particular for properties that relate the timing between “events” in analogue and Boolean signals. The translation from STL specifications to property monitors, and the monitor runtime against simulation traces induce negligible computational overhead. The framework was shown to be useful especially at the system integration phase, where analogue and digital components are integrated together and designers need to check the correctness of their interface. The methodological evaluation showed that the specification language needs further extensions in order to match specific needs of mixed-signal designers [JKN09].

Automata-based Approach to Model-Checking (IST Austria, CVF)

We propose and evaluate antichain algorithms to solve the universality and language inclusion problems for non-deterministic Buchi automata, and the emptiness problem for alternating Buchi automata. To obtain these algorithms, we establish the existence of simulation pre-orders that can be exploited to efficiently evaluate fixed points on the automata defined during the complementation step (that we keep implicit in our approach). We evaluate the performance of the algorithm to check the universality of Buchi automata using the random automaton model. We show that on the difficult instances of this probabilistic models, our algorithm outperforms the standard ones by several orders of magnitude [DR09].

From Real-time Specifications to Deterministic Timed Automata (IST Austria)

Building predictable systems has been identified as one of the main challenges in the embedded systems design in [Hen08]. The predictability of a system is defined as a form of determinism, and in particular time-determinism for embedded programming. In this work, we considered building deterministic real-time systems from high-level specifications. In particular, we studied the translation from real-time *metric temporal logic* (MTL) and *metric interval temporal logic* (MITL) to deterministic timed automata.

Our construction from MITL or MTL formulae to deterministic automata works under the assumption that there is a bound on the number of changes in the input signal in a given time interval. In order to achieve this result, we take a novel approach in which we separate our timed automaton into two parts: (1) the first automaton is a standard deterministic timed automaton. It reads input signals, and uses clocks to record times at which the input signal changes. The bounded variability assumption gives us a bound on the number of clock that can be active at any time, and (2) the second automaton is what we called a *dependent timed automaton (DTA)*, which is allowed to read clocks controlled by the first automaton. The DTA can make *discrete* predictions about the future. Although a DTA passively uses clocks by reading their values, it is essentially an untimed automaton.

The above-described separation of our timed automaton into a timed and an untimed part, allows us to use a slight variant of the standard determinization of untimed finite automata on infinite words. Essentially, only the only non-determinism that needs to be resolved are the discrete predictions made by the DTA. This results in a procedure that translates MTL and MITL formulae, with bounded variability assumption, into deterministic timed automata, that can be used to derive *predictable* implementations of real-time controllers [NP09].

Concurrent and Stochastic Games (IST Austria)

In this work, we surveyed stochastic games with limsup and liminf objectives. A stochastic game is a two-player game played on a graph, where in each state the successor is chosen either by one of the players, or according to a probability distribution. A real-valued award is assigned to each state, and the value of an infinite path is the limsup (resp. liminf) of all rewards alog the path. The value of a stochastic game is the maximal expected value of an infinite path that can be achieved by resolving the decisions of the first player. We presented the complexity of computing values of stochastic games and their subclasses, and the complexity of optimal strategies in such games [CDH09].

We also considered concurrent games played on graphs. At every round of a game, each player simultaneously and independently selects a move; the moves jointly determine the transition to a successor state. Two basic objectives are the safety objective to stay forever in a given set of states, and its dual, the reachability objective to reach a given set of states. We present in this paper a strategy improvement algorithm for computing the value of a concurrent safety game, that is, the maximal probability with which player 1 can enforce the safety objective. The algorithm yields a sequence of player-1 strategies which ensure probabilities of winning that converge monotonically to the value of the safety game.

Our result is significant because the strategy improvement algorithm provides, for the first time, a way to approximate the value of a concurrent safety game *from below*. Since a value iteration algorithm, or a strategy improvement algorithm for reachability games, can be used to approximate the same value from above, the combination of both algorithms yields a method for computing a converging sequence of upper and lower bounds for the values of concurrent reachability and safety games. Previous methods could approximate the values of these games only from one direction, and as no rates of convergence are known, they did not provide a practical way to solve these games [CAH09].

Verification of Markov chains (IST Austria, Saarland U.)

We present an on-the-fly abstraction technique for infinite-state continuous -time Markov chains. We consider Markov chains that are specified by a finite set of transition classes. Such models naturally represent biochemical reactions and therefore play an important role in the stochastic modeling of biological systems. We approximate the transient probability distributions at various time instances by solving a sequence of dynamically constructed abstract models, each depending on the previous one. Each abstract model is a finite Markov chain that represents the behavior of the original, infinite chain during a specific time interval. Our approach provides complete information about probability distributions, not just about individual parameters like the mean. The error of each abstraction can be computed, and the precision of the abstraction refined when desired. We implemented the algorithm and demonstrate its usefulness and efficiency on several case studies from systems biology [HMW09].

Model Checking Probabilistic Timed Automata (Saarland U)

Probabilistic timed automata (PTA) combine discrete probabilistic choice, real time and nondeterminism. We have developed mcpta, a tool that enables the fully automatic analysis of PTA via model checking. mcpta supports probabilistic and expected reachability properties. It uses PRISM as its backend solution engine. PTA are specified in Modest [5], a high-level compositional modelling language that includes features such as exception handling, dynamic parallelism and recursion, and thus enables model specification in a convenient fashion.

We have validated the approach with three case studies that have previously been studied using PRISM or UPPAAL. Two of these had already been modeled as PTA, while for the third, we combined existing TA and PA models into a single PTA model. The case studies concern communication protocols that exhibit a combination of probabilistic and time-dependent behaviour, such as probabilistic message loss, exponential backoff mechanisms, transmission delays as well as message retransmission on timeouts. We used different modelling approaches in Modest, to, for example, give a highly modularized model or encode the PTA that formed the original case study specification in a very straightforward manner. This showed the versatility and expressivity of the Modest language [HH09].

Best Probabilistic Transformers (Saarland U)

Markov decision processes (MDPs) play a crucial role as a semantic model in the analysis of systems with random phenomena like network protocols and randomized algorithms. MDPs feature non-determinism and probabilistic choice. Typically one is interested in computing (maximal or minimal) reachability probabilities, e.g., the probability of delivering three messages after ten transmission attempts. Recently predicate-abstraction techniques have evolved that scale to realistic programs which map to infinite MDPs.

In this work we develop an abstract-interpretation framework for MDPs which admits to compute both lower and upper bounds on reachability probabilities. This provides a solid basis to reason about the relative precision and optimality of abstract transformers. Further, we prove that a game-based abstraction, a pre-existing construction by Kwiatkowska et al., corresponds to best transformers in our framework. We also investigate abstraction-refinement technique for concurrent probabilistic programs that yields both lower and upper bounds. Previous analysis techniques for such programs were also based on predicate abstraction. However they either only yield effective upper bounds or come without refinement. The basis of our refinement technique is parallel abstraction, a novel abstraction. Parallel abstraction yields effective lower and upper bounds and combines well with refinement. We have implemented our ideas in the PASS tool and report on experimental results [WZ10].

Model-checking Transactional Memories (IST Austria)

Pseudo-code descriptions of STMs assume sequentially consistent program execution and atomicity of high-level STM operations like read, write, and commit. These assumptions are often violated in realistic settings, as STM implementations run on relaxed memory models, with the atomicity of operations as provided by the hardware. This paper presents the first approach to verify STMs under relaxed memory models with atomicity of 32 bit loads and stores, and read-modify-write operations. We present RML, a new high-level language for expressing concurrent algorithms with a hardware-level atomicity of instructions, and whose semantics is parameterized by various relaxed memory models. We then present our tool, FOIL, which takes as input the RML description of an STM algorithm and the description of a memory model, and automatically determines the locations of fences, which if inserted, ensure the correctness of the STM algorithm under the given memory model. We use FOIL to verify DSTM, TL2, and McRT STM under the memory models of sequential consistency, total store order, partial store order, and relaxed memory order [GHS09].

Transactional memories are typically speculative and rely on contention managers to cure conflicts. This paper explores a complementary approach that prevents conflicts by scheduling transactions according to predictions on their access sets. We first explore the theoretical boundaries of this approach and prove that (1) a TM scheduler with an accurate prediction can be 2- competitive with an optimal TM scheduler, but (2) even a slight inaccuracy in prediction makes the competitive ratio of the TM scheduler of the order of the number of transactions. We then show that, in practice, there is room for a pragmatic approach with good average case performance. We present Shrink, a scheduler that (a) bases its prediction on the access patterns of the past transactions from the same threads, and (b) uses a novel heuristic, which we call serialization affinity, to schedule transactions with a probability proportional to the current amount of contention [DSGS09].

The work done on transactional theories resulted in the PhD thesis of Vasu Singh from IST Austria [Sin09].

Symbolic Execution Techniques Extended to Systems (CEA)

We have defined a symbolic execution framework devoted to system models defined recursively by interconnecting component models. Our concern is to allow one to explicitly define interaction rules between potentially heterogeneous components while taking into account those rules at the symbolic execution phase. In order to reach that purpose, we have introduced a small set of primitives dedicated to describe such interaction rules, together with their associated symbolic execution rules. That work has been published at ICSEA 2009 ([GALB09]).

Verification and Validation of Self-configuring embedded systems (KTH)

As part of the Dyscas project (FP6, www.dyscas.org - the project finished in March 2009), a middleware architecture for self-configuring automotive embedded systems was developed (this middleware is mainly described in the Adaptivity cluster of the ArtistDesign network). The work included both the development of a reference architecture as well as concrete implementations of it. The middleware itself is described in the Adaptivity deliverable whereas modeling results are reported in the Modeling activity.

We here focus on the aspects of verification and validation (V&V) of the middleware. V&V is seen as a great challenge with the desire to exploit the flexibility of software, for example by enabling software upgrades, adding new nodes and functionalities. In the case of Dyscas, adaptivity will in one sense contribute to increased system robustness and improved performance, by including means for reconfiguration to handle failing services and on-line decisions on allocation (load balancing) and scheduling to improve performance. This leads to trade-offs since the middleware will impose overheads, adds complexity and provides new failure modes. While the Dyscas implementations clearly indicated that light-weight implementations are possible, dealing with the robustness of the middleware itself was considered as part of a validation effort in the Dyscas project. The middleware reference architecture as well as the implementation was subjected to several types of evaluation grouped into three categories, each with several activities: Concept evaluation (Safety analysis, Configuration algorithms, Role play, OEM manual, Formal verification), Validator analysis (evaluation of the implementations including SAINT+DyLite developed by KTH), and Simulation (including simulation with Matlab/Simulink/SimEvents and Matlab/Simulink/TrueTime), [WSPFPGANPSEFRS09].

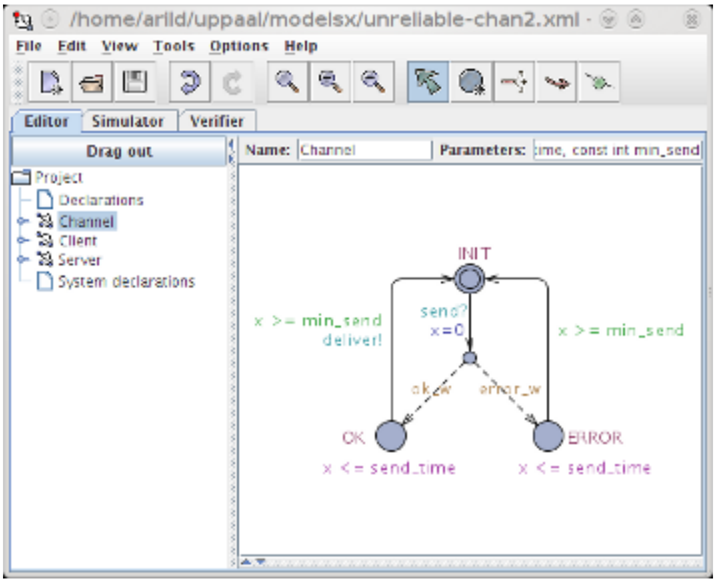
A dynamic system implies problems on testability. Current testbenches have been found not sufficiently capable of handling the advanced features provided by DySCAS. However, we have demonstrated that safety analysis and formal analysis techniques can play an important role in the design and verification, thereby to some extent reducing the need for testing, [FTC09]. A more complete executable of the architecture has been developed in one of the simulation activities. This work involved mapping UML concepts to Simulink concepts; the middleware reference architecture was chosen to be described in UML whereas Matlab/Simulink was used as a basis for simulation. Two toolboxes and modeling techniques were applied including discrete event modeling using SimEvents and more implementation close modeling using the Truetime toolbox. The results, including the experience gained from modelling, reinforce our belief that the architecture can relatively easily be implemented, [Q09]. In summary, the evaluation activities indicate that both the DySCAS concept and the DySCAS middleware architecture are viable, but need further refinement and investigation with regard to testability and security.

Model-based analysis of embedded java programs (CISS)

The approach is based on a translation of programs, written in the Safety Critical Java profile introduced by Schoeberl et. al (ISORC'07) for the Java Optimized Processor, to timed automata models verifiable by the Uppaal model checker. Schedulability analysis is reduced to a simple reachability question, checking for deadlock freedom. Experiments show that model-based schedulability analysis can result in a more accurate analysis than possible with traditional approaches, thus systems deemed non-schedulable by traditional approaches may in fact be schedulable, as detected by our analysis. In ongoing work focus is on application of static analysis related to the discrete part of Uppaal models in order to allow for more accurate and efficient schedulability analyses.

UPPAAL Pro (CISS)

In this work we present the tool UPPAAL-PRO - and extension of the real-time model checker UPPAAL - for the formalism of probabilistic timed automata. UPPAAL-PRO supports the computation of maximal probabilistic reachability, including time-bounded reachability. The tool uses time-convex federations - collections of convex zones where the novel notion of time-convexity allows for coarser representation of the state space. The overall algorithm is an on-they abstraction-refinement algorithm, allowing to successively compute refined probability bounds based on linear programming problems derived from successively refined partitionings, allowing for early termination and useful feedback during model-checking.



Name: Channel
Parameters: ime, const int min_send

WCET analysis of ARM processors using real-time model checking (CISS)

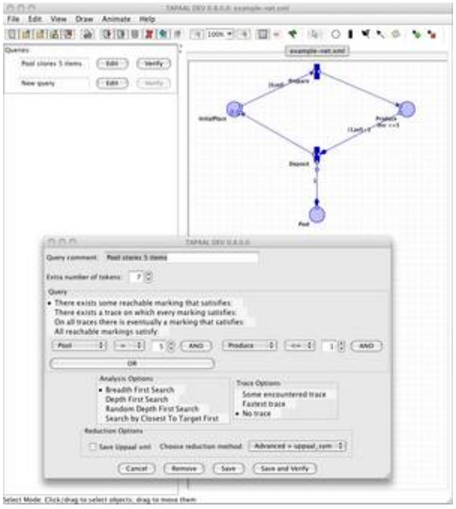
The ability to determine safe and sharp worst-case execution times (WCETs) for processes is very important when scheduling real-time systems, as it influences the reliability and efficiency of the resulting systems. This paper presents work towards a flexible WCET analysis method based on model checking and static analysis that determines safe and sharp WCETs for processes running on hardware platforms featuring caching and pipelining. The method is divided into four loosely coupled sub-analysis, which makes it very flexible. To demonstrate and evaluate the method, it is implemented for the ARM920T processor and tested successfully on most of the WCET benchmark programs from Mardalen Real-Time Research Center. The flexibility of the method allows for easy replacement and reuse of parts of the implementation, in order to add support for additional hardware platforms. Experiments on the implementation show that the principles used in the method look promising, and that taking caching into account is worth the effort.

Quantitative Analysis (CISS)

We present a general framework for the analysis of quantitative and qualitative properties of reactive systems, based on a notion of weighted transition systems. We introduce and analyze three different types of distances on weighted transition systems, both in a linear and a branching version. Our quantitative notions appear to be reasonable extensions of the standard qualitative concepts, and the three different types introduced are shown to measure inequivalent properties. When applied to the formalism of weighted timed automata, we show that some standard decidability and undecidability results for timed automata extend to our quantitative setting.

TAPAAL (CISS)

TAPAAL is a new platform independent tool for modeling, simulation and verification of timed-arc Petri nets. TAPAAL provides a stand-alone editor and simulator, while the verification module translates timed-arc Petri net models into networks of timed automata and uses the UPPAAL engine for the automatic analysis. We report on the status of the _first release of TAPAAL (available at www.tapaal.net), on its new modeling features and we demonstrate the efficiency and modeling capabilities of the tool on a few examples.



Queries:
Pool stores 5 items
New query

Query comment: Pool stores 5 items

Extra number of tokens: 7

Query
- ● There exists some reachable marking that satisfies:
- There exists a trace on which every marking satisfies:
- On all traces there is eventually a marking that satisfies:
- All reachable markings satisfy:

Pool = 5 AND Produce <= 1 AND

Analysis Options
- ● Breadth First Search
- Depth First Search
- Random Depth First Search
- Search by Closest To Target First

Trace Options
- Some encountered trace
- Fastest trace
- ● No trace

Reduction Options
☐ Save Uppaal xml Choose reduction method: Advanced + uppaal_sym

Select Mode: Click/drag to select objects; drag to move them

‘

Verification of real-time systems against scenario-based specifications (CISS)

We propose an approach to automatic verification of real time systems against scenario-based requirements. A real-time system is modeled as a network of Timed Automata (TA), and a scenario-based requirement is specified as a Live Sequence Chart (LSC). We define a trace-based semantics for a kernel subset of the LSC language. By equivalently translating an LSC chart into an observer TA and then non-intrusively composing this observer with the original system model, the problem of verifying a real-time system against a scenario-based requirement reduces to a classical real-time model checking problem. We show how this is accomplished in the context of the Uppaal model checker.

StopWatch Automata in UPPAAL (CISS)

The ability of allowing clocks of timed automata to be stopped in certain locations provides an extremely useful extended formalism for modeling scheduling problems where preemption may occur. Unfortunately, the resulting stopwatch automata model comes with undecidability of most interesting problems, including that of reachability; in fact as shown in 2000 [Cassez, Larsen] SWA has same expressive power as that of LHA, linear hybrid automata. Recently a zone-based over-approximate analysis of SWA has been made in UPPAAL proving to provide efficient yet accurate analysis on a number of examples, including schedulability analysis in presence of preemption and uncertainty of the computation times of tasks. Also the notion of a stop-watch has been used to model abstract caches in the sense of Wilhelm et al. Ongoing work include investigation as to when the over-approximate analysis is exact, and usage of linear

Model-based framework for schedulability analysis (CISS)

Embedded systems involve the monitoring and control of complex physical processes using applications running on dedicated execution platforms in a resource constrained manner in terms of for example memory, processing power, bandwidth, energy consumption, as well as timing behavior. Viewing the application as a collection of (interdependent tasks) various scheduling principles may be applied to coordinate the execution of tasks in order to ensure orderly and efficient usage of resources. Based on the physical process to be controlled, timing deadlines may be required for the individual tasks as well as the overall system. The challenge of schedulability analysis is now concerned with guaranteeing that the applied scheduling principle(s) ensure that the timing deadlines are met.

Statistical Analysis of Controller Area Network Message Response Times (Trento + GM)

Modern automobile architectures are composed by tens of Electronics Control Units (ECUs) connected by several buses, most of which are Controller Area Networks (CAN). The availability of multiple ECUs can be exploited by distributing control tasks of one domain (for example, power train) to several ECUs. In this case, a number of distributed functions are assigned to multiple tasks executing concurrently on different modules and communicating via messages transmitted on CAN. Distributed functions include time-critical controls, but most often, also functions that are characterized by requirements for average performance together with hard deadline constraints (as for most active-safety functions) and functions with soft real-time requirements (controls for enhanced driver comfort). The definition of a new architecture framework for one or more car product families is an extremely important step: ECUs, networks and the topology of connections must be defined and frozen years in advance of production. Later, during the architecture lifespan, functions are placed on ECUs and communication scheduled on the bus. This paper [ZDGSV09] presented a statistical approach to the early evaluation and selection of distributed embedded architectures for next-generation automotive controls, where the application performance depends on the end-to-end latencies of active-safety functions. Automobile architecture must be evaluated and selected having in mind that they will have a lifespan of 5 to 10 years and that during this lifespan the communication and computation load is partly unknown because new functions are still being decided on and have not been designed as yet. Hence, when verifying that the architecture is sufficiently robust with respect to constraints on latency and performance targets of present and future functionalities, loads can only be roughly estimated by looking at past trends or by exploiting early indications of designers. In this paper, we considered an application model that is currently deployed in GeneralMotors E/E architectures and is supported by the AUTOSAR standard. We described the use of statistical analysis to compute the probability distribution of Controller Area Network (CAN) message response times when only partial information is available about the electrical architecture of a vehicle as well as about its functionality. We provided results that showed our statistical inference allows predicting accurately the distribution of the response time of a CAN message, once its priority has been assigned, from limited information such as the bus utilization of higher priority messages.
This publication obtained the best paper award at the IEEE Symposium on Industrial Embedded Systems.

Sub-activity C: Cross-layer Validation

Adapting Abstraction Techniques to Black Box Analysis and Learning (Uppsala University, TU Dortmund)

Uppsala University and TU Dortmund are collaborating on the problem of developing automata learning (aka. regular inference) techniques to the point where they can be used to learn behavior of communicating systems in realistic contexts. The basis for our work is the use of regular inference technique, also called automata learning. In regular inference, a finite-state machine (or a regular language) is constructed from the answers to a set of {\em membership queries}, each of which observes the component's output in response to a certain input string. Given ``enough'' membership queries, the constructed automaton will be a correct model of the observed component.

During the year, we have addressed the problem that existing regular inference techniques can cope only with finite-state machines. However, typical communication systems may not be adequately modeled by finite-state models, since they use sequence numbers, buffers, and other unbounded data domains. We propose to address this problem by abstraction techniques. The idea is to define an abstraction, which provides a finite-state abstract view of its behavior, hiding infinitary aspects. This technique is inspired by predicate abstraction which has been successful for extending finite-state model checking to large and infinite state spaces. In contrast to that work, however, we are now in a black-box setting, so we cannot define the abstraction directly on the source code of a component. Instead, the abstraction must be realized by an external component, which we call a Mapper, which transforms an infinite-state view of the behavior into a finite-state one. Regular inference can be performed on the finite-state view, whereafter the effect of the Mapper can be reversed to obtain a model of the component's behavior. We have implemented our techniques by connecting the LearnLib tool for regular inference, developed at TU Dortmund, with the protocol simulator ns-2, which provides implementations of standard protocols. We have used it to generate models the ns-2 implementations of entities in the SIP and TCP protocols.

Control under Partial Observation (INRIA)

In [KGMM09a] we study the computational complexity of several decision and optimization control problems arising in partially observed discrete event systems. These problems are related to the state avoidance problem where one must compute a controller which prevents the system from accessing a set of bad states and which is maximal for a defined criterion, based on inclusion of the set of states remaining reachable after the control. We focus our study on memoryless controllers.

In [KGMM09b] we provide models of safe controllers both for potentially blocking and non blocking controlled systems. To obtain algorithms for these problems, we make the use of abstract interpretation techniques which provide over-approximations of the transitions set to be disabled. To our knowledge, with the hypotheses taken, the improved version of our algorithm provides a better solution than what was previously proposed in the literature. Our tool SMACS allowed us to make an empirical validation of our methods to show their feasibility and usability.

Verifying, monitoring and testing security properties (INRIA)

In [J09] we investigate the verification of opacity (absence of confidential information flow) using abstraction techniques to compute executable counterexamples (attack scenarios). Considering a system and a predicate over its executions, attackers are modeled as semi-conservative decision process determining from observed traces the truth of that predicate. Moreover, we show that the most precise the abstraction is, the most accurate (and then dangerous) the corresponding class of attackers will be. Consequently, when no attack scenario is detected on an approximate analysis, we know that this system is safe against all ``less precise'' attackers. This can therefore be used to provide a level of certification relative to the precision of abstractions.

In [DJM09] we are interested in constructing monitors for the detection of confidential information flow for partially observable discrete event systems. We characterize the set of observations allowing an attacker to infer the secret information and, based on the diagnosis of discrete event systems, we provide necessary and sufficient conditions under which detection and prediction of secret information flow can be ensured, and construct a monitor allowing an administrator to detect it. In [MDJ09], we investigate the combination of controller synthesis and test generation techniques for the testing of open, partially observable systems with respect to security policies: integrity properties and confidentiality properties. We show how to derive testers that test the conformance of the implementation with respect to its specification, the correctness of an access control, and the security property itself.

In [CDM09] we address the problem of synthesizing opaque systems. We introduce dynamic partial observability where the set of events the user can observe changes over time. We show how to check that a system is opaque w.r.t. to a dynamic observer and also address the corresponding synthesis problem: given a system G and secret states S, compute the set of dynamic observers under which S is opaque. Our main result is that the set of such observers can be finitely represented and can be computed in EXPTIME.

Diagnosability of pushdown systems (INRIA)

Diagnosis problems of discrete-event systems consist in detecting unobservable defects during system execution. For finite-state systems, the theory is well understood and a number of effective solutions have been developed. For infinite-state systems, however, there are only few results, mostly identifying classes where the problem is undecidable. We consider higher-order pushdown systems and investigate two basic variants of diagnosis problems: the diagnosability, which consists in deciding whether defects can be detected within a finite delay, and the bounded-latency problem, which consists in determining a bound for the delay of detecting defects.

Synthesis with Imperfect Information (LSV, CVF and IST Austria)

We developed a tool, ALPAGA, for solving two-player parity games with imperfect information. Given the description of a game, it determines whether the first player can ensure to win and, if so, it constructs a winning strategy. The tool provides a symbolic implementation of a recent algorithm based on antichains [BCW+09].

Observability and Controllability Issues in Conformance Testing of Web Service Composition (CEA)

We have defined a model based black-box testing approach to test conformance of Web Service compositions. Specifications of compositions are given as Input Output Symbolic Transition Systems. Usually, a composition under test makes use of Web Services whose behaviors are simulated by the tester, but it may also make use of their implementations. In the last case, two situations may occur: either communications between the composition and the Web Services are observable, or they are hidden internal actions. We have shown how to extract test purposes for Web Service Compositions. Test purposes are extracted from symbolic executions of composition specifications by means of different operations to take into account hidden or observable communications. Resulting test purposes are used as inputs of an algorithm of test case generation. Our verdicts are provided with symbolic scenarios which represent possible behaviors of Web Services illustrating the verdicts. That work has been published at TestCom 2009 ([EGLC09]).

Test purpose generation for service evolutions: a symbolic approach (CEA)

We have proposed an approach to test service evolution in the context of service oriented systems. Such systems are composed of orchestrations which interact with users and coordinate services to fulfill users' requests. The tester only interacts with services through orchestrations. We have used symbolic execution techniques in a model based black box approach to identify test purpose characterizing first class citizen behaviors to be tested. We have shown how test purposes characterized before a service evolution may be qualified as: obsolete test purposes (no more relevant after the evolution) non regression test purposes (not impacted by the evolution) and how to identify new emergent test purposes that reflect behaviors induced by the service evolution.

That work has been published at Sinter 2009 ([GR09])

Timed Testing under Partial Observvability (CISS)

This paper studies the problem of model-based testing of real-time systems that are only partially observable. We model the System Under Test (SUT) using Timed Game Automata (TGA) which has internal actions, uncontrollable outputs and timing uncertainty of outputs. We define the partial observability of SUT using a set of predicates over the TGA state space, and specify the test purposes in Computation Tree Logic (CTL) formulas. A recently developed partially observable timed game solver is used to generate winning strategies, which are used as test cases. We propose a conformance testing framework, define a partial observation-based conformance relation, present the test execution algorithms, and prove the soundness and completeness of this test method (i.e., a detected error really violates the conformance relation; and if the SUT violates the test purpose, then a test case can be generated to detect this violation). Experiments on some non-trivial examples show that this method yields encouraging results.

Verification, performance analysis and controller synthesis for real-time systems (CISS)

Work has been made towards providing a concise and precise Travellers Guide, Phrase Book or Reference Manual to the timed automata modeling formalism introduced by Alur and Dill. A collection of comprehensive definitions of timed automata, priced (or weighted) timed automata, and timed games has been made as well as highlights of a number of results on associated decision problems related to model checking, equivalence checking, optimal scheduling, and winning strategies.

Automatic synthesis of robust and optimal controllers (CISS)

In this paper, we show how to apply recent tools for the automatic synthesis of robust and near-optimal controllers for a real industrial case study. We show how to use three different classes of models and their supporting existing tools, TiGA for synthesis, PHAVer for verification, and Simulink for simulation, in a complementary way. We believe that this case study shows that our tools have reached a level of maturity that allows us to tackle interesting and relevant industrial control problems.

Timed Alternating Simulation (CISS)
In this work we focus on property-preserving preorders between timed game automata and their application to control of partially observable systems. We define timed weak alternating simulation as a preorder between timed game automata, which preserves controllability. We define the rules of building a symbolic turn-based two-player game such that the existence of a winning strategy is equivalent to the simulation being satisfied. We also propose an on-the-fly algorithm for solving this game. This simulation checking method can be applied to the case of non-alternating or strong simulations as well. We illustrate our algorithm by a case study and report on results.

UPPAAL TIGA 2009 (CISS)
In this work we present two major new features of the tool Uppaal-TiGa that will be available in its next release. The first novelty is the support of timed games with partial observability in the tool. We detail the improvements of the original algorithm that have been implemented. The second new feature is the support for timed games with Buchi objectives. We present a simple and elegant algorithm based on the current reachability control algorithm implemented in Uppaal-TiGa. A major application of this feature is the ability to generate nonzeno strategies with a simple encoding.

Optimizing the implementation of communication in synchronous reactive models with time constraints (Trento + Scuola di Sant'Anna + National Instruments)
Model-based design methodologies are gaining attention in the industrial community because of the possibility of early and efficient functional validation and formal verification of properties at high levels of abstraction. The advantages of validating the design using high-level models can be lost entirely if errors and modifications that are not back-annotated to the higher abstraction levels are introduced when refining the design to lower levels of abstraction. To overcome this problem and to reduce design time, automatic synthesis has been used for the refinement process from Register Transfer Languages to logic gates for digital circuit design. This approach guarantees (assuming that the synthesis algorithms are correctly implemented) that the semantics of the RTL description are semantically equivalent to the semantics of the logic circuit. Automatic code generation is similar in intent and applicability. However, the software implementation of the abstract model must make efficient use of the platform resources that may not reflect all the assumptions of the code generation algorithms. The implementation of communication in a synchronous reactive model requires buffering and access procedures at the kernel level. In previous work, we obtained tight bounds on the size of communication buffers to maintain semantics equivalence. In real-time systems, however, because of the longer execution times of access procedures, an implementation with minimum buffer size may lead to the violation of deadlines. To solve this problem, we proposed a Mixed Integer Linear Programming (MILP)-based optimization approach that provides the minimum memory implementation of a set of communication channels while guaranteeing that the task deadline constraints are met [WDSV09]. The analysis is validated by an OSEK/VDX-compliant implementation that provides an estimate of actual run-time overheads. The approach is applied to a set of task graphs and an automotive case study.

-- The above is new material, not present in the Y1 deliverable --

2.2 Individual Publications Resulting from these Achievements

Uppsala

[GSYY09] Nan Guan, Martin Stigge, Wang Yi and Ge Yu. New Response Time Bounds for Fixed Priority Multiprocessor Scheduling. In the proc. of RTSS09, the 30th IEEE Real-Time Systems Symposium, December 1 - December 4, 2009 Washington, D.C., USA.

[GSYY09b] Nan Guan, Martin Stigge, Wang Yi and Ge Yu. Cache-Aware Scheduling and Analysis for Multicores. In the proc. of the 7th International Conference on Embedded Software, Oct. 12-16, Grenoble, France.

[GGYY09] Nan Guan, Zonghua Gu, Wang Yi and Ge Yu. Improving Scalability of Model-Checking for Minimizing Buffer Requirements of Synchronous Dataflow Graphs. In the proc. of the 14th Asia and South Pacific Design Automation Conference, Jan. 19-22 2009. Yokohama, Japan.

[B090] Therese Bohlin: Regular Inference for Communication Protocol Entities, Ph. D. Thesis, Uppsala University, March 2009.

[BGJSY09] Frank S. de Boer, Immo Grabe, Mohammad Mahdi Jaghoori1, Andries Stam, and Wang Yi. Modeling and Analysis of Thread-Pools in an Industrial Communication Platform. In the proc. Of the 10th International Conference on Formal Engineering Methods. December 9-12, 2009, Rio de Janeiro, Brazil.

INRIA

[BLPR09] N. Bertrand, A. Legay, S. Pinchinat, J-P. Raclet. A Compositional Approach on Modal Specifications for Timed Systems. In Proceedings of the 11th International Conference on Formal Engineering Methods (ICFEM'09), Lecture Notes in Computer Science, Volume 5885, Pages 679-697, December 2009.

[BPR09] N. Bertrand, S. Pinchinat, J.B. Raclet. Refinement and Consistency of Timed Modal Specifications. In Proceedings of the 3rd International Conference on Language and Automata Theory and Applications (LATA'09), LNCS, Volume 5457, Pages 152-163, Tarragona, Spain, April 2009.

[MDJ09] H. Marchand, J. Dubreil, T. Jéron. Automatic Testing of Access Control for Security Properties. In TestCom'09, LNCS, Volume 5826, Pages 113-128, November 2009.

[CDM09] F. Cassez, J. Dubreil, H. Marchand. Dynamic Observers for the Synthesis of Opaque Systems. In 7th International Symposium on Automated Technology for Verification and Analysis (ATVA'09), Z. Liu, A.P. Ravn (eds.), LNCS, Volume 5799, Pages 352-367, Macao SAR, China, October 2009.

[MP09] C. Morvan, S. Pinchinat. Diagnosability of pushdown systems. In HVC2009, Haifa Verification Conference, to appear in LNCS, Haifa, Israel, October 2009.

[BGG09] N. Bertrand, B. Genest, H. Gimbert. Qualitative Determinacy and Decidability of Stochastic Games with Signals. In 24th Annual IEEE Symposium on Logic in Computer Science (LICS'09), Pages 319-328, Los Angeles, CA, USA, August 2009.

[DJM09] J. Dubreil, T. Jéron, H. Marchand. Monitoring Confidentiality by Diagnosis Techniques. In European Control Conference, Pages 2584-2590, Budapest, Hungary, August 2009.

[M09] C. Morvan. On external presentations of infinite graphs. In 11th International Workshop on Verification of Infinite-State Systems, INFINITY'09, to appear in eptcs, Bologna, Italy, August 2009.

[D09] J. Dubreil. Opacity and Abstraction. In Proceedings of the First International Workshop on Abstractions for Petri Nets and Other Models of Concurrency (APNOC'09), Paris, France, June 2009.

Aachen

[JHBK09] Marijn R. Jongerden, Boudewijn R. Haverkort, Henrik Bohnenkamp, and Joost-Pieter Katoen. Maximizing System Lifetime by Battery Scheduling. In Proc. DSN 2009, IEEE Computer Society, 2009.

[CHKM09] Taolue Chen, Tingting Han, Joost-Pieter Katoen, and Alexandru Mereacre. Quantitative Model Checking of Continuous-Time Markov Chains Against Timed Automata Specifications. In IEEE Symposium on Logic in Computer Science (LICS). IEEE CS Press, 2009.

[KaZa09] Joost-Pieter Katoen, and Ivan S. Zapreev. Simulation-based CTMC Model Checking: An Empirical Evaluation. In Quantitative Evaluation of Systems (QEST). IEEE CS Press, 2009.

[KRHK09] Daniel Klink, Anne Remke, Boudewijn R. Haverkort, and Joost-Pieter Katoen. Time-Bounded Reachability in Tree-Structured QBDs by Abstraction. In Quantitative Evaluation of Systems (QEST). IEEE CS Press, 2009.

[KHHJZ09] Joost-Pieter Katoen, E. Moritz Hahn, Holger Hermanns, David N. Jansen, and Ivan S. Zapreev. The Ins and Outs of the Probabilistic Model Checker MRMC. In Quantitative Evaluation of Systems (QEST). IEEE CS Press, 2009.

[KKN09] Joost-Pieter Katoen, Daniel Klink, and Martin R. NeuhŠu§er. Compositional Abstraction of Stochastic Systems . In Formal Modeling and Analysis of Timed Systems (FORMATS). pages 195Ð211. Volume 5813 of LNCS. Springer, 2009.

[CHKM09] Taolue Chen, Tingting Han, Joost-Pieter Katoen, and Alexandru Mereacre. LTL model checking of time-inhomogeneous Markov chains. In 7th International Symposium on Automated Technology for Verification and Analysis (ATVAÕ09). pages 104Ð119. Volume 5799 of LNCS. 2009.

Saltzburgh

[CKPRS09a] S.S. Craciunas, C.M. Kirsch, H. Payer, H. Roeck, A. Sokolova. Programmable Temporal Isolation through Variable-Bandwidth Servers. Proc. Symposium on Industrial Embedded Systems (SIES), 2009.

[CKPRS09b] S.S. Craciunas, C.M. Kirsch, H. Payer, H. Roeck, A. Sokolova. Programmable Temporal Isolation in Real-Time and Embedded Execution Environments. Proc. Workshop on Isolation and Integration in Embedded Systems (IIES), 2009.

Saarbrücken

[HH09] A. Hartmanns, H Hermanns. A Modest Approach to Checking Probabilistic Timed Automata. In QEST 2009. IEEE CS Press.

[HHZ09] Ernst Moritz Hahn, Holger Hermanns, Lijun Zhang: Probabilistic Reachability for Parametric Markov Models. SPIN 2009:88-106

[HMW09] T. A. Henzinger, M. Mateescu, and V. Wolf. Sliding-window abstraction for infinite Markov chains. Proceedings of the 21st International Conference on Computer-Aided Verification (CAV), LNCS 5643:337-352, Springer, 2009.

[WZ10] B Wachter, L Zhang. Best Probabilistic Transformers. In VMCAI 2010. LNCS 5944:361-379. 2010.

[KHHJZ09] Joost-Pieter Katoen, E. Moritz Hahn, Holger Hermanns, David N. Jansen, and Ivan S. Zapreev. The Ins and Outs of the Probabilistic Model Checker MRMC. In Quantitative Evaluation of Systems (QEST). IEEE CS Press, 2009.

KTH

[Q09] Tahir Naseer Qureshi. Towards Model-Based Development of Self Managing Automotive Systems: Modeling, Simulation, Model Transformations and Algorithms: Supporting the Development of the DySCAS Middleware. Licentiate Thesis, KTH, June 2009, TRITA MMK 2009-12, ISBN 978-91-7415-374-3. KTH, School of Industrial Technology and Management.

[FTC09] Lei Feng, Martin Törngren, DEJiu Chen. Safety Analysis of Dynamically Self Configuring Automotive Systems. Technical report MMK2008:13 (actually published in 2009). Division of Mechatronics, Dept of Machine Design, School of Industrial Engineering and Management, Royal Institute of Technology - Kungliga Tekniska Högskolan, 2009.

IST/EPFL

[CAH09] Krishnendu Chatterjee, Luca de Alfaro, and Thomas A. Henzinger. Termination criteria for solving concurrent safety and reachability games. *Proceedings of the 20th Annual Symposium on Discrete Algorithms* (SODA), ACM Press, 2009, pp. 197-206.

[CDH09] Krishnendu Chatterjee, Laurent Doyen, and Thomas A. Henzinger. A survey of stochastic games with limsup and liminf objectives. *Proceedings of the 36th International Colloquium on Automata, Languages and Programming* (ICALP), Lecture Notes in Computer Science 5556, Part II, Springer, 2009, pp. 1-15.

[GHS09] R. Guerraoui, T. A. Henzinger, and V. Singh. Software Transactional Memory on Relaxed Memory Models. In *Proceedings of the 21st International Conference on Computer Aided Verification*, Berlin, 2009. Springer.

[DSGS09] A. Dragojevic, A. Singh, R. Guerraoui, and V. Singh. Preventing versus Curing: Avoiding Conflicts in Transactional Memories. In *Twenty-Eighth Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing*, 2009.

[JKN09] K.D. Jones, V. Konrad, D. Nickovic. Analog Property Checkers: a DDR2 Case Study, in Formal Methods for System Design (FMSD), 2009.

[NP09] D. Nickovic, N. Piterman. From MTL to Deterministic Timed Automata, Technical Report 2009/2 Imperial College London, 2009.

[Sin09] V. Singh. *Formalizing and verifying transactional memories*. PhD thesis, Lausanne, 2009.

CEA

[GALB09] C. Gaston, M. Aiguier, D. Bahrami and A. Lapitre. Symbolic Execution Techniques Extended to Systems. In Proceedings of ICSEA 2009 - International Conference on Software Engineering Advances. IEEE Computer Society Press, 2009.

[EGLC09] J. P. Escobedo, C. Gaston, P. Le Gall and A. Cavalli. Observability and Controllability Issues in Conformance Testing of Web Service Compositions. In Proceedings of TestCom 2009 - Testing of Software and Communication Systems. Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 2009.

[GR09] C. Gaston and N. Rapin, Test purpose generation for service evolutions: a symbolic approach. In Proceedings of SINTER 2009 - the 2009 ESEC/FSE workshop on Software integration and evolution @ runtime. ACM New York, 2009.

CISS

[BRT09] T. Bøgholm, A. P. Ravn, and B. Thomsen. Model-based analysis of embedded java programs. In The 4th International Workshop on Systems Software Verification Aachen (SSV'09), 2009.

[DHL09] Alexandre David, Arild Haugstad, and Kim G. Larsen. UPPAAL Pro, A Tool for Performance Analysis of Probabilistic Tmed Automata. Downloadable from www.uppaal.com

[DOTHL09] A. E. Dalsgaard, M. C. Olesen, M. Toft, R. R. Hansen, and K. G. Larsen. WCET analysis of arm processors using real-time model checking. In 4th International Workshop on Systems Software Verification (SSV'09) Real Software, Real Problems, Real Solutions, 2009.

[FCDLLLW09] Benoit Caillaud, Benoit Delahaye, Kim G. Larsen, Mikkel Larsen, Axel Legay, and Andrzej Wasowski. Compositional design methodology with constraint markov chains. Under submission.

[BFLM09] Patricia Bouyer, Uli Fahrenberg, Kim Guldstrand Larsen, and Nicolas Markey. Exponentially priced timed automata. Under submission.

[TFL09] Claus Thrane, Uli Fahrenberg, and Kim Guldstrand Larsen. Quantitative analysis of weighted transition systems. Journal of Logic and Algebraic Programming, 2009. To appear.

[LLBP09] Kim G. Larsen, Shuhao Li, Brian Nielsen, and Saulius Pusinskas. Verifying real-time systems against scenario-based requirements. In Proc. 16th Int'l Symposium on Formal Methods (FM'09), 2009.

[L09a] Kim Guldstrand Larsen: Verification and Performance Analysis for Embedded Systems. Third IEEE International Symposium on Theoretical Aspects of Software Engineering, 29-31 July 2009, Tianjin, China. IEEE Computer Society 2009.

[L09b] Kim G. Larsen. Quantitative and compositional model checking. In Proceedings of Seventh International Andrei Ershov Memorial Conference (PSI), 2009. To appear.

[BJS09] J. Byg, K.Y. Jørgensen, and J. Srba. Tapaal: Editor, simulator and verifier of timed-arc petri nets. In Proceedings of the 7th International Symposium on Automated Technology forVerifcation and Analysis (ATVA'09), 2009.

[DLLN09] Alexandre David, Kim G. Larsen, Shuhao Li, and Brian Nielsen. Timed testing under partial observability. In ICST '09: Proceedings of the 2009 International Conference on Software Testing Verification and Validation, pages 61{70, Washington, DC, USA, 2009. IEEE Computer Society.

[FLT08] Uli Fahrenberg, Kim Guldstrand Larsen, and Claus Thrane. Verification, performance analysis and controller synthesis for real-time systems. In ASI 08, 2008.

[DILS09] Alexandre David, Jacob Illum, Kim G. Larsen, and Arne Skou. Model-based framework for schedulability analysis using uppaal 4.1. In Gabriela Nicolescu, editor, Model-Based Design for Embedded Systems. CRC Press, November 2009.

[FLT09] Uli Fahrenberg, Kim Guldstrand Larsen, and Claus Thrane. A quantitative characterization of weighted kripke structures in temporal logic. Abstract for invited talk at the workshop on Quantitative logics, satellite event of ICALP 2009, Rhodes, Greece.

[CJL09] Franck Cassez, Jan Jacob Jessen, Kim G. Larsen, Jean-François Raskin, Pierre-Alain Reynier:. Automatic synthesis of robust and optimal controllers - an industrial case study. In Hybrid Systems: Computation and Control, 12th International Conference (HSCC 2009), volume 5469 of LNCS, pages 90{104. Springer, 2009.

[BCDL09] Peter Bulychev, Thomas Chatain, Alexandre David, and Kim G. Larsen. Efficient on-the-fly algorithm for checking alternating timed simulation. In Procedings of FORMATS09. 2009.

[CDL09] Thomas Chatain, Alexandre David, and Kim G. Larsen. Playing games with timed games. In Proceedings of IFAC Int. Conference on Analysis and Design of Hybrid Systems (ADHS'09), Accepted for publication, 2009.

[DLL09] Alexandre David, Kim G. Larsen, and Didier Lime. UPPAAL TIGA 2009 towards realizable strategies. In Proceedings of Workshop on Games for Design, Verification and Synthesis, GASICS, Grenoble, 2009 (to appear), 2009.

[HRLPS09] Ulrik H. Hjort, Jacob Illum Rasmussen, Kim Guldstrand Larsen, Michael A. Petersen, Arne Skou: Model-Based GUI Testing Using Uppaal at Novo Nordisk. FM 2009: 814-818.

VERIMAG

[BBS09] Saddek Bensalem, Marius Bozga, Thanh-Hung Nguyen, Joseph Sifakis. D-Finder: A Tool for Compositional Deadlock Detection and Verification. CAV 2009, Grenoble, France, June 26 - July 2, 2009. Proceedings. Springer, Lecture Notes in Computer Science 5643

[MFK09] Hitashyam Maka, Goran Frehse, Bruce H. Krogh. Polyhedral Domains and Widening for Verification of Numerical Programs. In “NSV-II: Second International Workshop on Numerical Software Verification”, 2009.

[FR09] Goran Frehse, Rajarshi Ray. Design Principles for an Extendable Verification Tool for Hybrid Systems. In ADHS'09: 3rd IFAC Conference on Analysis and Design of Hybrid Systems, 2009

[BBM09] R. Ben Salah, M. Bozga, O. Maler, Compositional Timing Analysis, EMSOFT, 2009.

[TDM09] Stavros Tripakis and Thao Dang. Model-based Design of Heterogeneous Systems, chapter Modeling, Verification and Testing using Timed and Hybrid Automata. CRC Press, 2009.

[FFM09] Ylies Falcone, Jean-Claude Fernandez, and Laurent Mounier. Enforcement monitoring wrt. the safety-progress classification of properties. In Sung Y. Shin and Sascha Ossowski, editors, Proceedings of the 2009 ACM Symposium on Applied Computing (SAC), Honolulu, Hawaii, USA, March 9-12, 2009, pages 593–600. ACM, 2009.

[BIL09] Marius Bozga, Radu Iosif, and Yassine Lakhnech. Flat parametric counter automata. Fundamenta Informaticae, 91(2):275–303, 2009.

[BGI09] Marius Bozga, Codruta Girlea, and Radu Iosif. Iterating octagons. In Stefan Kowalewski and Anna Philippou, editors, TACAS, volume 5505 of Lecture Notes in Computer Science, pages 337–351. Springer, 2009.

TRENTO

[WDSV09] G. Wang, M. Di Natale, A. Sangiovanni-Vincentelli, "Improving the Size of Communication Buffers in Synchronous Models With Time Constraints," IEEE Transactions on Industrial Informatics, Volume 5, Issue 3, Aug. 2009 Page(s):229 - 240.

[WDMSV09] G. Wang, M. Di Natale, P. J. Mosterman, A. Sangiovanni-Vincentelli, "Automatic Code Generation for Synchronous Reactive Communication," ICESS, pp.40-47, 2009 International Conference on Embedded Software and Systems, 2009.

[ZDGSV09] H. Zeng, M. Di Natale, P. Giusto, A. Sangiovanni-Vincentelli. "Statistical Analysis of Controller Area Network Message Response Times". In Proceedings of the IEEE Symposium on Industrial Embedded Systems (SIES), July 2009. [Best Paper Award].

-- The above are new references, not present in the Y1 deliverable --

2.3 Interaction and Building Excellence between Partners

Uppsala have been collaborating with ETH Zurich, Switzerland on combining UPPAAL with the Real Time Calculus (RTC), to improve the analysis precision of RTC and to enhance the scalability of the UPPAAL model checker.

INRIA . with TU Dresden we collaborate on probabilistic and timed models and their analysis; with LSV Cachan they work on the analysis of timed systems; with ULB Bruxelles they work on controller synthesis.

IST Austria+CFV collaborated on efficient algorithms for classical decision problems in automata theory (emptiness, language inclusion, universality).

IST Austria+Salzburg+Uni. Porto provided modular methods for checking time-determinism of HTL programs

IST Austria+Saarland Uni. collaborated on sliding-window abstractions for infinite Markov chains.

IST Austria+ETHZ collaborated on program analysis methods.

KTH-Volvo-**Offis**-Bosch- Enea: Joint work in the evaluation and validation of self-configuring embedded systems in the context of the Dyscas project.

CISS, LSV has collaborated substantially on development of algorithms for analyzing and model checking priced timed automata.

CISS, INRIA (Rennes) has collaborated substantially on compositional verification and development methodologies for probabilistic as well as timed systems.

CISS, Uppsala has collaborated on the continued development and maintenance of the real-time model checking tool UPPAAL.

CISS, Verimag, Brno are collaborating on development of various approaches for probabilistic analysis of timed automata models.

CISS, CFV, LSV are collaborating on development and applications of tools for real-time controller synthesis using in particular game-based approaches.

CISS, LSV are collaborating on efficient algorithms for refinement checking between timed automata specifications.

Aachen and Saarland University has collaborated on design notations and model checking

Aachen and CISS has collaborated on quantitative versions of priced timed automata

Aachen and ENS Cachan has interacted on learning of regular languages;

Aachen and University of Twente on CTMDPs has interacted on battery scheduling, and model checking of Markov chains.

ETHZ, INRIA, OFFIS, Trento and VERIMAG has collaborated within the SPEEDS project lead on the definition of the SPEEDS metamodel HRC which is the basis of an important analysis platform. This collaboration continues for the definition of a verification methodology. From the collaboration in SPEEDS has started a broader collaboration on a general framework for the semantics of communication in distributed systems with INRIA, PARADES and VERIMAG with external collaboration of University of Columbia and Cadence Design Systems [BCC+].

In the Combest project several joint activities are being carried out. In particular, Verimag and ETHZ collaborate on the combination of analytical performance analysis via performance analysis of a corresponding more precise operational model in order to obtain more precise results.

The collaboration between **VERIMAG and LIAFA** lead to important progress in the verification of quantitative properties of programs with dynamic structures (memory consumption, properties of arrays)

VERIMAG and CISS have collaborated within the Multiform project on tool integration.

CISS, ESI, CVF and LSV have collaborated within the Quasimodo project particular on extending the theory of priced timed automata and on controller synthesis for timed systems.

-- Changes wrt Y1 deliverable --

The above collaborative efforts each involves a number of exchange visits between the involved partners.

2.4 Joint Publications Resulting from these Achievements

[BBG09] C. Baier, N. Bertrand, M. Grosser. Probabilistic Acceptors for Languages over Infinite Words. In 35th Conference on Current Trends in Theory and Practice of Computer Science, LNCS, Volume 5404, Pages 19-33, Spindleruv Mlyn, Czech, 2009.

[BBBB09] C. Baier, N. Bertrand, P. Bouyer, T. Brihaye. When are timed automata determinizable?. In 36th International Colloquium on Automata, Languages and Programming (ICALP'09), LNCS No 5556, Pages 43-54, Rhodes, Greece, July 2009.

[KGMM09a] G. Kalyon, T. Le Gall, H. Marchand, T. Massart. Computational Complexity for State-Feedback Controllers with Partial Observation. In 7th International Conference on Control and Automation, ICCA'09, Christchurch, New Zealand, December 2009.

[KGMM09b] G. Kalyon, T. Le Gall, H. Marchand, T. Massart. Control of Infinite Symbolic Transition Systems under Partial Observation. In European Control Conference, Pages 1456-1462, Budapest, Hungary, August 2009.

[BCW+09] D. Berwanger, K. Chatterjee, M. De Wulf, L. Doyen, and T. A. Henzinger. Alpaga: a tool for solving parity games with imperfect information. *Proceedings of the 15th International Conference on Tools and Algorithms for the Construction and Analysis of Systems* (TACAS), Lecture Notes in Computer Science 5505, Springer, 2009, pp. 58-61.

[DR09] L. Doyen and J.-F. Raskin. Antichains for the automata-based approach to model-checking. *Logical Methods in Computer Science* 5(1:5), 2009.

[HHKV10] T. Henzinger, T. Hottelier, L. Kovács and A. Voronkov (2010). "Invariant and Type Inference for Matrices". Proc. of VMCAI 2010. (to appear)

[HKMS09] T. Henzinger, C. M. Kirsch, E. R. B. Marques, A. Sokolova. Distributed, Modular HTL, in Real-Time Systems Symposium (RTSS'09), 2009.

[HMW09] T. A. Henzinger, M. Mateescu, and V. Wolf. Sliding-window abstraction for infinite Markov chains. *Proceedings of the 21st International Conference on Computer-Aided Verification* (CAV), Lecture Notes in Computer Science 5643, Springer, 2009, pp. 337-352.

[WSPFPGANPSEFRS09] Florian Wildschütte, Detlef Scholle, Stefan Poon, Lei Feng, Magnus Persson, Javier García, Richard Anthony, Tahir Naseer, Claes Pihl, Thomas Söderqvist, Cecilia Ekelin, Viktor Friesen, Achim Rettberg and Jan Söderberg. D4.3 Evaluation Report. Deliverable 4.3, DySCAS-Dynamically Self Configuring Automotive Systems, IST project no. FP6-IST-2006-034904, February, 2009. Downloadable: http://www.dyscas.org/downloads.htm

[FCDLLLW09] Benoit Caillaud, Benoit Delahaye, Kim G. Larsen, Mikkel Larsen, Axel Legay, and Andrzej Wasowski. Compositional design methodology with constraint markov chains. Under submission.

[BFLM09] Patricia Bouyer, Uli Fahrenberg, Kim Guldstrand Larsen, and Nicolas Markey. Exponentially priced timed automata. Under submission.

[CJL09] Franck Cassez, Jan Jacob Jessen, Kim G. Larsen, Jean-François Raskin, Pierre-Alain Reynier:. Automatic synthesis of robust and optimal controllers - an industrial case study. In Hybrid Systems: Computation and Control, 12th International Conference (HSCC 2009), volume 5469 of LNCS, pages 90{104. Springer,
2009.

[BCDL09] Peter Bulychev, Thomas Chatain, Alexandre David, and Kim G. Larsen. Efficient on-the-fly algorithm for checking alternating timed simulation. In Procedings of FORMATS09. 2009.

[CDL09] Thomas Chatain, Alexandre David, and Kim G. Larsen. Playing games with timed games. In Proceedings of IFAC Int. Conference on Analysis and Design of Hybrid Systems (ADHS'09), Accepted for publication, 2009.

[DLL09] Alexandre David, Kim G. Larsen, and Didier Lime. UPPAAL TIGA 2009 towards realizable strategies. In Proceedings of Workshop on Games for Design, Verification and Synthesis, GASICS, Grenoble, 2009 (to appear), 2009.

[NSK09] Martin R. NeuhŠu§er, Marielle Stoelinga, and Joost-Pieter Katoen. Delayed Nondeterminism in Continuous-Time Markov Decision Processes. In Foundations of Software Science and Computation Structures (FoSSaCS). pages 364Ð379. Volume 5504 of LNCS. Springer-Verlag, 2009.

[HKD09] Tingting Han, Joost-Pieter Katoen, and Berteun Damman. Counterexample Generation in Probabilistic Model Checking. IEEE Transactions on Software Engineering, 35(2):241Ð257, 2009.

[BHKL09] Benedikt Bollig, Peter Habermehl, Carsten Kern, and Martin Leucker. Angluin-Style Learning of NFA. In Proceedings of the Twenty-first International Joint Conference on Artificial Intelligence (IJCAI-09). pages 1004Ð1009. AAAI Press, 2009.

[BHI*09] Marius Bozga, Peter Habermehl, Radu Iosif, Filip Konecny and Tomas Vojnar. Automatic Verification of Integer Array Programs. *In the International Conference on Computer Aided Verification, CAV '09, June. 26th 2009, Grenoble, France.*

-- The above are new references, not present in the Y1 deliverable --

2.5 Keynotes, Workshops, Tutorials

Conference: 21th International Conference on Computer-Aided Verification
Grenoble – June 26th- July 2nd, 2009

Verimag has organised CAV 2009, the major conference on computer-aided verification which had been held for the first time in Grenoble 20 years ago. The conference and its satellite workshops have attracted more than 350 participants for a period of week, and featured many embedded-oriented presentations.

http://www-cav2009.imag.fr/

Workshop: 9th International Workshop on Runtime Verification
Grenoble – June 26th- June 28th, 2009

This ARTIST workshop is held in conjunction with CAV 2009, the objective of RV'09 is to bring scientists from both academia and industry together to debate on how to monitor and analyze the execution of programs, for example by checking conformance with a formal specification written in temporal logic or some other form of history tracking logic. The purpose might be testing a piece of software before deployment, detecting errors after deployment in the field and potentially triggering subsequent fault protection actions, or the purpose can be to augment the software with new capabilities in an aspect oriented style. The longer-term goal is to investigate whether the use of lightweight formal methods applied during the execution of programs is a viable complement to the current heavyweight methods proving programs correct always before their execution, such as model checking and theorem proving. This year's workshop is organized as a satellite event of CAV.

http://www-rv2009.imag.fr/

Workshop: 2nd International Workshop on Verification and Validation of Planning and Scheduling Systems
Toulouse -- September 29th, 2008

This ARTIST workshop is held in conjunction with ICAPS 2009. The first VVPS workshop was held with ICAPS in 2005 in Monterey, California: http://planning.cis.strath.ac.uk/vvpsws. Verification techniques, such as model checking, and planning techniques have many commonalities. Planning and scheduling (P&S) systems are finding increased application in safety- and mission-critical systems that require a high level of assurance. Experience has shown that most errors are in domain models, which can be inconsistent, incomplete or inaccurate models of the target domains. However tools and methodologies for verification and validation (V&V) of P&S systems have received relatively little attention. The objective of this workshop is to maintain an interaction between the V&V and P&S communities, to identify specialized and innovative V&V tools and methodologies that can be applied to P&S. Topics of interest include: V&V of domain models, using technologies such as static analysis, theorem proving, and model checking; consistency and completeness of domain models; domain model coverage metrics; regression, stress and boundary testing; runtime verification of plan executions; generation of robust plans; compositional verification of domain models; how to structure domain models which are more amenable to static analysis; inspection methods; the relationship between timed automata and domain models; investigations of the impact wrt. V&V of procedural versus declarative plan models; etc..
http://www-vvps09.imag.fr/

Automatic test generation of Reactive and timed systems, T. Jéron MSR'09 (http://msr09.irccyn.ec-nantes.fr/), Nantes, France French colloquium on modelling, analysis and command of reactive and real-time systems.

Automatic test generation of Reactive and timed systems, T. Jéron ETR'09 summer school (Ecole d'été Temps réel, http://etr09.telecom-paristech.fr/), Paris, France, 31/08-04/09. Summer school on methods, techniques and tools for real-time systems.

EJCP (Ecole Jeunes Chercheurs en Programmation, http://ejcp2009.inria.fr/) Rennes, France, June 2009. Summer school organized by V. Rusu on modelling, analysis of computer systems.

GASICS Workshop on Games for Design, Verification and Synthsis. Co-located with CAV'09, Grenoble, June 28, 2009. *www.lsv.ens-cachan.fr/Events/gasics09/*

GASICS is an ESF project of the EUROCORES programme LogICCC (Modelling intelligent interaction – Logic in the Humanities, Social and Computational sciences). It studies game theoretic formalizations of interactive computational systems and algorithms for their analysis and synthesis. Our aim is to extend the existing notions of games played on graphs introduced by computer scientists. Currently, most of the games played on graphs are of the sort "two-player zero-sum", we aim to extend them to "multiple-player non-zero-sum", and show the applicability of the new theory to the analysis and synthesis of interactive computational systems.

The aim of this workshop is to bring together researchers working on game-related subjects, and to discuss on various aspects of game theory in the fields where it is applied. The workshop will be composed of two invited talks, together with contributed talks on the following (non-exhaustive) list of relevant topics:

- Adapted notions of games for synthesis of complex interactive computational systems
- Games played on complex and infinite graphs
- Games with quantitative objectives
- Game with incomplete information and over dynamic structures
- Heuristics for efficient game solving.

QUANTLOG Workshop on Quantitative Logics July 11, 2009, Rhodes, Greece Satelite event of ICALP 2009 *quantlog09.web.auth.gr/*

The Workshop on Quantitative Logics (QUANTLOG 2009) will take place in Rhodes, Greece, July 11, 2009 as a satellite event of the 36th International Colloquium on Automata, Languages and Programming (ICALP 2009). It is organized under the auspices of the Department of Mathematics of the Aristotle University of Thessaloniki. The aim of the workshop is to provide a forum for researchers interested in the topic of quantitative logics to present their new results and to combine their efforts in the further development of the topic, with emphasis to its connection with automata theory as well as to practical applications.

Invited Tutorial: *Validation, Performance Analysis and Synthesis of Embedded Systems* **Kim G. Larsen, ARTIST Summer School in Europe, September 7-11, 2009, Autrans, France**

Keynote: *Verification and Performance Analysis of Embedded Systems* **Kim G. Larsen, TASE, 3rd IEEE International Symposium on Theoretical Aspects of Software Engineering,** July 29 - 31, 2009, Tianjin, China

Invited Tutorial: *Real-Time Systems Validation and Synthesis* **Kim G. Larsen, ARTIST Summer School in China, July 19-24, 2009, Tsinghua University, Beijing, China**

Invited Tutorial: *Real-Time Systems Validation and Synthesis* **Kim G. Larsen, Software Engineering Summer School, July 15-22, SEI East China Normal University, Shanghai, China**

Invited Talk*: Quantitative and Compositional Model Checking* **Kim G. Larsen, Seventh International Andrei Ershov Memorial Conference, June 15-19, 2009, Novosibirsk, Russia,**

Invited Talk: *Verification and Performance Analysis of Real-Time and Embedded Systems* **Kim G. Larsen, Joint China/Denmark Symposium on ICT, April 21-23, 2009, Odd Fellow Palæ, Copenhagen.**

Keynote: *Verification and Controller Synthesis of Real-Time Systems* **Kim G Larsen. 3rd International Conference on Fundamentals of Software Engineering, FSEN09, April 15-17, Kish Island, Iran**

Invited talk Kim G. Larsen Formal Methods for Components and Objects (FMCO'09)

Invited Talk: *Playing Games with Timed Interfaces* **Kim G Larsen COMBEST meeting on Interfaces, Rennes, France, March 3-4 2009. Invited Talk:** *Probabilistic Modal Transition Systems*

Kim G. Larsen, COMBEST meeting on Interfaces, Rennes, France, March 3-4 2009.
Keynote: *“Timing and Performance Analysis: Static Analysis versus Model Checking“*

Invited talk Joost-Pieter Katoen Nordic Workshop on Programming Theory

Invited talk Joost-Pieter Katoen IFIP WG 2.2 on Programming Concepts and Methodology

Invited talk Joost-Pieter Katoen CDC Workshop on Stochastic Hybrid Systems

Invited talk Joost-Pieter Katoen Formal Methods for Components and Objects (FMCO'09)

Invited talk Joost-Pieter Katoen Soiree FMWeek 2009

-- The above is new material, not present in the Y1 deliverable --

3. Milestones, and Future Evolution

3.1 Problem to be Tackled over the next 12 months (Jan 2010 – Dec 2010)

Uppsala will work on extending UPPAAL and TIMES for multiprocessor scheduling, in particular we will add the RTC analysis framework in the UPPAAL tool.

INRIA will be interested in stochastic games of imperfect information in the context of control synthesis. Also they will continue our work on the compositional design of timed systems. For model-based testing of timed systems, they intend to contribute to test generation and semantic coverage criteria.

IST Austria will continue the work on property-base mixed-signal validation by actively participating in a standardization committee for extending SystemVerilog Assertions (SVA) language with analogue operators.

Salzburg intends to work on developing variable-bandwidth servers (VBS) further. In particular, higher-level scheduling may enable non-trivial load balancing and power management while maintaining temporal isolation.

CEA aim at defining a testing framework for integration testing devoted to systems defined recursively by interconnecting heterogeneous components.

> To reach that goal they will investigate how to describe integration models of systems using the set of primitives defined in [GALB09] and how to define testing algorithms based on symbolic execution. The key point is to abstract away as much as possible of the knowledge of underlying component behaviors to only focus interaction rules. Indeed, focusing on those interaction rules allows one to define test purposes that involve interactions, which is the goal of integration testing. Moreover, abstracting away from component behaviors should limit complexity of symbolic computations due to internal treatment of data. That complexity is evenmore strengthened by potential heterogeneity of component models which would require the testing framework to take into account various modelling language, which we would like to avoid. We have shown ([EGLC09]) how to test orchestrations of web services by means of symbolic execution techniques. This is done possibly without any knowledge of web services models. The techniques presented in this contribution will be the starting point to abstract away from component knowledge when focussing on integration testing.

Aachen will further investigate compositional abstraction techniques for probabilistic systems, and apply abstraction technique to infinite-state tree-based probabilistic systems. Furthermore, they will intensivate our activities on model checking of CTMDPs.

Aachen will investigate parametric model checking of probabilistic models, including decidability issues, approximate algorithms, and if possible, prototypical tool development.
Also semantics of AADL including its error annex is planned and model checking support for this language will be developed.

VERIMAG will continue to work on Analysis of energy related properties of sensor Networks:

- Within the French RNTL ARESA-2 project we will focus on security solutions for WSN. In particular we will analyse the energy consumption of classical secure wireless protocols, and try to adapt them to this particular context.

- In order to produce long term simulation results and predict the entire network lifetime (which is unreachable with classical simulation techniques), we will combine our behavioural simulation model with a stochastic approach based on Markovian models.
- Enforcing global energy-related properties within a single node is particularly difficult because there is no centralized component able to manage the energy. We will work on dedicated architecture based on a centralized controller communicating with the drivers associated to each hardware component (radio, CPU, etc.). Controller synthesis techniques could then be used to generate such a controller from a set of global properties.

VERIMAG will continue the development of D-finder and of other structural and compositional verification methods for heterogeneous systems. In particular, Verimag plans to extend the verification techniques for BIP in two directions (1) to include incrementality support for invariant generation in D-Finder and (2) to develop, with INRIA, a statistical model-checking tool based on probabilistic simulation.

VERIMAG will finalize the connection from DOL, performance analysis tool developed by ETHZ, and handle the extra-functional layers i.e., the hardware and the mapping.

CISS will continue its work – often in collaboration with other partners of ARTIST Design – on developing the theoretical framework for extensions of timed automata, the algorithmic support and implementation in the UPPAAL tool suite as well as application. This includes :

- Continued effort on developing the theory of priced timed automata with negative and positive cost-rates and with linear and exponential cost-rates aiming at settling open decidability and complexity issues.
- Improved implementation of (probabilistic) reachability for probabilistic timed automata as well as their application to performance analysis of soft real-time systems.
- Application of the developed schedulability framework to an industrial case provided by the space division of Terma.
- Support for verification of timed automata models with respect to Live Sequence Charts.
- Implementation of a 64-bit version of UPPAAL in order to allow for the verification of timed automata models yielding larger state-spaces.
- Tool support for automatic test-case generation from UML state-charts utilizing an implemented translation to UPPAAL’s xml-format.
- Tool support for the compositional development methodology developed for timed systems. Direct support for refinement, consistency, compatibility between component specifications will be made utilizing the timed game engine of UPPAAL Tiga.

-- Changes wrt Y1 deliverable --

There is a visible trend that problems considered in Year 2 are linking methods for quantitative analysis with (quantitative extended) industrial design notations and also an increase in the industrial applications of the methods proposed.

3.2 Current and Future Milestones

The following highlights some of the problems of Section 3.1 to be worked on by the partners of the Validation Activity with explicit milestones to be reached before end of Year 2:

- **INRIA and CISS**
  will explore new coverage criteria for model-based testing which take into account the behaviors of systems, not only the structure of their description, as opposed to what is the usual approach. Based on these coverage criteria, design new test generation techniques.
  Semantic coverage criteria for model-based testing of timed systems

- **CEA**
  aim at defining a testing framework for integration testing devoted to systems defined recursively by interconnecting heterogeneous components. To reach that goal we will investigate how to describe integration models of systems using the set of primitives defined in [GALB09] and how to define testing algorithms based on symbolic execution. We will also study compositional results to state about the conformance of a system with respect to its model, by only performing unitary and integration testing.

  Testing framework for integration testing of systems defined by interconnecting heterogeneous components

- **IST**
  will continue the work on property-base mixed-signal validation by actively participating in a standardization committee
  Impact on extensions of SystemVerilog Assertions (SVA) language with analogue operators.

- **VERIMAG**
  will continue work on compositional verification methods for heterogeneous systems, as well as finalize work on connections from DOL.

  Tool support for compositional verification.

- **Aachen**
  will work on compositional abstraction verification techniques for probabilistic systems.

  Tool support for compositional abstraction of probabilistic systems.

- **Uppsala and CISS**
  will work on frameworks for schedulability analysis in the setting of multiprocessors and their realization in the verification tool UPPAAL.

- **CISS and INRIA**
  Will work on tool support for compositional verification of real-time systems.
  Tool support for refinement, consistency and compatibility checking of timed component specifications.

3.3 Main Funding

The ArtistDesign NoE funds integration and building excellence with the partners, and with the European research landscape as a whole. Beyond this “glue” for integration and excellence, during Year2 this activity has benefited from direct funding from:

- **UPMARC:** Uppsala Programming for Multicore Architectures Research Center, supported by the Swedish Research Council
- **CoDeR-MP** - Real-Time Applications on Multicore Platforms, Supported by the Swedish strategic research foundation.
- **CREDO (http://www.cwi.nl/projects/credo/),** Modeling and analysis of evolutionary structures for distributed services, supported by EU
- **Modeling and verification of timed systems supported by the Swedish research council**
- **ANR project TesTec**: Test of Real-time and critical embedded System. Industrial research project that gathers two companies: an end-user (EDF R&D) and one software editor for embedded real-time systems and automation systems (Geensys), and four laboratories from automation engineering and computer science (I3S, INRIA Rennes, LaBRI, LURPA). This project focuses on automatic generation and execution of tests for embedded real-time systems.
- **European Strep Project Combest** (http://www.combest.eu/home/). The aim of this project is to provide a theoretical framework as well as implemented methods and tools for the component-based design of embedded systems. Our role in Combest is to work on timed components, and more precisely develop a theory around timed modal specifications.
- **PHC Procope PIPS**: Partial Information Probabilistic Systems The objective of this bilateral collaboration with the group of Pr. Christel Baier in TU Dresden (Germany) is to study partially observable probabilistic systems.
- **INRIA - DGRST project** with ENIS Sfax in Tunisia (Maher Ben Jemaa and Moez Krichen) on model-based testing of embedded systems.
- **TReaTiES: Test of REAl-TIme Embedded Systems** (http://www.irisa.fr/vertecs/EA-Brazil09.html). INRIA associated team with Federal University of Campina Grande in Brazil (Pr. Patrícia D. L. Machado) and University Pernambuco (Pr. Augusto Sampaio) on test case generation, selection and abstraction for embedded real-time systems
- **The JAviator Project**, IBM Faculty Award 2007 (Helicopter Platform).
- **Concurrent Programming** with Threading by Appointment, Austrian Science Fund (FWF), Grant P18913-N15 (Three PhD students).
- **ArtistDesign, Austrian Federal Ministry of Science and Research**, Grant 651.394/0001-II/2/2009 (Supplemental Support).
- **RNTL project HeCoSim** (http://projet-hecosim.org/) The goal of this project is to study Simulation and validation of heterogeneous virtual platforms of automotive industrial use case, following two different approaches the co-simulation and the global simulation, on the base of existing tools and of generated critical scenarii.
- **ITEA2 project VERDE** (www.itea2.org/public/project_leaflets/VERDE_profile_oct-09.pdf) VERDE will develop and industrialisea solution for iterative, incremental development and validation of realtime embedded systems (RTES) in aerospace, software radio, railway and automotive domains. The project will integrate model-driven

engineering (MDE), component-based infrastructures and verification-and-validation (V&V) techniques.

- **ATESST** (Advancing Traffic Efficiency and Safety through Software Technology) ATESST2 is a two-year European project (FP7, Strep), coordinated by Volvo Technology and including OEMs, Suppliers/Tool vendors and Universities. http://www.atesst.org
- **CESAR** - Cost-efficient methods and processes for safety relevant embedded systems. CESAR is an Artemis project three year project resulting from the first call of Artemis. The project focuses on the gathering, and further development, of methods and tools for safety critical embedded systems. The project has a large number of industrial and academic partners.
  https://cesarproject.eu/index.php
- **SPEEDS IP Project**
  The SPEEDS project aims at significant enhancement of model-based systems engineering by semantics-based modelling for complex embedded systems using heterogeneous sub-system models, an by sound integration of existing and new tools using contract-based compositional analysis. Includes the ARTIST partners INRIA, OFFIS, PARADES and VERIMAG and affiliated industrial partners EADS and IAI.
  http://www.speeds.eu.com/
- **COMBEST (funded by European Union IST STREP)**
  COMponent-Based Embedded Systems design Techniques. COMBEST aims at enhancing techniques for the correct design of embedded systems. Combest emerged from collaborations in SPEEDS and ARTIST. Verimag, ETHZ, U. Braunschweig, IST, INRIA, OFFIS, U. Trento are partners.
  http://www.combest.eu
- **ARESA French National ANR project**
  The project aims at modelling energy consumption of Sensor networks with the aim to facilitate research, developments and commercialization of wireless sensor networks. Includes partners VERIMAG and affiliated partner FTRD.
  http://www-verimag.imag.fr/SYNCHRONE/index.php?page=fiche-aresa
- **French RNTL AVERILES Project**
  This project aims at the analysis and verification of embedded software systems with dynamic memory structures. It includes ARTIST partners VERIMAG and LSV, and affiliated partner LIAFA.
  www.lsv.ens-cachan.fr/rntl-averiles/
- **PROSYD IST Project**
  This project aims at the design of a standard, integrated property-based paradigm for the design of electronic systems building upon the emerging standard property specification language PSL/Sugar.
  http://www.prosyd.org/
- **MULTIFORM IST Project**
  This project aims Integrated Multi-formalism Tool Support for the Design of networked Embedded Control Systems. It includes ARTIST partners
  http://www.multiform.bci.tu-dortmund.de/

○ **Quasimodo.** This is a project under the 7th Framework Programme of the European Committee. The main goal of Quasimodo is to develop new techniques and tools for model-driven design, analysis, testing and code-generation for advanced embedded systems where ensuring quantitative bounds on resource consumption is a central

problem.
http://www.quasimodo.aau.dk/

- **DaNES - Danish Network of Embedded Systems**
  DaNES. Danish national project sponsored by the Danish Advanced Technology Foundation. The goal of DaNES is to determine, develop and test a model-driven and component-based development-process for the realization of the intelligent embedded systems of the future, cross-cutting the industrial sectors spanned by the participating partners.
  http://www.danes.aau.dk/
- **MT-LAB: Modeling Information Technology.** Danish national project sponsored by Villum-Kahn Rasmussne Foundation. A collaboration between CISS (Aalborg University), IMM (Denmark Technical University) and ITU (Copenhagen). The scope fo the research centre is to explore and develop methods for formal verification of modern advanced software systems. The aim is to develop new methods and expand the applicability of previous methods in order to formally verify the functionality of complex interacting modern software systems.
  http://www.mtlab.dk/

-- Changes wrt Y1 deliverable --

Whereas a number of funding sources from Year 1 have been terminated, an even larger number of funding sources has emerged for Year 2 comprised by a combination of newly started European projects and new (large) national projects.

4. Internal Reviewers for this Deliverable

- **Susanne Graf** (Verimag)
- **Bruno Bouyssounouse** (Verimag)