IST-214373 ArtistDesign
Network of Excellence
on Design for Embedded Systems

Activity - Progress Report for Year 1

JPRA Activity (WP3)

Validation

Clusters:

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 19th 2008

Table of Contents

1. Overview of the Activity

1.1 ArtistDesign Participants and Roles

Ed Brinksma (ESI - Netherlands);
Validation, 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 criteria, as well as for quantitative verification, control and diagnosis.

Christoph Kirsch (Salzburg - Austria)*;*
Compositional timing and reliability validation in HTL and the Exotask system.

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.

Joseph Sifakis, Susanne Graf (VERIMAG - France);
Component-based design, the BIP framework, platform-aware implementation of embedded systems, structural verification.
Context-based analysis

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);
Resource, verification and timing analysis.

1.2 Affiliated Participants and Roles

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

Prof. Tiziano Villa, University of Verona (Italy
Formal verification methods for hybrid systems. Competence in reachability for Hybrid Systems.

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 Tripkis – 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.

Holger Hermanns (Saarlandes 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.

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.

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.

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.

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.

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.

1.7 Problem Tackled in Year 1

Within the sub–activity A "Compositional Validation", we focus 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 has been addressed. Also, validation methods based on abstractions and refinements have been developed.

Within the sub-activity B "Quantitative Validation", we provide (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 has been made towards controller synthesis from rich game models as well as conformance testing of non-functional propeties.

We give below a more detailed view of each sub-activity:

Sub-activity A: Compositional Validation

CVF and LSV has worked on model checking based on refinement of abstract domains.

Achen has developed three-valued abstraction techniques for probabilistic systems, in particular interval MDPs and their continuous-time variants. It has been shown that these abstractions are "safe" and preserve a rich class of logical properties.

Aachen has developed compact representations for counterexamples in quanti- tative model checking using regular expressions, and established a connection between counterexample generation and shortest-path algorithms.

OFFIS tackled during the year compositional safety and failure propagation analyses. For a hierarchical model, it is computed whether a safety assertion for the model is dominated (a specific form of implication) by the assertions for its components. And based on failure-propagation assertions for its sub-components, fault trees for component failures are derived. The deployment synthesis which had been planned for the first year has been delayed to the second.

KTH in cooperation with Volvo Techology have been investigating methods and tools to support the design of dynamically configurable systems and their validation (corresponding models and algorithms for adaptivity are described in the corresponding activity reports). We are in particular exploring the systematic usage of traditional safety and robustness analysis methods, together with simulation and formal verification. The work has been performed in the DySCAS project (www.dyscas.org).

KTH in cooperation with Volvo Technology, in the context of DySCAS (www.dyscas.org) and ATESST (www.atesst.org), have been investigating the incorporation of state-of the art techniques for high-level compositional safety and reliability analysis of automotive embedded systems.

CISS is working Modal transistion systems as interface specifications. This work is with ITU in Denmark and Imperial College in UK.

Verimag has continued its work on deadlock detection/verification and its implementation in the DeadlockFinder tool by combining structural analysis for component behaviours with structural analysis of connectors.

Verimag has developed a general framework for contract-based reasoning allowing circular reasoning and proposed some instances of it.

Sub-activity B: Quantitative Validation

VERIMAG is studying quantitative properties of programs with arrays and dynamic data structures. This year we have proposed two decidable logics for the expression of such properties.

VERIMAG has developed a method for generating scheduling policies for streams with structured jobs.

VERIMAG has developed a verification technique for Linear Hybrid Automata based on the use of linear constraints for the expression of path condition and implemented in the PHAVer tool.

VERIMAG has studied the analysis of energy consumption of wireless sensor networks and developed a framework for the validation of wireless sensor networks (WSNs) with respect to energy consumption.

VERIMAG has worked on the evaluation of the memory consumption of an application on a given platform architecture using symbolic polynomial approximations of the amount of dynamic memory required.

VERIMAG and ETHZ have collaborated on the evaluation of performance properties with by connecting the DOL tool with BIP in order to refine DOL analysis with an executable specification.

EPFL has defined a new framework to integrate different techniques of program analysis, and allowing to switch from one to the other for improving the performance of the verification.

EPFL has worked on quantitative models: new models and algorithms for model-checking of Markov chains, and for constructing robust controllers in timed games.

EPFL has pursued the formal description and analysis of transactional memory protocols.

EPFL made a survey on value iteration algorithms on graphs. Such algorithms can be used for determining the existence of certain paths (model checking), the existence of certain strategies (game solving), and the probabilities of certain events (performance analysis) [CH08].

LSV has tackled the problem of quantitative verification of extensions of timed automata: alternative semantics of timed automata: the usual semantics is a mathematical idealization, assuming infinite precision of the hardware.

LSV has studied alternative semantics that are more "robust". weighted timed automata: timed automata have been extended to include "costs", ie. real-valued variables that do not interfere with thebehaviour of the system. This naturally leads to quantitative evaluation and optimization problems.

INRIA worked on verification of systems with queues and stacks, quantitative model-checking of timed-automata and decidability questions on probabilistic Büchi automata.

CISS is working multipriced timed automata with emphasis on Pareto-optimal reachaibility and optimal infinite scheduling.

CISS is working one-clock priced timed automata with emphasis on model checking as well as optimal strategies. This work is in collaboration with LSV, ENS Cachan, France.

CISS is working on energy-constrained infinite runs in priced timed automata. This work is in collaboration with LSV, ENS Cachan, France.

CISS is working on algorithms for time-bounded, probabilistic reachability for probabilistic timed automata.

Sub-activity C: Croos-Layer Validation

VERIMAG has proposed several methods for testing and monitoring real-time properties. We developed a memory efficient test generation for analog clock tests. We also propose a method for the generation of path conditions taking concurrency into account.

EPFL has developed new algorithms to solve game questions that arise in the automatic synthesis from formal specification, such as constructing a correct controller in the context of imperfect information, correcting unrealizable specifications, and synthesizing resource-constrained controllers.

CISS and CVF has worked on efficient algorithms and tool implementation for the synthesis of timed controller.

ESI has worked on the Trader project addressing the problem of high product failures that are exposed to the user. Reliability is to be ensured by studying and showing proof of concept of methods to be applied at design time, test time, and product run-time.

ESI has worked on the Poseidon project addressing the challenge of gaining flexibility, adaptability and evolvability while retaining reliability at the same time.

INRIA worked on diagnosis for discrete event systems, diagnosis and control synthesis for information flow security as well as modular control synthesis.

INRIA worked on integration of verification and conformance testing.

Salzburg has in collaboration with the Technical University of Timisoara, Cadence, UC Berkeley, and EPFL introduced the notion of logical reliability for real-time software tasks as a way to model the desired, long-run rather than the estimated, short-term reliability of real-time computation. Here, a program is correct if its estimated, short-term reliability is sufficiently high to guarantee its logical reliability in the long run.

CISS is working model-based testing based on timed automata using the UPPAAL verification engine. Support for both off-line and on-line test generation.

CISS is working on synthesis algorithms for timed games with partial observability with emphasis on synthesis of strategies for reachability and safety objectives. This work is in collaboration with INRIA (Rennes), France and CFV, Belgium.

2. Summary of Activity Progress

2.1 Technical Achievements

Program Analysis: Dynamic combination of multiple program analyzes and proving non-termination. (EPFL)
We present and evaluate a framework and tool for combining multiple program analyzes which allows the dynamic (on-line) adjustment of the precision of each analysis depending on the accumulated results. For example, the explicit tracking of the values of a variable may be switched off in favor of a predicate abstraction when and where the number of different variable values that have been encountered has exceeded a specified threshold. The method is evaluated on verifying the SSH client/server software and shows significant gains compared with predicate abstraction-based model checking [BHT08].
The search for proof and the search for counterexamples (bugs) are complementary activities that need to be pursued concurrently in order to maximize the practical success rate of verification tools. While this is well-understood in safety verification, the current focus of liveness verification has been almost exclusively on the search for termination proofs. A counterexample to termination is an infinite program execution. In this paper, we propose a method to search for such counterexamples. The search proceeds in two phases. We first dynamically enumerate lasso-shaped candidate paths for counterexamples, and then statically prove their feasibility. We illustrate the utility of our nontermination prover, called TNT, on several nontrivial examples, some of which require bit-level reasoning about integer representations [GHM+08].

Games for Verification and Synthesis (EPFL)

The game framework is a natural model to formalize the controller synthesis problem where one player (the program or controller) has to entail some objective (the specification) no matter how the other players (other programs and external environment) behave. A model of the controller can be extracted from the synthesis of a winning strategy in such a game.

Several issues have been addressed about games for synthesis:

- [Strategy construction] We have developed an algorithm for constructing the winning strategies in parity games of imperfect information. We have implemented this algorithm as a prototype. To our knowledge, this is the first implementation of a procedure for solving imperfect-information parity games on graphs [BCD+08].
- [Environment assumptions] The synthesis problem asks to construct a reactive finite-state system from an omega-regular specification. Initial specifications are often unrealizable, which means that there is no system that implements the specification. A common reason for unrealizability is that assumptions on the environment of the system are incomplete. We study the problem of correcting an unrealizable specification g by computing an environment assumption a such that the new specification a -> g is realizable. Our aim is to construct an assumption a that constrains only the environment and is as weak as possible. We show that the problem of finding a minimal set of fair edges is computationally hard, and we use probabilistic games to compute a locally minimal fairness assumption [CHJ08].
- [Resource-constrained games] We study the controller synthesis problem under budget constraints. In this problem, there is a cost associated with making an observation, and a controller can make only a limited number of observations in each round so that the total cost of the observations does not exceed a given fixed budget. The controller must ensure

some omega-regular requirement subject to the budget constraint. Such budget constraints arise in designing and implementing controllers for resource-constrained embedded systems, where a controller may not have enough power, time, or bandwidth to obtain data from all sensors in each round. We also study the budget optimization problem, where given a plant, an objective, and observation costs, we have to find a controller that achieves the objective with minimal accumulated cost (or minimal peak cost).We show that these problems are reducible to games of imperfect information where the winning objective is a conjunction of an omega-regular condition and a long-run average condition (or a least max-cost condition), and leads to an exponential-time algorithm [CMH08].

- [Robustness in timed games] We consider two-player games played in real time on game structures with clocks and parity objectives. The games are concurrent in that at each turn, both players independently propose a time delay and an action, and the action with the shorter delay is chosen. To prevent a player from winning by blocking time, we restrict each player to strategies that ensure that the player cannot be responsible for causing a Zeno run. First, we present an efficient reduction of these games to turn-based (i.e., non-concurrent) finite-state (i.e., untimed) parity games. The states of the resulting game are pairs of clock regions of the original game. Our reduction improves the best known complexity for solving timed parity games. Moreover, the rich class of algorithms for classical parity games can now be applied to timed parity games. Second, we consider two restricted classes of strategies for the player that represents the controller in a real-time synthesis problem, namely, limit-robust and bounded-robust strategies. Using a limit-robust strategy, the controller cannot choose an exact real-valued time delay but must allow for some nonzero jitter in each of its actions. If there is a given lower bound on the jitter, then the strategy is bounded-robust. We show that exact strategies are more powerful than limit-robust strategies, which are more powerful than bounded-robust strategies for any bound. For both kinds of robust strategies, we present efficient reductions to standard timed automaton games. These reductions provide algorithms for the synthesis of robust real-time controllers [CHP08].

Verification of Markov chains (EPFL)
We have studied two problems about Markov chains. First, we considerInterval-valued Discrete-time Markov Chains (IDTMC) for which the exact transition probabilities are notknown. Instead in IDTMCs, each transition is associated with an interval in which the actual transition probability must lie. Second, we consider the equivalence problem for labeled Markov chains (LMCs), where each state is labeled with an observation. Two LMCs are equivalent if every finite sequence of observations has the same probability of occurrence in the two LMCs.

We consider two semantic interpretations for the uncertainty in the transition probabilities of an IDTMC. In the first interpretation, we think of an IDTMC as representing a (possibly uncountable) family of (classical) discrete-time Markov Chains, where each member of the family is a Markov Chain whose transition probabilities lie within the interval range given in the IDTMC. We call this semantic interpretation Uncertain Markov Chains (UMC). In the second semantics for an IDTMC, which we call Interval Markov Decision Process (IMDP), we view the uncertainty as being resolved through nondeterminism. In other words, each time a state is visited, we adversarially pick a transition distribution that respects the interval constraints, and take a probabilistic step according to the chosen distribution. We introduce the logic omega-PCTL, which can express liveness, strong fairness, and omega-regular properties (such properties cannot be expressed in PCTL). We show that the omega-PCTL model checking problem for Uncertain Markov Chain semantics is decidable in PSPACE (same as the best known upper bound for PCTL) and for Interval Markov Decision Process semantics is decidable in coNP (improving the previous known PSPACE bound for PCTL). We also show that the qualitative fragment of the logic can be solved in coNP for the UMC interpretation, and

can be solved in polynomial time for a subclass of UMCs. We also prove lower bounds for these model checking problems. We show that the model checking problem of IDTMCs with LTL formulas can be solved for both UMC and IMDP semantics by reduction to the model checking problem of IDTMC with omega-PCTL formulas [CSH08].

We show that equivalence of LMC can be decided in polynomial time, using a reduction to the equivalence problem for probabilistic automata, which is known to be solvable in polynomial time. We provide an alternative algorithm to solve the equivalence problem, which is based on a new definition of bisimulation for probabilistic automata. We also extend the technique to decide the equivalence of weighted probabilistic automata [DHR08].

Model-checking transactional memories (EPFL)
Software transactional memory (STM) offers a disciplined concurrent programming model for exploiting the parallelism of modern processor architectures. We present the first deterministic specification automata for strict serializability and opacity in STMs. Using an antichain-based tool, we show our deterministic specifications to be equivalent to more intuitive, nondeterministic specification automata (which are too large to be determinized automatically). Using deterministic specification automata, we obtain a complete verification tool for STMs. We also show how to model and verify contention management within STMs. We automatically check the opacity of popularSTM algorithms, such as TL2 and DSTM, with a universal contention manager. The universal contention manager is nondeterministic and establishes correctness for all possible contention management schemes [GHS08].

Model checking software transactional memories (STMs) is difficult because of the unbounded number, length, and delay of concurrent transactions and the unbounded size of the memory. We show that, under certain conditions, the verification problem can be reduced to a finite-state problem, and we illustrate the use of the method by proving the correctness of several STMs, including two-phase locking, DSTM, TL2, and optimistic concurrency control. The safety properties we consider include strict serializability and opacity; the liveness properties include obstruction freedom, livelock freedom, and wait freedom. Our main contribution lies in the structure of the proofs, which are largely automated and not restricted to the STMs mentioned above. In a first step we show that every STM that enjoys certain structural properties either violates a safety or liveness requirement on some program with two threads and two shared variables, or satisfies the requirement on all programs. In the second step we use a model checker to prove the requirement for the STM applied to a most general program with two threads and two variables. In the safety case, the model checker constructs a simulation relation between two carefully constructed finite-state transition systems, one representing the given STM applied to a most general program, and the other representing a most liberal safe STM applied to the same program. In the liveness case, the model checker analyzes fairness conditions on the given STM transition system [GHJS08].

Model-checking and Synthesis for linear time temporal logic (EPFL)
The linear temporal logic (LTL) was introduced by Pnueli as a logicto express properties over the computations of reactive systems.

- [Efficient model-checking] We propose new efïcient algorithms for LTL satisfiability and model-checking. Our algorithms do not construct nondeterministic automata from LTL formulas but work directly with alternating automata using efï□cient exploration techniques based on antichains [DDMR08a].We have developed a tool called ALASKA that implements these new algorithms to decide the satisfiability and validity problems for LTL, and to solve the model-checking problem for LTL over symbolic (BDD-encoded)Kripke structures [DDMR08b].

- [Fixing faults] Knowing that a program has a bug is good, knowing its location is better, but a fixis best. We present a method to automatically locate and correct faults in a finite state system, either at the gate level or at the source level. We assume that the specification is given in LTL, and state the correction problem as a game, in which the protagonist selects a faulty component and suggests alternative behavior. The basic approach is complete but as complex as synthesis. It also suffices from problems of readability: the correction may add state and logic to the system. We present two heuristics. The ï¬rst avoids the doubly exponential blowup associated with synthesis by using nondeterministic automata. The second heuristic ï¬nds a memoryless strategy, which we show is an NP-complete problem. A memoryless strategy corresponds to a simple, local correction that does not add any state. The drawback of the two heuristics is that they are not complete unless the specification is an invariant. Our approach is general: the user can deï¬ne what constitutes a component, and the suggested correction can be an arbitrary combinational function of the current state and the inputs. We show experimental results supporting the applicability of our approach [JSGB08].

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

Infinite Runs in Weighted Timed Automata with Energy Constraints (**CISS** + LSV)
We study the problems of existence and construction of infinite schedules for finite weighted automata and one-clock weighted timed automata, subject to boundary constraints on the accumulated weight. More specifically, we consider automata equipped with positive and negative weights on transitions and locations, corresponding to the production and consumption of some resource (e.g. energy). We ask the question whether there exists an infinite path for which the accumulated weight for any finite prefix satisfies certain constraints (e.g. remains between 0 and some given upper-bound). We also consider a game version of the above, where certain transitions may be uncontrollable.

Complexity of Decision Problems for Mixed and Modal Specifications (**CISS** + ITU, Copenhagen and Imperial College London)
We consider decision problems for modal and mixed transition systems used as specifications: the common implementation problem (whether a set of specifications has a common implementation), the consistency problem (whether a single specification has an implementation), and the thorough refinement problem (whether all implementations of one specification are also implementations of another one). Common implementation and thorough refinement are shown to be PSPACE-hard for modal, and so also for mixed, specifications. Consistency is PSPACE-hard for mixed, while trivial for modal specifications. We also supply upper bounds suggesting strong links between these problems.

Testing Real-Time Systems Using UPPAAL (**CISS** + Uni. Uppsala)
This chapter presents principles and techniques for model-based black-box conformance testing of real-time systems using the Uppaal model-checking tool-suite. The basis for testing is given as a network of concurrent timed automata specified by the test engineer. Relativized input/output conformance serves as the notion of implementation correctness, essentially timed

trace inclusion taking environment assumptions into account. Test cases can be generated offline and later executed, or they can be generated and executed online. For both approaches this chapter discusses how to specify test objectives, derive test sequences, apply these to the system under test, and assign a verdict.

Fast Directed Model Checking Via Russian Doll Abstraction (CISS + Uni. Freiburg and Uni. Innsbruck)
Directed model checking aims at speeding up the search for bugs in a system through the use of heuristic functions. Such a function maps states to integers, estimating the state's distance to the nearest error state. The search gives a preference to states with lower estimates. The key issue is how to generate good heuristic functions, i.e., functions that guide the search quickly to an error state. An arsenal of heuristic functions has been developed in recent years. Significant progress was made, but many problems still prove to be notoriously hard. In particular, a body of work describes heuristic functions for model checking timed automata in Uppaal, and tested them on a certain set of benchmarks. Into this arsenal we add another heuristic function. With previous heuristics, for the largest of the benchmarks it was only just possible to find some (unnecessarily long) error path. With the new heuristic, we can find provably shortest error paths for these benchmarks in a matter of seconds. The heuristic function is based on a kind of Russian Doll principle, where the heuristic for a given problem arises through using Uppaal itself for the complete exploration of a simplified instance of the same problem. The simplification consists in removing those parts from the problem that are distant from the error property. As our empirical results confirm, this simplification often preserves the characteristic structure leading to the error.

Model-checking one-clock priced timed automata (**CISS** + LSV)
We consider the model of priced (a.k.a. weighted) timed automata, an extension of timed automata with cost information on both locations and transitions, and we study various model-checking problems for that model based on extensions of classical temporal logics with cost constraints on modalities. We prove that, under the assumption that the model has only one clock, model-checking this class of models against the logic WCTL, CTL with cost-constrained modalities, is PSPACE-complete (while it has been shown undecidable as soon as the model has three clocks). We also prove that model-checking WMTL, LTL with cost-constrained modalities, is decidable only if there is a single clock in the model and a single stopwatch cost variable (i.e., whose slopes lie in {0,1}).

Optimal infinite scheduling for multi-priced timed automata (**CISS + ESI** + LSV)

This work is concerned with the derivation of infinite schedules for timed automata that are in some sense optimal. To cover a wide class of optimality criteria we start out by introducing an extension of the (priced) timed automata model that includes both costs and rewards as separate modelling features. A precise definition is then given of what constitutes optimal infinite behaviours for this class of models. We subsequently show that the derivation of optimal non-terminating schedules for such double-priced timed automata is computable. This is done by a reduction of the problem to the determination of optimal mean-cycles in finite graphs with weighted edges. This reduction is obtained by introducing the so-called corner-point abstraction, a powerful abstraction technique of which we show that it preserves optimal schedules.

We prove the decidability of the minimal and maximal reachability problems for multi-priced timed automata, an extension of timed automata with multiple cost variables evolving according to given rates for each location. More precisely, we consider the problems of synthesizing the minimal and maximal costs of reaching a given target location. These problems generalize conditional optimal reachability, i.e., the problem of minimizing one

primary cost under individual upper bound constraints on the remaining, secondary, costs, and the problem of maximizing the primary cost under individual lower bound constraints on the secondary costs. Furthermore, under the liveness constraint that all traces eventually reach the goal location, we can synthesize all costs combinations that can reach the goal.

Optimal reachability for multi-priced timed automata (CISS)
The decidability of the minimal reachability problem is proven by constructing a zone-based algorithm that always terminates while synthesizing the optimal cost tuples. For the corresponding maximization problem, we construct two zone-based algorithms, one with and one without the above liveness constraint. All algorithms are presented in the setting of two cost variables and then lifted to an arbitrary number of cost variables.

Development of UPPAAL (CISS)
In 2008 the concrete simulator of UPPAAL-TIGA was improved. It is now more stable and its interface has been updated. Another completely new algorithm was implemented to handle timed games with partial observability. It is now possible to define actions on edges inside the graphical editor and define observations when checking properties. The implementation only need to have loop detections added to be complete w.r.t. our paper. A second new major feature was also the implementation of timed games with Buchi accepting states, while avoiding some other bad states. This new algorithm is on-the-fly in the sense that it can stop whenever it has found a stable set of accepting and winning states. It works in two stages where a fix-point on the set of winning states is computed and then a fix-point on the set of winning states that are Buchi accepting.
Concerning UPPAAL, the engine is now able to merge DBMs dynamically when exploring the state-space. This is a transparent feature for the user. This is done automatically whenever possible.
Another new feature has been the addition of stop-watches. It is now possible to add to locations expressions of the form "x'==expr" where x is a clock and expr an expression evaluating to 0 or 1. There is no other needed syntax additions. Any clock can be stopped. However, the algorithm used becomes an over-approximation whenever a state that is stopping a clock is reached.

We also mention that the DBM library has been updated internally to cope with the extensions we have made. A new version will be released soon.

Discount-Optimal Infinite Runs in Priced Timed Automata (CISS)
Discount-optimal infinites scheduling for priced timed automata has been shown decidable using region-based techniques (so-called corner-point abstraction). Using discounting in optimization criteria is a often used in Control Theory, and leads to a simple fixed-point characterization in the setting of weighted timed automata. The fixed-point characterization suggests an efficient algorithm in contrast to limit-ratio optimality.

Off-line test case generation (CISS)
Off-line test-case generation from I/O timed automata models using increasingly techniques depending on properties of the given model. The techniques ranges from model checking (suitable if the model is controllable, i.e. deterministic and has neither timing uncertainty nor conflicting outputs), synthesis of testing strategy (suitable if the model is deterministic but fully observable), synthesis of strategy under partial observability. Also, testing strategies with respect to a given test purpose but relying on corporation from the system under test have been given.

Slicing for UPPAAL (CISS)
The focus of this thesis is to introduce slicing for Uppaal. Slicing is a technique based on static analysis used to reduce the syntactic size of models or applications. In this thesis, we show how slicing may be used to construct reachability preserving reductions of Uppaal models possibly improving the performance of the tool. Using automated slicing in Uppaal will eliminate the need for users to manually optimize models for faster verification of a certain property. Moreover, it allows less experienced users of Uppaal, which unknowingly may design models, containing unnecessary large amounts of data, to verify properties which \uppaal otherwise would have been unable to check.

Model-based Schedulability Analysis of Safety Critical Hard Real-Time Java Programs (CISS)

We describe the implementation of SARTS, a model based schedulability analysis tool used for hard real-time systems. SARTS is used to translate hard real-time systems, implemented in Java, to a timed automata model in UPPAAL.

The system being analyzed must be implemented in SCJ2, a safety critical profile for Java developed in this project, based on SCJ. The target hardware is the time predictable Java processor JOP, developed specifically for hard real-time systems.

Several experiments have been conducted to illustrate the accuracy of SARTS compared to existing tools. It is shown how the model based approach can result in a more accurate analysis, than possible with traditional analyses.

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

Synthesis with incomplete information (CISS, CVF and EPFL)
We have continued our collaboration with EPFL on algorithms for the synthesis of controller with imperfect information. In this research, we have proposed a fixed point theory to solve games of imperfect information. The fixed point theory is defined on the lattice of antichains of sets of states. Contrary to the classical solution proposed by Reif, our new solution does not involve determinization. As a consequence, it is readily applicable to classes of systems that do not admit determinization. Notable examples of such systems are timed and hybrid automata. As an application, we show that the discrete control problem for games of imperfect information defined by rectangular automata is decidable. This result extends a result by Henzinger and Kopke.

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

Synthesis of timed controllers - Industrial case study (CISS and CVF)

In this work, 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.

Quantitative properties of timed automata under alternative semantics (LSV)
We developped a new approach, using channel-automata techniques, for verifying that a system *robustly* satisfies a quantitative property (w.r.t. time), even under some imprecisions of the clocks. We have developed algorithms for checking quantitative properties of a probabilistic semantics of timed automata, in order to compute the proportion of executions that satisfy a given property.

Timed automata with energy constraints (CISS and LSV)
We studied a new kind of problems in weighted timed automata, where the aim is to keep the value of the cost within certain bounds. We developped algorithms for some cases and proved undecidability for the case of games. A number of interesting case remain open.

We study the problems of existence and construction of infinite schedules for finite weighted automata and one-clock weighted timed automata, subject to boundary constraints on the accumulated weight. More specifically, we consider automata equipped with positive and negative weights on transitions and locations, corresponding to the production and consumption of some resource (*e.g.* energy). We ask the question whether there exists an infinite path for which the accumulated weight for any finite prefix satisfies certain constraints (*e.g.* remains between 0 and some given upper-bound). We also consider a game version of the above, where certain transitions may be uncontrollable.

Contract-based verification for rich interaction models (Verimag):
We have proposed a general framework for contract-based reasoning. Previously, we started from contracts and notions of satisfaction of contracts and dominance between contracts as they are defined in the SPEEDS project and from similar notions in the literature. We had made some proposals for the expression of proper encapsulation in BIP and had given a proof rule for dominance in the resulting framework [GQ07]. Now we have generalised the contract-related concepts defined in HRC and defined a contract framework by (1) a behaviour description formalism, (2) a set of composition operators $\gamma \in \Gamma$ with a composition on Γ as in BIP, such that each γ represents a composition $[\gamma]$ on behaviours, and (3) a notion of refinement under context on behaviours. Circular reasoning is defined as a property of refinement under context preorder, and a set of proof rules are given representing sufficient conditions for proving dominance, that is refinement between contracts, for any framework allowing circular reasoning. We study 2 particular instances of that framework: the first one – corresponding to the simplest framework considered in SPEEDS - uses I/O automata to describe behaviours with the usual composition operator and a notion of refinement based on trace inclusion [QG08b]. In the second one behaviours are defined by modal transition systems, allows all composition operators definable in BIP – that means any composition definable by SOS rules – and refinement under context is obtained as a strengthening of the usual notion of simulation between MTS. This framework allows the expression of both safety and progress properties and their compositional verification [QG08a]. We are also implementing a tool verifying and constructing contracts.

Compositional Verification for Component-based Systems (Verimag):
Verimag worked 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.

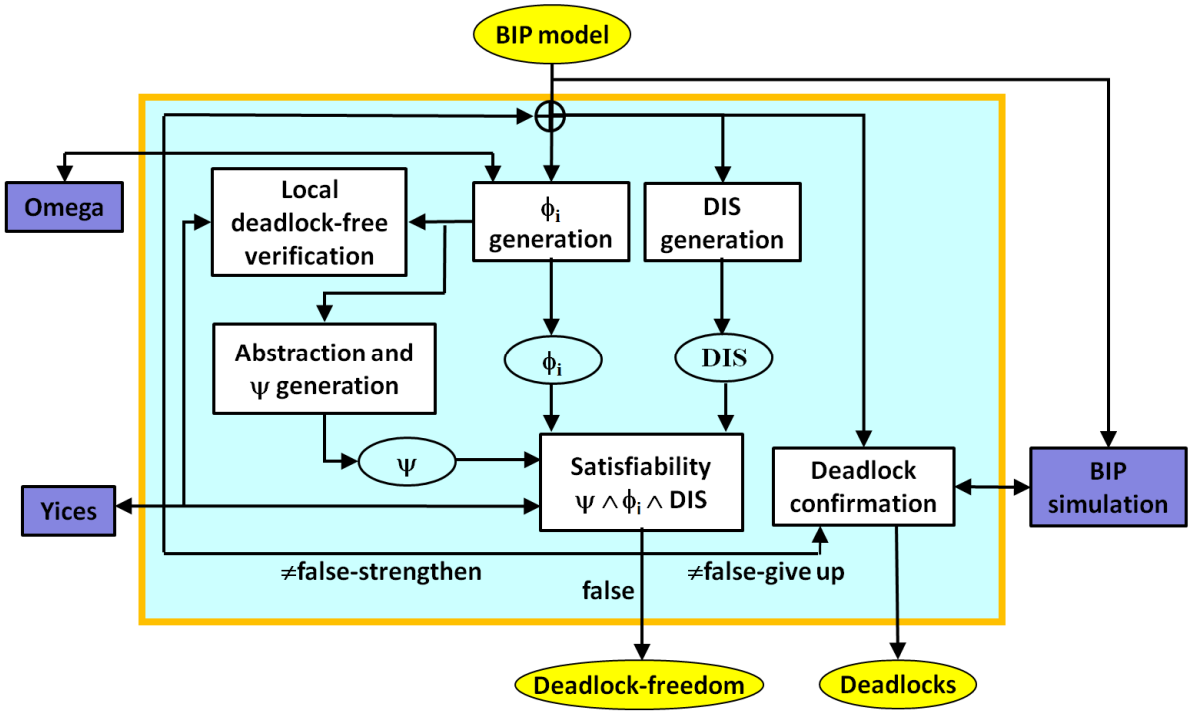


Figure 1 Functional view of the D-finder tool

The D-Finder toolset 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 [BBSN08].

Logics for programs with integer arrays (Verimag, LIAFA)
Programs with integer arrays pose interesting challenges for the existing methods and tools for software verification. In particular, logics for reasoning about infinite state spaces modeling unbounded arrays are required by e.g. predicate abstraction, abstract interpretation or Hoare-style program proofs. Moreover, push-button verification needs decidable logics in which program properties can be expressed.

We have developped two decidable logics in which universally quantified array properties can be expressed. These logics enhance the expressivity of existing logics by allowing arithmetic comparisons between adjacent elements of arrays (such as difference bounds constraints or octagonal constraints). The decision procedures for the logics are based on translations to

classes of counter automata, for which the emptiness problem (existence of a run leading to some final state) is decidable [HIV08a, HIV08b, NV08].

Monitoring Real-Time Properties (Verimag, Weizman)
Formal verification is a very ambitious activity due to its exhaustiveness and for this reason testing/simulation are still the most commonly used validation techniques. Nevertheless, testing can be made more formal by employing a precise formal specification logic based on temporal logic, against which simulation traces can be checked. This technique called monitoring or runtime verification is gaining popularity and it does not suffer from the state explosion and other difficulties associated with traditional model checking. Motivated by the verification of analog circuits we have developed new algorithms for monitoring timed and hybrid temporal properties, expressed in the logic MITL, against Boolean and analog signals [MPN+08]. We have developed a tool that has rised interest in several companies (ST, Freescale, Rambus and Mentor Graphics) and applied it to several case studies.
http://www-verimag.imag.fr/TEMPORISE/AMT/

Generating Analog-Clock Real-Time Testers Using Action Refinement Techniques:
In a previous work we proposed a method for generating digital-clock tests for real-time systems using action refinement techniques. We have extended this method for generating analog-clock testers. Analog-clock testers are testers which can observe real-time with precision. Our goal from testing is to check the conformance of a given implementation with respect to a given specification (the model). The main benefit of the method is to save memory space needed to build and to store tests. One important contribution of this work is a simplified way for both modelling and testing real-time systems. We first write a (high-level) simplified version of the model of the system, as an input-output transition system (IOTS) and then we refine it into a more detailed (low-level) model as a timed input-output transition system (TIOTS). This same mechanism applies to the test generation procedure [BKT08a].

Automatic Generation of Path Conditions for Concurrent Timed Systems:
We concentrate on the automatic generation of test cases for concurrent real-time systems. In order to test a particular behavior of the system, we generate path conditions for (concurrent real-time) execution paths. Instantiating such path conditions allows us to test the desired path. We do not assume finite state systems. Hence our modeled systems may reference unbounded variables in tests and assignments (when we ignore the particular word length in a given machine). Such a precondition characterizes all the states from which we can execute the path. However, there may be other possible executed paths, due to nondeterministic choice, which can be eliminated by adding further synchronization. The path condition calculation can be used in a model checking search, hunting for a path satisfying a given temporal property. It allows us to verify a procedure or collection of procedures in isolation, without providing initial values. Using the weakest precondition calculation, verification is performed symbolically, or for all parameters at once? The temporal property is translated into an automaton and contributes to calculation of the path condition (i.e., it is a condition for executing a path while satisfying the temporal property).

For the real-time case, we need to generalize the calculation of a path condition, taking into account only the essential conditions to follow a particular path in the execution. For example, if the path is ***abcd***, we may constrain only ***a*** to precede ***b***, for being on the same process, ***c*** to precede ***d***, again, for being on the other process, and ***b*** to precede ***d***, for referring to the same variable. We start with a given path (in the flow chart, or interleaved from different flow charts for concurrent processes) merely from a practical consideration; it is very simple to specify an interleaved execution sequence. However, we look at the essential partial order, which is consistent with real-time constraints, rather than at the total order. We cannot assume that transitions must follow each other, unless this order stems from some sequentiality constraints

(such as transitions belonging to the same process or using the same variable) or from timing constraints. Thus, with the above restrictions, ***acbd*** is equivalent to ***abcd*** and represents the same (partial order) execution. For untimed systems, there is no difference between the condition for partial order execution and the condition for executing any of the sequences (linearizations) consistent with it. Because of commutativity between concurrently executed transitions, we obtain the same path condition either way. However, when taking time constraints into account, the actual time and order between occurrences of transitions does affect the path condition (which now includes time information) **[BPT08].**

Scheduling Policies for Streams of Structured Jobs (Verimag)

The need to process efficiently streams of tasks that arrive nondeterministically is a crucial problem in embedded system design. Traditional models of real-time systems are not always appropriate for these situations as they often treat periodic and independent tasks. We have defined a new class of scheduling problems where a request generator (a timed language) models the requests which are themselves, partially-ordered sets of tasks (jobs) that may require different types of resources. On these models we prove some fundamental results concerning schedules and scheduling strategies of bounded backlog and latency [DM08].

Formal Verification of Linear Hybrid Automata with PHAVer (Verimag)

Linear hybrid automata (LHA) are characterized by piecewise constant bounds on the derivatives. They are of interest in formal verification because their dynamics are so simple that basic operators such as discrete and continuous successor states can be computed with exact integer arithmetic, and relatively efficiently over an infinite time horizon. Our tool PHAVer uses exact polyhedral computations to compute the set of reachable states and to verify equivalence and abstraction between automata using assume/guarantee reasoning. Its characteristic is the ability to conservatively overapproximate polyhedra with polyhedra of substantially lower complexity. It is also able to handle more complex dynamics, a generalized form of piecewise affine dynamics, by overapproximation. On-the-fly, adaptive partitioning allows us to target the accuracy of the overapproximation to relevant parts of the state space. Forward/backward refinement, in which the partitioning is iteratively refined while alternating forward and backward reachability, has allowed us to formally verify oscillation of a nonlinear circuit model with three state variables.

Another verification approach for LHA avoids polyhedral computations altogether. It exploits the fact that for LHA reachability along a given path can be formulated as satisfiability of a conjunction of linear constraints, and can therefore be computed very efficiently using linear programming techniques. Various methods of counter example guided abstraction refinement have been proposed in literature to verify safty. We have generically extended these methods to parameter synthesis [Fre08].
http://www-verimag.imag.fr/~frehse/phaver_web/index.html

Quantitative analysis of embedded software (Verimag)

In [BFG+08] we have developed a technique to compute symbolic polynomial approximations of the amount of dynamic memory required to safely execute a method without running out of memory, for Java-like imperative programs. Given an initial configuration of the stack and the heap, the peak memory consumption is the maximum space occupied by newly created objects in all states along a run from it. We over-approximate the peak memory consumption using a scoped-memory management where objects are organized in regions associated with the lifetime of methods. We model the problem of computing the maximum memory occupied by any region configuration as a parametric polynomial

optimization problem over a polyhedral domain and resort to Bernstein basis to solve it. We apply the developed tool to several benchmarks.

Analysis of Energy related properties of sensor Networks (Verifmag)

VERIMAG has started recently to study simulation of wireless sensor networks for the purpose of estimating network lifetime. Network lifetime is determined by the energy consumption due to commutations in individual nodes and communication activities. Large scale deployement of a WSN still faces a number of challenging problems. In particular, lowering energy consumption is a critical issue as long-term network lifetimes (more than 10 years) must be guaranteed. 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 have in particular addressed the problem of developing accurate prototypes of WSNs, that can be formaly 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 mainly worked on the improvement of the ***Glonemo*** simulator (http://www-verimag.imag.fr/~samper/Glonemo/) which allows simulating networks of up to several hundred thousands nodes, on typical monitoring application, running models of existing communication protcols (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. In particular, we are currently working on a new protocol[1] combining the MAC and routing layers and which uses vitual sensor coordinates computations, without requiring a precise (and expensive) node location mechanism. The purpose of this work is twofold: first, to provide a detailed description of the protocol that would be suitable for implementation; second, to evaluate this protocol with respect to more classical static routing schemes from the energy comsumption point of view. Finally, we also proposed a theoretical framework to perform component-based abstractions of a WSN while preserving (over-)approximations of energy consumptions. This framework allows the verification of network lifetime lower bounds.

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

Performance evaluation of Networked systems (Verimag)

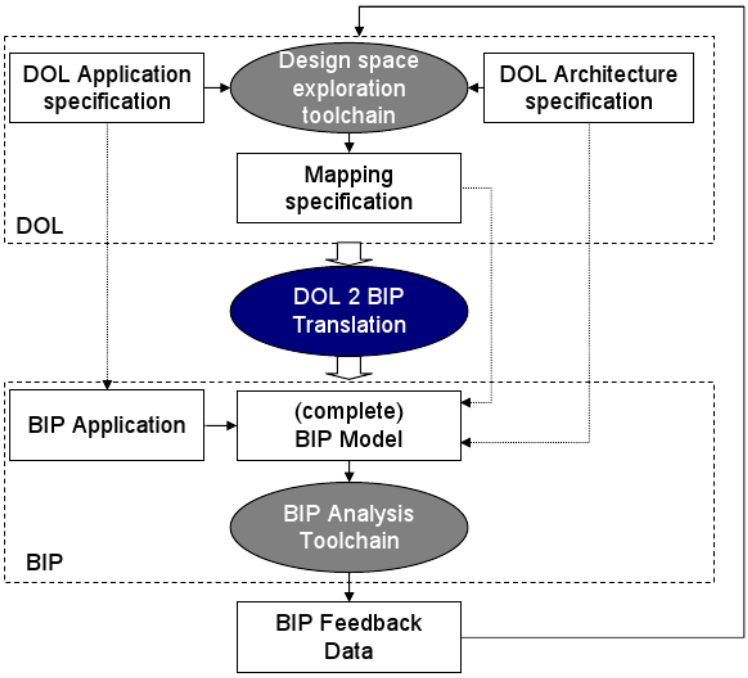
We have studied and partially carried out a translation from performance modesl as they are analysed by the analytical performance analysis tool DOL by ETHZ into BIP models.

The behavior of a DOL model is described as a transfer function transforming input streams of event and resources into output streams of events and resources. The Real-Time calculus is used to express the transfer functions of atomic components as well as the global behavior of a system. This is computed compositionally by composing the behavior of atomic components and taking into account the constraints induced by the architecture through the mapping.

We have studied a method for translating DOL models into BIP models. In contrast to DOL models, BIP models are executable. They can be used for performance analysis by simulation

[1] *On Using Virtual Coordinates for Routing in the Context of Wireless Sensor Networks, Thomas Watteyne, David Simplot-Ryl, Isabelle Augé-Blum, Mischa Dohler. 18th IEEE Int. Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07), Athens, September 2007*

or by using verification techniques. The principle of the translation currently studied combines 3 steps:



1. For each atomic DOL component an atomic BIP component is built with an equivalent executable behavior. Furthermore atomic BIP components are built for the generation of flows of events and resources with given characteristics.

2. A BIP model equivalent to the DOL model of the application software is built. This model involves all the atomic components and connectors implementing the interactions between them.

3. A global BIP model representing the DOL model is obtained from the BIP model of the application software by adding architectural constraints represented by the architecture and the mapping of the DOL model. These constraints are of two types: 1) mutual exclusion constraints between atomic components induced by their assignment to the same processor; 2) coordination constraints induced by the assignment of a set of BIP connectors to a communication device.

Reduced problem report analysis time (ESI)
In the Trader project a.o. spectrum based fault localization tools were matured to work with NXP Semiconductor's software tools. The tool is tested on various PR databases. The tool can be useful for a number of problem reports. It have been shown that certain problem reports are pinpointed in 15 to 30 minutes total time, compared to hours or days without the tooling.

Stress testing (ESI)
Code for a cycle eater implemented in released version of new TV software. A real-time CPU usage monitor was added.

Prototypes for maritime safety and security systems (ESI)
In the Poseidon project the first prototypes of maritime safety and security systems have been developed. Also feasibility studies of these prototypes were conducted.

Verification of Systems with Queues and Stacks (INRIA)

Many scientific studies analysed the FIFO channel systems, but none offered a fully satisfying solution. We proposed to tackle this problem within the abstract interpretation framework, by defining some abstract lattices adapted to this kind of systems. We considered systems with a finite alphabet of messages, then more complex systems, with an infinite alphabet of messages. This leads us to define and to study a new kind of automata: the lattice automata. Those automata are also useful for the analysis of programs with a call stack. http://www.irisa.fr/vertecs/Publis//Publi/legall08.html.

Quantitative Model-Checking of One-Clock Timed Automata (INRIA, LSV, Dresden)

In [BBB*08] (http://www.irisa.fr/vertecs/Publis//Publi/BBBBG-lics08.html), we have defined two relaxed semantics (one based on probabilities and the other one based on the topological notion of largeness) for LTL over infinite runs of timed automata which rule out unlikely sequences of events. We proved that these two semantics match in the framework of single-clock timed automata (and only in that framework), and proved that the corresponding relaxed model-checking problems are PSPACE-Complete. Moreover, we proved that the probabilistic non-Zenoness can be decided for single-clock timed automata in NLOGSPACE.

In [BBBM08] (http://www.irisa.fr/vertecs/Publis//Publi/BBBM-qest08.html), we consider the quantitative model-checking problem for omega-regular properties: we aim at computing the exact probability that a given timed automaton satisfies an omega-regular property. We develop a framework in which we can compute a closed-form expression for this probability; we furthermore give an approximation algorithm, and finally prove that we can decide the threshold problem in that framework.

Probabilistic Büchi Automata (INRIA, Dresden):
Probabilistic Büchi automata (PBA) are finite-state acceptors for infinite words where all choices are resolved by fixed distributions and where the accepted language is defined by the requirement that the measure of the accepting runs is positive. The main contribution of this paper is a complementation operator for PBA and a discussion on several algorithmic problems for PBA. All interesting problems, such as checking emptiness or equivalence for PBA or checking whether a finite transition system satisfies a PBA-specification, turn out to be undecidable. An important consequence of these results are several undecidability results for stochastic games with incomplete information, modelled by partially-observable Markov decision processes and omega-regular winning objectives. Furthermore, an alternative semantics for PBA is discussed where it is required that almost all runs for an accepted word are accepting, which turns out to be less powerful, but has a decidable emptiness problem. http://www.irisa.fr/vertecs/Publis//Publi/BBG-fossacs08.html.

Diagnosis and predictability (INRIA with Univ. Michigan)
We studied the problem of predicting the occurrences of a pattern in a partially-observed discrete-event system. The system is modeled by a labeled transition system. The pattern is a set of event sequences modeled by a finite-state automaton. The occurrences of the pattern are predictable if it is possible to infer about any occurrence of the pattern before the pattern is completely executed by the system. An off-line algorithm to verify the property of predictability is presented. The verification is polynomial in the number of states of the system. An on-line algorithm to track the execution of the pattern during the operation of the system is also presented. This algorithm is based on the use of a diagnoser automaton. http://www.irisa.fr/vertecs/Publis//Publi/ifac2008.html.

Diagnosis 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. We establish that the diagnosability problem is decidable for arbitrary sub-classes of higher-order visibly pushdown systems provided unobservable events leave the stacks unchanged. For this case, we present an effective algorithm. Otherwise, we show that diagnosability becomes undecidable already for first-order visibly pushdown automata. Furthermore, we establish that the bounded-latency problem for higher-order pushdown systems is as hard as deciding finiteness of a higher-order pushdown language. This is in contrast with the case of finite-state systems where the problem reduces to diagnosability.
http://www.irisa.fr/centredoc/publis/PI/2008/diagnosis-of-pushdown-systems

Mixing diagnosis and control synthesis for infomation flow security (Inria):
We have been interested in constructing monitors for the detection of confidential information flow in the context of partially observable discrete event systems. We focus on the case where a secret information is given as a regular language. We first characterized the set of observations allowing an attacker to infer the secret behaviors. We considered the general case where the attacker and the administrator have different partial views of the system. Further, 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 a construction of a monitor ensuring this task.

Given a finite transition system and a regular predicate, we also addressed the problem of computing a controller enforcing the opacity of the predicate against an attacker (that partially observes the system), supposedly trying to push the system to reveal the predicate. Assuming that the controller can only control a subset of the events it observes (possibly different from the ones of the attacker), we showed that an optimal control always exists and provide sufficient conditions under which it is regular and effectively computable. These conditions rely on the inclusion relationships between the observable alphabets of the attacker and the controller and the controllable alphabet.
http://www.irisa.fr/vertecs/Publis//Publi/opacity2.html

Modular control synthesis (Inria):
In this work sufficient conditions for modular (supervisory) control synthesis are presented which equal global control synthesis. In modular control synthesis a supervisory control is synthesized for each module separately and the supervisory control consists of the parallel composition of the modular supervisory controls. The general case of the specification that is indecomposable and not necessarily contained in the plant language, which is often the case in practice, is considered. The usual assumption that all shared events are controllable is relaxed by introducing two new structural conditions relying on the global mutual controllability condition. The novel concept used as a sufficient structural condition is strong global mutual controllability. The main result uses a weaker condition called global mutual controllability together with local consistency of the specification. An example illustrates the approach.
http://www.irisa.fr/vertecs/Publis//Publi/komenda-automatica.html

Integration of verification and testing (Inria)
A methodology integrating verification and conformance testing for the formal validation of reactive systems has been proposed. A specification of a system - an extended input-output automaton, which may be infinite-state - and a set of safety properties (â€œnothing bad ever happensâ€□) and possibility properties (â€œsomething good may happenâ€□) are assumed. The properties are first tentatively verified on the specification using automatic techniques based on approximated state-space exploration, which are sound, but, as a price to pay for automation, are not complete for the given class of properties. Because of this incompleteness and of state-space explosion, the verification may not succeed in proving or disproving the properties. However, even if verification did not succeed, the testing phase can proceed and provide useful information about the implementation. Test cases are automatically and symbolically generated from the specification and the properties, and are executed on a black-box implementation of the system. The test execution may detect violations of conformance between implementation and specification; in addition, it may detect violation/satisfaction of the properties by the implementation and by the specification. In this sense, testing completes verification. http://www.irisa.fr/vertecs/Publis//Publi/book-chap-react-systems.html.

STG symbolic test generation tool (Inria):
The tool has been improved and a new version can be downloaded from Inria Gforge: https://gforge.inria.fr/plugins/scmsvn/viewcvs.php/?root=bjeannet.

Biomedical Sensor Network (Uppsala)
As a case study in validation, the Uppsala team has studied Biomedical Sensor Network (BSN)[TXY08]. A UPPAAL model has been developed for BSN networks where the sensor nodes communicate using the Chipcon CC2420 transceiver (developed by Texas Instruments) according to the IEEE 802.15.4 standard. UPPAAL has been used to validate and tune the temporal configuration parameters of a BSN in order to meet desired QoS requirements on network connectivity, packet delivery ratio and end-to-end delay. Our experiments show that even though the main feature of the tool is model checking, it is also a promising and competitive tool for efficient simulation and parameter tuning. The simulator scales well; it can easily handle up to 50 nodes in our experiments. The model checker installed on a notebook can also deal with networks with 5 up to 16 nodes within minutes depending on the properties checked; these are BSNs of reasonable size for medical applications.

Timed Automata and Real-Time Calculus (Uppsala and ETH, Zurich)
Cyclic dependencies in component-based real-time systems, have not been well-understood in the context of modular performance analysis. In a joint work [JPTY08] with ETH, Zurich, Uppsala has developed a general operational semantics underlying the Real-Time Calculus, and use this to show that the behavior of systems with cyclic dependencies can be analyzed by fixpoint iterations. The work also characterizes conditions under which such iterations give safe results, and also show how precise the results can be.

Along the same line of work on compositional analysis, Uppsala has developed a prototype tool, CATS for compositional timing and performance analysis of real-time systems modeled using timed automata and the real-time calculus. It is based on an (over-) approximation technique in which a timed automaton is abstracted as a transducer of streams described by arrival curves from network calculus. As the main feature, the tool can be used to check the schedulability of a system and to estimate the best and worst case response times of its computation tasks. The tool is available for evaluation at www.timestool.com/cats.

Multiprocessor Scheduling (Uppsala)
To extend the TIMES tool to handle multi-processor scheduling and analysis, Uppsala has studied multiprocessor scheduling in different settings. In a recent work [GYGY08], new test conditions for schedulability checking of real-time tasks on multiprocessor platforms have been established. Simulation experiments demonstrate that the test conditions improve significantly existing test bounds for global non-preemptive multiprocessor scheduling.

Techniques for high-level compositional safety and reliability analysis of (automotive) embedded systems. (KTH)
Safety is a systems property that needs to considered throughout the life-cycle of a product. During the system development, safety is classically approach by techniques such as hazard and risk analysis, functional failure analysis, failure modes effects analysis, event tree analysis and so on. It should be noted that safety can and should be addressed at different levels of abstraction and using both top-down and bottom up techniques. A key problem is that safety analysis is still typically carried out isolated from the system design models. In the ATESST and ATESST2 projects, error modelling inspired by so called interface FMEA and error modelling in the AADL standard, has been incorporated into the EAST-ADL embedded systems modeling language. The error modelling enables the failure modes and causes for each component (at different levels of abstraction) to be expressed. Applying earlier results from the EU SETTA project we have shown that these error models can be composed into system fault-trees, which can be used for system analysis. In further work, tool capabilities to support this will be developed. We have also shown that the approach, in the way it is integrating systems modelling, requirements and safety analysis, provides a sound basis for expressing a safety case and meeting the requirements expressed by safety standards (ISO26262 in the automotive industry), see Chen et al (2008) and Törner et al (2008).

Towards methods and tools to support the validation of dynamically (self-) configurable systems (KTH)
In introducing self-configuration into embedded systems in order to meet flexibility requirements, there are strong needs to provide supporting methods whereby the system correctness and robustness in the presence of faults can be assessed. As part of the DySCAS project (www.dyscas.org), a model-driven design methodology is promoted and being developed, where the system architecture is described at a functional level using UML models. These system models form the basis for evaluation by simulation, different types of formal analysis and safety analysis. Currently the components of our preliminary methodology have been investigated and assessed in case studies. We have applied simulation, design time static analysis, model checking and safety analysis to the developed middleware. In particular the combination of the methods, and the application of traditional safety analysis to these kinds of systems was found rewarding during the development of the middleware. Further work is needed along several lines, including investigating how the different techniques best can be combined, and in addressing high-level as well as more detailed analysis on concrete instances of the middleware. Feng et al (2008-CDC), Feng et al (2008).

Logical reliability validation (Salzburg)
Salzburg in collaboration with the Technical University of Timisoara, Cadence, UC Berkeley, and EPFL proposed the notion of logical reliability for real-time program tasks that interact through periodically updated program variables. We described a reliability analysis that checks if the given short-term (e.g., single-period) reliability of a program variable update in an implementation is sufi¬□cient to meet the logical reliability requirement (of the program variable) in the long run. We then presented a notion of design by reï¬□nement where a task can be refined by another task that writes to program variables with less logical reliability. The resulting analysis can be combined with an incremental schedulability analysis for interacting real-time tasks proposed earlier for the Hierarchical Timing Language (HTL), a coordination

language for distributed real-time systems. We implemented a logical-reliability-enhanced prototype of the compiler and runtime infrastructure for HTL.

Dominance Analysis (OFFIS)
OFFIS has developed a Dominance Analysis for HRC (heterogenous rich component) models. Starting point for this analysis is a hierarchical component where safety specifications both for the component and its sub-components are given. These specifications have an assumption/promise format, of which each are built up from temporal-logic patterns. The developed dominance analysis checks by means of model-checking technology for a component's safety requirement, whether it is dominated by the contracts of its sub-components, where dominance is a specific form fo implication. A successful check thus reduces the safety requirement of the hierarchical component to those of its sub-components.

Failure Propagation Analysis (OFFIS)
The Failure Propagation Analysis developed by OFFIS computes failure dependencies based on contracts using failure propagation patterns. These failure propagagtion patterns permit to define exactly how one or more failures can cause another failure of a component. The developed Failure Propagation Analysis is performed by an existing fault tree computation algorithm using model-checker technologies. It takes an HRC component as input and computes, based on the failure propagation contracts of its sub-components, for each component failure which failures combinations are necessary to cause this one.

2.2 Individual Publications Resulting from these Achievements

CISS

[LR08] Kim Guldstrand Larsen, Jacob Illum Rasmussen: Optimal reachability for multi-priced timed automata. Theor. Comput. Sci. 390(2-3): 197-213 (2008)

[KHL08] Sebastian Kupferschmid, Jörg Hoffmann, Kim Guldstrand Larsen: Fast Directed Model Checking Via Russian Doll Abstraction. TACAS 2008: 203-217.

[HLM+08] Anders Hessel, Kim Guldstrand Larsen, Marius Mikucionis, Brian Nielsen, Paul Pettersson, Arne Skou: Testing Real-Time Systems Using UPPAAL. Formal Methods and Testing 2008: 77-117.

[AHL+08] Adam Antonik, Michael Huth, Kim Guldstrand Larsen, Ulrik Nyman, Andrzej Wasowski: Complexity of Decision Problems for Mixed and Modal Specifications. FoSSaCS 2008: 112-126.

[DLLN08] Alexandre David, Kim Guldstrand Larsen, Shuhao Li, Brian Nielsen: A Game-Theoretic Approach to Real-Time System Testing. DATE 2008: 486-491.

[AHL+08] Adam Antonik, Michael Huth,Kim G. Larsen, Ulrik Nyman, Andrzej Wasowski.: 20 Years of Modal and Mixed Specifications. In Concurrency Column of Bulletin of EATCS no 95, 2008.

[KRS07] John Knudsen, Anders P. Ravn, Arne Skou: Design Verification Patterns. Formal Methods and Hybrid Real-Time Systems 2007: 399-413.

[CLS+07] Zhenbang Chen, Zhiming Liu, Volker Stolz, Lu Yang, Anders P. Ravn: A Refinement Driven Component-Based Design. ICECCS 2007: 277-289.

[BKO+08] Thomas Bøgholm, Henrik Kragh-Hansen, Petur Olsen, Bent Thomsen, Kim G. Larsen: Model-Based Schedulability Analysis of Safety Critical Hard Real-Time Java

Programs. JTRES 2008: Proceedings of the 6th International Workshop on Java Technologies for Real-Time and Embedded Systems, p. 106—114, 2008.

[N08] Ulrik Nyman: Modal Transition Systems as the basis for Interface Theories and Product Lines. PhD Thesis, Aalborg University, 2008.

[TS08] Claus Thrane, Uffe Sørense. Slicing for UPPAAL. 2008 Annual IEEE Conference. Aalborg, Denmark, 2008. Best Student Paper Award.

[Srb08]] Jirí Srba: Comparing the Expressiveness of Timed Automata and Timed Extensions of Petri Nets. FORMATS 2008: 15-32.

[JS08] Petr Jancar, Jirí Srba: Undecidability of bisimilarity by defender's forcing. J. ACM 55(1): (2008).

EPFL

[CHP08] Krishnendu Chatterjee, Thomas A. Henzinger, and Vinayak Prabhu. Timed parity games: Complexity and robustness. Proceedings of the Sixth International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS), Lecture Notes in Computer Science 5215, Springer, 2008, pp. 124-140.

[BHT08] Dirk Beyer, Thomas A. Henzinger, and Gregory Theoduloz. Program analysis with dynamic change of precision. Proceedings of the 23rd International Conference on Automated Software Engineering (ASE), ACM Press, 2008, pp. 29-38.

[CHJ08] Krishnendu Chatterjee, Thomas A. Henzinger, and Barbara Jobstmann. Environment assumptions for synthesis. Proceedings of the 19th International Conference on Concurrency Theory (CONCUR), Lecture Notes in Computer Science 5201, Springer, 2008, pp. 147-161.

[GHS08] Rachid Guerraoui, Thomas A. Henzinger, and Vasu Singh. Completeness and nondeterminism in model checking transactional memories. Proceedings of the 19th International Conference on Concurrency Theory (CONCUR),Lecture Notes in Computer Science 5201, Springer, 2008, pp. 21-35.

[GHJS08] Rachid Guerraoui, Thomas A. Henzinger, Barbara Jobstmann, and Vasu Singh.Model checking transactional memories. Proceedings of the International Conference on Programming Language Design and Implementation (PLDI), ACM Press, 2008, pp. 372-382.

[CMH08] Krishnendu Chatterjee, Rupak Majumdar, and Thomas A. Henzinger. Controller synthesis with budget constraints. Proceedings of the 11th International Workshop on Hybrid Systems: Computation and Control (HSCC), Lecture Notes in Computer Science 4981, Springer, 2008, pp. 72-86.

[CSH08] Krishnendu Chatterjee, Koushik Sen, and Thomas A. Henzinger. Model checking omega-regular properties of interval Markov chains. Proceedings of the 11th International Conference on Foundations of Software Science and Computational Structures (FOSSACS), Lecture Notes in Computer Science 4962, Springer, 2008, pp. 302-317.

[GHM+08] Ashutosh Gupta, Thomas A. Henzinger, Rupak Majumdar, Andrey Rybalchenko,and Ru-Gang Xu. Proving non-termination. Proceedings of the 35th Annual Symposium on Principles of Programming Languages (POPL), ACM Press, 2008, pp. 147-158.

[CH08] Krishnendu Chatterjee and Thomas A. Henzinger. Value iteration. In 25 Years of Model Checking, Lecture Notes in Computer Science 5000, Springer, 2008, pp. 107-138.

ESI

[AZG08] R. Abreu, P. Zoeteweij, A.J.C. van Gemund, An Observation-based Model for Fault Localization Proceedings of the 6th Workshop on Dynamic Analysis (WODA'08), colocated with the International Symposium on Software Testing and Analysis (ISSTA'08): 64-70. 2008

[AGZ08a] R. Abreu, A. González, P. Zoeteweij, and A.J.C. van Gemund, Automatic Software Fault Localization using Generic Program Invariants, Proceedings of the 23rd Annual ACM Symposium on Applied Computing (SAC'08) - Software Engineering Track, 712--717. 2008

[AGZ08b] R. Abreu, A. González, P. Zoeteweij, and A.J.C. van Gemund, On the Performance of Fault Screeners in Software Development and Deployment, Proceedings of the 3rd International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE'08): 123--130. 2008

[Bra08] N.C.W.M. Braspenning, Model-based Integration and Testing of High-tech Multi-disciplinary Systems, PhD thesis Eindhoven University of Technology. 2008

[BH08] E. Brinksma and J. Hooman, “Dependability for high-tech systems: an industry-as-laboratory approach”, Proceedings Design, Automation & Test in Europe (DATE'08), European Design and Automation Association (EDAA), 1226-1231. 2008

[BM08a] C. Boogerd, L. Moonen, On the Use of Data Flow Analysis in Static Profiling, Proceedings of the 8th IEEE International Working Conference on Source Code Analysis and Manipulation (SCAM). 2008

[BM08b] C. Boogerd, L. Moonen, Assessing the Value of Coding Standards: An Empirical Study, Proceedings of the 24th IEEE International Conference on Software Maintenance (ICSM). 2008

[Bru08] M. Bruntink, Renovation of Idiomatic Crosscutting Concerns in Embedded Systems, PhD Thesis Delft University of Technology. 2008

[Dur08] P. Durr, Resource-based Verification for Robust Composition of Aspects, PhD thesis University of Twente. 2008

[DBA08] P. Durr, L. Bergmans, M. Aksit, A Controlled Experiment for the Assessment of Aspects - Tracing in an Industrial Context, Technical Report TR-CTIT-08-04 Centre for Telematics and Information Technology, University of Twente, Enschede. ISSN 1381-3625. 2008

[HH08] J. Hooman and T. Hendriks, "Model-Based Run-Time Error Detection", Models in Software Engineering, Workshops and Symposia at MoDELS 2007, Lecture Notes in Computer Science (LNCS), Vol. 5002, pp. 225-236, Springer. 2008

[HKO08] J. Hooman, H. Kugler, I. Ober, A. Votintseva, and Y.Yushtein “Supporting UML-based Development of Embedded Systems by Formal Techniques”, Software and Systems Modeling, 7(2): 131-155. 2008

[Jon08] I.S.M. de Jong, Integration and test strategies for complex manufacturing systems, PhD thesis Eindhoven University of Technology. 2008

[Tre08] J. Tretmans, Model Based Testing with Labelled Transition Systems, Formal Methods and Testing, volume 4949 of Lecture Notes in Computer Science, pages 1-38. Springer-Verlag. 2008

[VHK08] Vanya, L. Hofland, S. Klusener, P. van de Laar, H. van Vliet, Assessing Software Archives with Evolutionary Clusters, IEEE International Conference on Program Comprehension. 2008

[ZPA08a] P. Zoeteweij, J. Pietersma, R. Abreu, A. Feldman, and A.J.C. van Gemund, Automated Fault Diagnosis in Embedded Systems, Proceedings of the 2nd IEEE International Conference on Secure Systems and Reliability Improvement (SSIRI'08). 2008

[ZPA08b] P. Zoeteweij, J. Pietersma, R. Abreu, A. Feldman, and A.J.C. van Gemund, Automated Fault Diagnosis in Embedded Systems, Proceedings of the 2nd IEEE International Conference on Secure Systems and Reliability Improvement (SSIRI'08). 2008.

KTH

[FCT08] Feng, L., Chen DJ, and M. Törngren (2008 – CDC). Self configuration of dependent tasks for dynamically reconfigurable automotive embedded systems. In Proceedings of the 47th IEEE Conference on Decision and Control, Cancún, Mexico, 2008

[FCT08b] Feng L, Chen DJ, Törngren M. (2008). Safety, robustness and formal analysis of dynamically configurable embedded systems. Technical report, Department of Machine Design, KTH, Stockholm, Sweden, 2008.

INRIA

[KSGM08] J. Komenda, J. van Schuppen, B. Gaudin, H. Marchand, Supervisory Control of Modular Systems with Global Specification Languages, Automatica, 44:1127-1134, 2008.

[CJMR08] C. Constant, T. JÃ©ron, H. Marchand, V. Rusu, Validation of Reactive Systems, in Modeling and Verification of Real-TIME Systems - Formalisms and software Tools, S. Merz, N. Navet (eds.), Chapter 2, Pages 51-76, HermÃ¨s Science, January 2008.

[DDM08] J. Dubreil, Ph. Darondeau, H. Marchand, Opacity Enforcing Control Synthesis, in Workshop on Discrete Event Systems, WODES'08, Gothenburg, Sweden, March 2008.

[J08] Thierry JÃ©ron, Symbolic model-based test selection, in Proceedings of the Brazilian Symposium on Formal Methods (SBMF 2008), Salvador, Bahia, Brazil, P. Machado, A. Andrade, A. Duran (eds.), Pages 17-32, 2008. Revised lecture to appear in ENTCS.

[JMGL08] T. JÃ©ron, H. Marchand, S. Genc, S. Lafortune, Predictability of Sequence Patterns in Discrete Event Systems, in IFAC World Congress, Seoul, Korea, July 2008.

[DJM08] J. Dubreil, T. JÃ©ron, H. Marchand, Monitoring Information flow by Diagnosis Techniques, Research Report IRISA, No 1901, August 2008.

[LG08] T. Le Gall, Abstract Lattices for the Verification of Systems with Queues and Stacks, PhD Thesis UniversitÃ© de Rennes 1, July 2008.

[C08] C. Constant, GÃ©nÃ©ration automatique de tests pour modÃ¨les avec variables ou rÃ©cursivitÃ©, PhD Thesis UniversitÃ© de Rennes 1, November 2008.

[MP08] C. Morvan, S. Pinchinat Diagnosis of Pushdown Systems, Research Report IRISA, No 1904, October 2008.

OFFIS

[DJMNKSV08] W Damm, B. Josko, A. Metzner, M. Di Natale, H. Kopetz, A. Sangiovanni Vincentelli. Software Components for Reliable Automotive Systems. In Proceedings Date, 2008

Salzburg

[CGIKHPSV08] K. Chatterjee, A. Ghosal, D. Iercan, C.M. Kirsch, T.A. Henzinger, C. Pinello, and A.L. Sangiovanni-Vincentelli. Logical Reliability of Interacting Real-Time Tasks. Proc. International Conference on Design, Automation and Test in Europe (DATE), 2008.

Uppsala
[TXY08] Simon Tschirner, Liang Xuedong and Wang Yi. Model-Based Validation of QoS Properties of Biomedical Sensor Networks. Regular paper accepted by the 8th International Conference on Embedded Software, Atlanta, USA, 2008.

Verimag
[BGL*08] Ananda Basu, Matthieu Gallien, Charles Lesire, Thanh-Hung Nguyen, Saddek Bensalem, Felix Ingrand and Joseph Sifakis. Incremental Component-Based Construction and Verification of a Robotic System. *International Workshop on Current Software frameworks in Cognitive Robotics integrating different computational paradigms, Sept. 22nd 2008, Nice, France.*

[BBG*08] Saddek. Bensalem, Marius. Bozga, Matthieu. Gallien, Felix. Ingrand, Moez. Krichen and Stavros Tripakis. Automatic Generation of Observers for the Dala Robot with TTG. *In the International Conference CISA 2008, Annaba, Algeria*.

[BBSN08] Saddek Bensalem, Marius Bozga, Joseph Sifakis, Thanh-Hung Nguyen. Compositional Verification for Component-based Systems and Application. *6th International Symposium on Automated Technology for Verification and Analysis, October 20-23, 2008, Seoul, South Korea*

[BKT08a] Saddek Bensalem, Moez Krichen and Stavros Tripakis. Generating Analog-Clock Real-Time Testers Using Action Refinement Techniques. In the International Conference ROGICS 2008, Mahdia, Tunisia.

[BKTb08] Saddek Bensalem, Moez Krichen and Stavros Tripakis. State Identification Problems for Input/Output Transition Systems. In WODES'08, the 9th international Workshop on Discrete Event Systems, May 28-30, 2008, Goteborg, Sweden.

[BPT08] Saddek Bensalem, Doron Peled, Hongyang Qu and Stavros Tripakis. Automatic Generation of Path Conditions for Concurrent Timed Systems. In Theoritical Computer Science, Volume 404, number 3, September 2008.

[BGMO08] Marius Bozga, Susanne Graf, Laurent Mounier, Iulian Ober. Real Time Systems 1: Modeling and verification techniques. Hermes, Lavoisier 2008

[BFG+08] V. Braberman, F. Fernandez, D. Garbervetsky, S. Yovine. Parametric Prediction of Heap Memory Requirements. ISMM'08, June 7-8, 2008, Tucson, Arizona, USA. ACM 2008.

[DM08] A. Degorre, O. Maler, On Scheduling Policies for Streams of Structured Jobs, FORMATS'08, 2008

[Fre08] Goran Frehse. A Counter Example Guided Approach to Parameter Synthesis for Linear Hybrid Automata. In HSCC'08, 2008

[GP08] Manuel Garnacho and Michaël Périn, Convincing proofs for program certification, in Certification of Safety-Critical Software Controlled Systems (SafeCert'08), electronically published in Electronic Notes in Theoretical Computer Science.

[HIV08a] P. Habermehl, R. Iosif and T. Vojnar. What else is decidable about integer arrays? In Proc. FoSSaCS 2008, LNCS, pp. 474-489

[HIV08b] P. Habermehl, R. Iosif and T. Vojnar. A Logic of Singly Indexed Arrays. In Proc. LPAR 2008

[MPN+08] O. Maler, A. Pnueli, D. Nickovic, Checking Temporal Properties of Discrete, Timed and Continuous Behaviors, Pillars of Computer Science, Springer, 2008.

[NV08] Iman Narasamdya and Andrei Voronkov, Proving Inter-Program Properties in Translation Validation, in the 7th International Workshop on Compiler Optimization Meets Compiler Verification (COCV'08), electronically published in Electronic Notes in Theoretical Computer Science.

[OGYO08] Iulian Ober, Susanne Graf, Yuri Yushtein, Ileana Ober. Timing analysis and validation with UML: the case of the embedded MARS bus manager. In *Innovations in Systems and Software Engineering* vol. () 2008

[QG08a] Sophie Quinton, Susanne Graf. Contract-Based Verification of Hierarchical Systems of Components. In 6th IEEE Int. Conferences on Software Engineering and Formal Methods, SEFM08, Cape Town, South Africa, november 2008 vol. IEEE Computer Society Press 2008

[QG08b] Sophie Quinton, Susanne Graf. A Framework for Contract-Based Reasoning: Motivation and Application. In *Second Workshop on Formal Languages and Analysis of Contract-Oriented Software, FLACOS, Malta, November 2008*

CVF

Pierre Ganty, Gilles Geeraerts, Jean-François Raskin, Laurent Van Begin. Méthodes algorithmiques pour l'analyse des réseaux de Petri. To appear in Journal Techniques et sciences informatiques. 2009.

M. De Wulf, L. Doyen, N. Markey, and J.F. Raskin. Robust Safety of Timed Automata. To appear in Formal Methods in System Design, 2008. Martin De Wulf, Laurent Doyen, Nicolas Maquet and Jean-François Raskin. LTL Satisfiability, Alternating Büchi Automata Emptiness, and Model-Checking with Alaska. To appear in ATVA'08. 6 pages. 2008.

Jean-François Raskin and Frédéric Servais. Visibly Pushdown Transducers. In ICALP'08. 386-397. 2008.

Pierre Ganty, Jean-François Raskin, Laurent Van Begin. From Many Places to Few: Automatic Abstraction Refinement for Petri Nets. Invited extended version. To appear in Journal of Fundamenta Informaticae. 28 pages. 2008.

Laurent Doyen, Tom Henzinger, Jean-François Raskin. An equivalence relation for Markov Chains. Invited paper. In International Journal of Foundations of Computer Science,19(3):549-563, 2008.

Martin De Wulf, Laurent Doyen, Nicolas Maquet and Jean-François Raskin. Antichains: Alternative Algorithms for LTL Satisfiability and Model-Checking. In TACAS'08, LNCS, Springer, 63-77, 2008.

Véronique Bruyère, Emmanuel Dal'ollio, and Jean-François Raskin. Durations and Parametric Model-Checking in Timed Automata. In Transactions on Computational Logic,9(2):1-23, ACM press, 2008.

LSV

[BMR08] P. Bouyer, N. Markey and P.-A. Reynier. Robust Analysis of Timed Automata via Channel Machines. Proceedings of FoSSaCS: Foundations of Software Science and Computation Structures, LNCS 4962, Springer, pp.157-171.

[CDF+08] N. Chamseddine, M. Duflot, L. Fribourg, C. Picaronny and J. Sproston. Computing Expected Absorption Times for Parametric Determinate Probabilistic Timed Automata. Proceedings of QEST: Quantitative Evaluation of Systems, IEEE, 2008, pp.254-263.

RWTH
[BKKL08] B. Bollig, J.-P. Katoen, C. Kern, M. Leucker. Smyle: A Tool for Synthesizing Distributed Models from Scenarios by Learning. CONCUR 2008, LNCS 5201, 162-166. 2008

[KKLW08] J.-P. Katoen, D. Klink, M. Leucker, V. Wolf. Abstraction for Stochastic Systems by Erlang's Method of Stages. CONCUR 2008, LNCS 5201, 279-294. 2008

[K08a] J.-P. Katoen. Quantitative Evaluation in Embedded System Design: Trends in Modeling and Analysis Techniques. DATE 2008: 86-87

[KM08] J.-P. Katoen, A. Mereacre: Model Checking HML on Piecewise-Constant Inhomogeneous Markov Chains. FORMATS 2008, LNCS 5215, 203-217. 2008

[HKM08] T. Han, J.-P. Katoen, A. Mereacre: Compositional Modeling and Minimization of Time-Inhomogeneous Markov Chains. HSCC 2008, LNCS 4981, 244-258. 2008

[SFK08] M. Swaminathan, M. Frnzle, J.-P. Katoen: The Surprising Robustness of (Closed) Timed Automata against Clock-Drift. IFIP TCS 2008: 537-553. 2008

[CHK08] T. Chen, T. Han, J.-P. Katoen: Time-Abstracting Bisimulation for Probabilistic Timed Automata. TASE 2008: 177-184. 2008

[K08b] J.-P. Katoen: Perspectives in Probabilistic Verification. TASE 2008: 3-10. 2008.

2.3 Interaction and Building Excellence between Partners

In 2008 de EU FP7 strep "Quasimodo" (Quantitative System Properties in Model-Driven-Design of Embedded Systems) started, which was initiated by the ARTIST DESIGN cluster "Testing and Verification" partners:

- Centre for Embedded Software Systems, Department of Computer Science at Aalborg University, Denmark. Contact: Associate Prof. Brian Nielsen
- Embedded Systems Institute, The Netherlands. Contact: Director, Professor Ed Brinksma. In collaboration with the Informatics for Technical Application Group, Radboud University Nijmegen, Contact: Professor Frits Vaandrager, and the Formal Methods and Tools Group, University of Twente, Contact: Prof. Jaco van de Pol
- Laboratoire Spécification et Vérification at CNRS & ENS, France. Contact: Associate Professor François Laroussinie
- Centre Fédéré en Vérification at Université Libre de Bruxelles, Belgium. Contact: Associate Professor Jean-Francois Raskin

Partner IRISA organised the summerschool EJCP (Ecole Jeunes Chercheurs en Programmation - from 29 May to 6 June 2008) where Jan Tretmans (Embedded Systems Institute) was lecturing on "Software Testing". Jan Tretmans also gave an invited talk at the TESTNET conference in Aalborg on 30.10.2008.

Kim Larsen was awarded Doctor Honoris Causa at ENS Cachan acknowledging his regular collaboration with LSV. Kim Larsen also spent a month as an invited professor at LSV.

From Aalbrog to CFV (Brussels): one week visit of Prof. Kim Larsen to the team of Prof. JF Raskin.

From ENS Cachan to Aalborg: one week visit of Patricia Bouyer and Nicolas Markey.

Ghassan Oreiby wil after his position as PhD student at LSV go to Aalborg University for a post doc position starting November 1, 2008.

Saltzburg and EPFL has working jointly in defining a fully compositional semantics of HTL and the notion of logical reliability.

PARADES and Salzburg has workied jointly in defining the notion of logical reliability.

EPFL + CFV collaborated on efficient algorithms for classical decision problems in automata theory (emptiness, language inclusion, universality), with application to the model-checking of linear time properties.

EPFL + LSV collaborated on games with imperfect information. We work on building a tool to solve such games, with parity objectives.

From INRIA to LSV and CVF (Mons): one week visit of Nathalie Bertrand in each place on probabilistic semantics for timed automata.

From CFV (Brussels) to Inria Rennes: two month visit of Gabriel Kalyon and one month visit of Thierry Massart.

From INRIA to CFV (Brussels) one week visit of T. Legall to ULB followed by post-doc started in September 2008.

From ESI to Inria Rennes: one week visit of Jan Tretmans to Inria for participation to the summer school EJCP.

Uppsala has collaborated with ETH in Zurich on modular performance analysis. Jointly, we have established a fixed point theorem on the existence of fixed points for component networks containing feedback cycles. Uppsala has also initiated collaboration with North Eastern University in China, on multiprocessor scheduling.

The SPEEDS project lead to an important collaboration between INRIA, OFFIS, PARADES and VERIMAG on the definition of the SPEEDS metamodel HRC [BCSM07] which is the basis of an important analysis platform (platform 1). 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.

Interaction between RWTH and Saarland University on design notations and model checking

Iinteraction between CISS and RWTHon quantitative versions of priced timed automata

From Aalbrog to CFV (Brussels): one week visit of Prof. Kim Larsen to the team of Prof. JF Raskin.

From CFV (Brussels) to EPFL (Henzinger): Dr. Laurent Doyen formerly in CFV is post-doct at EPFL.

From CFV (Brussels) to EPFL (Henzinger): several visits during 2007-2008 by Prof. JF Raskin.

From EPFL (Henzinger) to CFV (Brussels): several visits during 2007-2008 by Dr. L Doyen.

2.4 Joint Publications Resulting from these Achievements

[BBL08] P. Bouyer, E. Brinksma, K.G. Larsen, Optimal infinite scheduling for multi-priced timed automata. Formal Methods in System Design 32(1), 3-23. 2008 (CISS, ESI, LSV)

[BCD+08] Dietmar Berwanger, Krishnendu Chatterjee, Laurent Doyen, Thomas A. Henzinger, and Sangram Raje. Strategy construction for parity games with imperfect information. Proceedings of the 19th International Conference on Concurrency Theory (CONCUR), Lecture Notes in Computer Science 5201, Springer, 2008, pp. 325-339. (EPFL + LSV)

[BD08] Dietmar Berwanger and Laurent Doyen. On the power of imperfect information. Proceedings of the 26th International Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS), Lecture Notes in Computer Science, Springer, 2008. (EPFL + LSV)

[DDMR08a] Martin De Wulf, Laurent Doyen, Nicolas Maquet, and Jean-Francois Raskin. Antichains: alternative algorithms for LTL satisfiability and model-checking. Proceedings of the 14th International Conference on Tools and Algorithms for ´the Construction and Analysis of Systems (TACAS), Lecture Notes in Computer Science 4963, Springer, 2008, pp. 63-77. (EPFL + CFV)

[DDMR08b] Martin De Wulf, Laurent Doyen, Nicolas Maquet, and Jean-Francois Raskin. Alaska: antichains for logic, automata and symbolic Kripke structures analysis. Proceedings of the 6th International Symposium on Automated Technology for Verification and Analysis (ATVA), Lecture Notes in Computer Science 5311, Springer, 2008, pp.240-245. (EPFL + CFV)

[DHR08] Laurent Doyen, Thomas A. Henzinger, and Jean-Francois Raskin. Equivalence of labeled Markov chains. International Journal of Foundations of Computer Science 19:549-563, 2008. (EPFL + CFV)

[JSGB08] B. Jobstmann and S. Staber and A. Griesmayer and R. Bloem. Finding and Fixing Faults. Journal of Computer and System Sciences (JCSS), 2008. (EPFL + TU Graz)

[BBB*08] Christel Baier, Nathalie Bertrand, Patricia Bouyer, Thomas Brihaye, Marcus Groesser, Almost-Sure Model Checking of Infinite Paths in One-Clock Timed Automata, in Proceedings of the 23rd Annual IEEE Symposium on Logic in Computer Science (LICS'08), Pittsburgh, PA, USA, June 2008 (IRISA, Inria, LSV and Dresden)

[BBG08] Christel Baier, Nathalie Bertrand, Marcus Groesser, On Decision Problems for Probabilistic BÃ¼chi Automata, in Proceedings of the 11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'08), Budapest, Hungary, March 2008 (IRISA, Inria and Dresden)

[BBBM08] N. Bertrand, P. Bouyer, Th. Brihaye, N. Markey, Quantitative Model-Checking of One-Clock Timed Automata under Probabilistic Semantics, in Proceedings of the 5th International Conference on the Quantitative Evaluation of SysTems (QEST'08), Saint Malo, France, September 2008 (IRISA, INRIA, LSV)

[GYGY08] Nan Guan, Wang Yi, Zonghua Gu and Ge Yu. New Schedulability Test Conditions for Non-Preemptive Scheduling on Multiprocessor Platforms. Accepted by the 29th IEEE Real-Time Systems Symposium, Barcelona (Uppsala + MCI Denmark)

[JPTY08] Bengt Jonsson, Simon Perathoner, Lothar Thiele, and Wang Yi. Cyclic dependencies in modular performance analysis. Accepted by the 8th International Conference on Embedded Software, Atlanta, USA, 2008. (Uppsala + ETH)

[CJL08] DeJiu Chen, Rolf Johansson, Henrik Lönn, Yiannis Papadopoulos, Anders Sandberg, Fredrik Törner, Martin Törngren (2008 – Safecomp). Modelling Support for Design of Safety-Critical Automotive Embedded Systems. SAFECOMP 2008: The 27th International

Conference on Computer Safety, Reliability and Security. 22-25 September 2008, Newcastle upon Tyne, UK.

[TCJLT08]Fredrik Törner, D.J. Chen, Rolf Johansson, Henrik Lönn, Martin Törngren. Supporting an Automotive Safety Case through Systematic Model Based Development - the EAST-ADL2 Approach. SAE World Congress, 2008. SAE paper number 2008-01-0127.

[CSST08] P. Caspi, N. Scaife, Ch. Sofronis, S. Tripakis. Semantics-preserving multitask implementation of synchronous programs. *ACM Transactions on Embedded Computing Systems*, 7(2), February 2008

[CWG08] Olivier Constant, Wei Monin, Susanne Graf. A model transformation tool for performance simulation of complex UML models. ICSE Companion 2008.

[CGIKHPSV08] K. Chatterjee, A. Ghosal, D. Iercan, C.M. Kirsch, T.A. Henzinger, C. Pinello, and A.L. Sangiovanni-Vincentelli. Logical Reliability of Interacting Real-Time Tasks. Proc. International Conference on Design, Automation and Test in Europe (DATE), 2008. (Salzburg, EPFL, PARADES)

[CJLRR09] Automatic Synthesis of Robust and Optimal Controllers – An Industrial Case Study, accepted for HSCC09.

[WDMR08] Martin De Wulf, Laurent Doyen, Nicolas Maquet and Jean-François Raskin. Antichains: Alternative Algorithms for LTL Satisfiability and Model-Checking. In TACAS'08, LNCS, Springer, 63-77, 2008.

[DHR08] Laurent Doyen, Tom Henzinger, Jean-François Raskin. An equivalence relation for Markov Chains. Invited paper. In International Journal of Foundations of Computer Science,19(3):549-563, 2008.

[CDLLR07] Franck Cassez, Alexandre David, Kim Larsen, Didier Lime and Jean-François Raskin. Timed Control with Observation Based and Stuttering Invariant Strategies}. In ATVA'07, Lecture Notes in Computer Science, 4762, pp. 192--206, Springer, 2007.

2.5 Keynotes, Workshops, Tutorials

Keynote: The Quest for Correctness -- Beyond Verification
Joseph Sifakis - CAV 2008, Princeton, July 2008, http://www.princeton.edu/cav2008/

Invited Lecture: E. Brinksma, Quantitative Testing Theory, Invited lecturer, Artist Summer School in Europe, Autrans (France), 8 September 2008.

Invited Lecture: E. Brinksma, Model-based Testing for Embedded Systems, Invited lecturer, Artist Summer School in China, Shanghai (China), 14 July 2008.

Invited talk:J. Hooman, Reliability of High-Volume Products, Invited talk at Software Reliability Seminar, Holland Innovative BV, Eindhoven, 20 March 2008.

Workshop lecture: J. Hooman, Towards Checking Stateflow Models with mCRL2, IPA Spring Days on Integrating Formal Methods, Rhenen, 8 May 2008.

Workshop lecture: J. Hooman, User-Perceived Reliability of High-Volume Products, The 2nd International Joint Workshop on Embedded S/W and System Engineering Design Challenges, Center for Embedded Software Technology (CEST), Daegu, South Korea, 21 May 2008.

Keynote: "Timing and Performance Analysis: Static Analysis versus Model Checking"
Kim G. Larsen. Invited Talk on the Honoris Causa to Professor Dr. Reinhard Wilhelm from RWTH Aachen. Germany. October 24, 2008.

Keynote: "Model-driven Test and Verification of Real-Time and Embedded Systems"
Kim G. Larsen. Test Conference, Aalborg University. Denmark. October 20, 2008.

Keynote: "Verification, Performance Analysis, and Controller Synthesis for Real-Time Systems"
Kim G. Larsen, Invited talk. Marktoberdorf Summerschool. Marktoberdorf, Germany. August 5-16, 2008. http://asimod.in.tum.de/index.shtml

Keynote: "Quantitative Verification and Synthesis for Embedded Systems"
Kim G. Larsen. Invited Talk. ARTIST2 Summer School Autrans (near Grenoble), France. September 8-12, 2008. http://www.artist-embedded.org/artist/ARTIST2-Summer-School-2008.html

Keynote: "Priced Timed Automata and Games"
Kim G. Larsen. Automata and Verification Workshop University of Mons-Hainaut. Mons, Belgium. August 25, 26, 2008. http://w3.umh.ac.be/~infofs/av08/index.html

Keynote: "Modeling, Verification and Synthesis of Timed Systems"
Kim G. Larsen. Invited Talk at The Centre for Interdisciplinary Computational and Dynamical Analysis (CICADA) Launch Event. Manchester University, England. July 1, 2008.http://www.staffnet.manchester.ac.uk/news/display/?id=3721

Keynote: "Model-driven Testing of Real-Time and Embedded Systems"
Kim G. Larsen.. Invited Talk at Pan-European Conference Systematic Testing. Berlin, Germany. June 5, 2008.
http://www.eniac.eu/web/downloads/events/Events_Systematic%20Testing%202008.PDF

Keynote: "Playing Games with Timed Interfaces"
Kim G. Larsen. Invited Talk. Foundation for Interface Theory (FIT). Budapest, Hungary. April 5, 2008. *http://fit2008.cs.aau.dk/*

Keynote: "Model Checking Embedded and Real Time Systems"
Kim G. Larsen. Invited Talk. 9th International Workshop on Discrete Event Systems (WODES). Gothenburgh, Sweden. May 28-30, 2008. http://www.wodes2008.org/

Keynote: "Validation, Performance Analysis and Synthesis of Embedded Systems"
Kim G. Larsen. Invited Talk. 3rd intl Workshop on Systems Software Verification (SSV08). Sidney, Austrailia. February 25-27, 2008. http://nicta.com.au/research/projects/l4.verified/ssv08

Keynote: "Performance analysis, scheduling and synthesis of embedded systems"
Kim G. Larsen. . Invited Talk. Final Workshop of Centre for Dependable Computing (CDC). Tallinn, Estonia. January 21-22, 2008.

Keynote: "Verification, optimization and synthesis for timed systems: from theory to tools"

Kim G. Larsen.. Invited talk given at the receipt of Dr Honoris Causa from LSV, ENS Cachan. Cachan, France. November 26, 2007.

Keynote lecture "Games in System Design and Verification". Thomas A. Henzinger (EPFL) Eighth International Conference on Logic and the Foundations of Game and Decision Theory (LOFT), Amsterdam, The Netherlands, July 2008.

Keynote: T. Jeron, Symbolic model-based test selection, In Brazilian Symposium on Formal Methods (SBMF 2008), Salvador, Bahia, Brazil, August 2008. Revised lecture to appear in ENTCS.

Keynote: Joost-Pieter Katoen: Perspectives in Probabilistic Verification: Second Int. IEEE Symposium on Theoretical Aspects of Software Engineering (TASE), Nanjing, China, June 2008.

Keynote : Adding SPEEDS to AUTOSAR. Werner Damm, OFFIS - DATE 08, Automotive Session, Munich, Germany, March 12, 2008. The invited talk discussed how AUTOSAR based design processes can be enriched with the SPEEDS enabled system leven analysis methods.http://www.date-conference.com/

Tutorial Joost-Pieter Katoen: GLOBAN Summerschool, Warsaw, Poland, September 2008. Invited session on quantitative analysis of embedded systems at DATE 2008, Munich, Germany, March 2008.

Invited talk Joost-Pieter Katoen:: IEEE CDC-Workshop on Stochastic Hybrid Systems (SHS), Cancun, Mexico, December 2008.

Invited talk: Jean-Francois Raskin ``Timed automata: verification, control and optimality". Artist 2 Summer School in China. Shanghai. July 2008.

Invited talk: Jean-Francois Raskin Fixpoint-based Abstraction Refinements, LABRI, U Bordeaux, France, June 12, 2008.

Jean-Francois Raskin. Invited Talk. "An Introduction to Games Played on Graphs", University of Luxembourg, May 26, 2008.

Organization of the workshop, **Veronique Bruyere and Jean-Francois Raskin.** "Automata and Verification", University of Mons-Hainaut, Belgium, August 25-26, 2008.

Summer school: Movep 08: Co-organization of the Movep school (http://www.univ-orleans.fr/movep2008/) about modeling and verifying parallel processes in June 2008, partially funded by Artist 2.

RTSS08 track on Design and Verification of Embedded Real-Time Systems, the 29th IEEE Real-Time Systems Symposium. Barcelona, Spain. November 30 - December 3, 2008. This is one of the four tracks of RTSS 2008. The objective is to promote research on design and analysis, and verification of embedded real-time systems. It intends to cover the whole spectrum from theoretical results to concrete applications with an emphasis on practical and scalable techniques and tools providing the designers with automated support for obtaining high-quality software and hardware systems. A particular goal is to provide a forum for interaction between different research communities, such as scheduling, hardware/software co-design, and formal techniques. http://www.rtss.org

Workshop : SafeCert 2008, International Workshop on the Certification of Safety-Critical Software Controlled Systems, ETAPS 2008 Budapest, Hungary, 29 March, 2008, organized by TU Braunschweig and OFFIS. The need for certification, like for instance in the rail sector, imposes the burden of not only validating a system, but also proving in a juridical sense, that the validation can be trusted. The major question addressed in the workshop was how to embed formal methods and tools in a seamless design process which covers several development phases and which includes an efficient construction of a safety case for the product.

http://safecert08.offis.de/

Tutorial: M. Winokur, S. Graf, B. Josko. Contract Based System Design- The SPEEDS Approach INCOSE 2008, Utrecht, The Netherlands, June 2008. The aim of this half-day tutorial was to disseminate the results of the SPEEDS project towards the community of the potential users of the developed technology. The tutorial focused on the contracts based development methodology being worked-out within the project. It aimed specifically at iterative development as opposed to the traditional waterfall requirement flow down. At the centre of the methodology is the definition of a rich component model which allows the capture of functional and non functional system properties in the form of contracts.
http://www.incose.org/symp2008/

3. Milestones, and Future Evolution

3.1 Problem to be Tackled over the next 12 months (Jan 2009 – Dec 2009)

Within each sub-activity, the partners will continue to develop and ewxtend the results obtained in Year 1. We are also working on application of the tools already implemented as well as implementation of our previous results in new tool developments (either as extensions of existing tools, or new prototypes) in the next year. We see both these acitivities as vital in the continued dessimination of our results. We give below a short summary of the problems that will be addressed in Year 2:

Sub-activity A: Compositional Validation

CISS wil work on metrics for weighted (timed) automata with particular emphasis of continuity of composition operators, allowing for compositional (approximate) analysis.

Good specifications are crucial for the quality of verification and synthesis tasks. EPFL will address the problem of improving the quality of temporal specifications. Our techniques will help users to identify flaws in their specifications and help them to write specifications that meet their intentions more precisely.

OFFIS will pursue the planned extension of the scope of the HRC approach. The dominance and failure-propagation analyses will be demonstrated on examples formerly treated in other methodologies. In addition, stochastic failure analyses will be considered.

Salzburg intends to work on integrating the notion of logical reliability into the new compositional semantics of HTL. The existing work is based on the non-compositional semantics of HTL and is therefore limited in modularity and scalability.

Sub-activity B: Quantitative Validation

CISS will work on validation for and combining time, probabilities and cost. We consider extensions of timed automata with both probabilities as well as cost and consider probabilistic reachability problems involving both time and cost-bounds.

CISS will continue work on energy-bounded Infinite Runs: this line of work is based on an extension of weighted imed automata (or discrete weighted automata) where energy may both be consumed and produced. Here interest is in the existence (or universality) of behaviours where bounds (lower- as well as upper) bounds on the energy is respected. Several questions are at the moment open, and we hope to make progress during the next year.

EPFL will develop new algorithms for transient and steady-state analysis of infinite-state Markov chains that are well-structured and evolve in continuous time. These algorithms will be based on abstraction techniques and numerical solution algorithms, such as Krylov subspace methods.

EPFL are working on the problem of verifying safety of software program artifacts. We are going to explore opportunities of extending the current techniques to combine multiple analyzes in novel, flexible way.

IRISA will continue work on verification: quantitative verification and application to information flow security analysis. Partially observable stochastic games. Integration of timing constraints in modal specifications. Further work on probabilistic semantics for timed automata.

Sub-activity C: Cross-Layer Validation

CISS will extend its tool effort for on-line testing: extension of on-line testing technique of UPPAAL Tron to hybrid systems. Refinement checking based on conformance testing.

CISS will continue its work on controller synthesis: for timed games with partial observability and with dynamic computation of the "cheapest" observations that will ensure that enable controllability. Incorporation of efficient on-the-fly, CEGAR-like algorithms within UPPAAL TIGA are planned.

In the Trader project of ESI the Triceps architecture, proposed for car systems, will be further evaluated. Trader knowledge on how to define reliable systems is used as guiding knowledge.

In the Poseidon project of ESI the maritime security systems will be further developed.

Within the EU project Quasimodo, several partners will elaborate further on the time testing theory integration with symbolic data test theory. Furthermore, we aim at an application of quantitative verification methods to the Quasimodo case studies.

IRISA will continue work on testing: integration of time and data and test coverage criteria. Diagnosis and predictability for infinite state systems.

IRISA will continue work on control synthesis: control under partial observation of infinite symbolic transitions systems handling data, and extension to modular symbolic STS and distributed systems modeled by STS with fifo queues.

OFFS: the deployment synthesis which had been planned for year one will be implemented over the next twelve month.

CFV intends to continue the application of synthesis techniques to industrial relevant applications. We hope to be able to consider techniques for games of imperfect information in that context. Also, CFV intends to study new algorithms for the synthesis of controller with omega-regular properties and to apply antichains techniques in that context.

3.2 Current and Future Milestones

EPFL: Games for Verification and Synthesis

Our work in Year established new algorithms for solving games of imperfect information, including resource-constrained games. We have also considered issues such as repair of unrealizable specifications and robustness in timed games.

We plan to make a first release of a tool for solving games of imperfect information with parity objectives. This tool will be a prototype, based on theoretical results obtained in Year 1 [BCD+08].

Existing algorithms for solving concurrent games have no known rate of convergence. We expect to find termination criteria for solving concurrent safety and reachability games.

In the next year, we will concentrate on improving specifications specifically for the synthesis task. We will pursuit two maindirections.

(1) We will investigate how to handle freedom (unspecified parts) in aspecification. The idea is to put additional constraints usin quantitative specifications. This will allow to define differentdegrees of freedom and/or correctness.

(2) We will develop a notion of robustness that allows to predict how sensitive a constructed system is to incorrect inputs.

EPFL and CFV: Verification of Markov chains

An algorithm for the transient solution of well-structured Markov chains with very large state spaces has been implemented. It is based on a finite state projection.

The extension of the algorithm to infinite-state models and to steady-state solutions will be investigated next year.

EPFL: Verification of safety properties for software program artifacts.

We have worked on techniques that combine symbolic analyzes (e.g., predicate abstraction, shape abstraction) and explicit analyzes.We will explore opportunities of combining different analyzes in novel, flexible way.

In the next year, the focus will be on interactions between abstractionrefinement and dynamic precision adjustment among analyzes, in particular exploiting explicit values to help inferring meaningfulpredicates.

CISS, ESI and INRIA will continue to work on test generation for models with data and time, using approximate verification, and ideas from diagnosis and control. We already mixed ideas of diagnosis and control for testing in the context of security. In the following months we will try to adapt these ideas in the context of embedded sysems. We will also start our work on semantic coverage criteria for timed models. The general idea is to try to use our previous work on the correspondance between probabilistic and topological semantics of timed automata.
INRIA and LSV will continue to study probabilistic semantics for timed automata for qualitative as well as quantitative aspects, in order to make advances in performance estimation for real-time systems.
We already solved the problem of qualitative model-checking for single clock timed automata, and gave a partial answer in the quantitative study of these particular timed systems as outlined above in the quoted publications.
Future work will consist in extending the scope of systems that are encompassed, by broadening the class of timed automata we can treat for qualitative analysis and quantitative analysis afterwards.

CISS and INRIA will explore timed extension of modal specifications as a stepping step towards component-based design of systems with real-time aspects. In particular CISS will work towards an embedded We are currently working on a definition of Timed Modal Specifications, extending modal specifications as well as timed automata. So far, we justified notions of model relation, specification refinement, and consistency. Next year, further developments on Timed Modal Specifications, such as product and quotient operations will be studied.

INRIA will try to solve problems in stochastic partially observable games.
Probabilistic Büchi Automata are special instances of 1 player stochastic game of partial information. Decision problems for PBA such as emptiness test (corresponding to the nonexistence of a winning strategy), and combination operators have been studied, as reflected in the quoted publications.
Further study of these particular kind of games, as well as the exploration of more general types of games (2 player games) for diverse objectives will be the focus of the coming year.

CISS and LSV will work on the open problems related to cost-bounded infinite runs for weighted timed automata and games.

CISS and CFV will continue collaboration on controller synthesis for timed games aiming at abstraction/refinement algorithms for (priced) timed games with partial observability.

OFFIS will work on deployment synthesis and extended compositional analyses for HRC (safety, failure). Date: December 2009

3.3 Main Funding

- **Trader project**. This project is partially supported by the Dutch Ministry of Economic Affairs under the BSIK program.
- **Poseidon project**. This project is partially supported by the Dutch Ministry of Economic Affairs under the BSIK program.
- **Quasimodo.** This is a project under the 7th Framework Programme of the European Committee.
- **DaNES - Danish Network of Embedded Systems**
  DaNES. Danish national project sponsored by the Danish Advanced Technology Foundation.
- **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).
- **COMBEST** (COMponent-Based Embedded Systems design Techniques). Project funded by the European Science Foundation.
- **SNSF** (Swiss National Science Foundation).
- **French ANR project Testec** (Testing of real-time embedded control-command systems) with Lurpa (Ens Cachan), Inria (Rennes), I3S (Nice) , Labri (Bordeaux), EDF R&D, TNI Software.
- **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.
- **Dynamically Self-Configuring Automotive Systems (FP6)**
  DySCAS is a research project funded by the European Commission within FP6. The project started June 1 2006 and will end in February 2009.
- **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/
- **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/
- **The JAviator Project**, IBM Faculty Award 2007 (Helicopter Platform).
- **Concurrent Programming with Threading by Appointment**, Austrian Science Fund (FWF), Grant P18913-N15
- **GASICS** (ESF project of games for synthesis)
- **MOVES** (Belgian project on software evolution and verification)
- **CFV** (FNRS project on computer aided verification)
- **QUPES**: Dutch Research Council (NWO)
- **COMPASS**: European Space Agency (ESA)

4. Internal Reviewers for this Deliverable

Martin Törngren (KTH Stokholm, Sweden)

Laurent Doyen (EPFL, Austria)