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

Activity Progress Report for Year 3

Validation

Cluster:

Modeling and Validation

Activity Leader:

Professor Kim G. Larsen (CISS, Aalborg University)

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

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

Versions

number	comment	date
1.0	First version delivered to the reviewers	February 4th 2011

Table of Contents

1. Overview of the Activity 4
1.1 ArtistDesign participants and their role within the Activity 4
1.2 Affiliated participants and their role within the Activity 5
1.3 Starting Date, and Expected Ending Date 6
1.4 Policy Objective 7
1.5 Background 7
1.6 Technical Description: Joint Research 7
1.7 Work achieved in Year 1 (Jan-Dec 2008) 8
1.8 Problem Tackled in Year 2 (Jan-Dec 2009) 9
1.9 Problems Tackled in Year 3 (Jan-Dec 2010) 10

2. Summary of Activity Progress in Year 2 11
2.1 Technical Achievements 11
Sub-activity A: Compositional Validation 11
Distributed and Modular HTL (Salzburg + Uni. Porto + IST Austria + Uni. Trento) 13
Heterogeneous Composition (TRENTO + IST + CMI + UC Berkeley + UTRC) 14
Statistical Analysis of Controller Area Network Message Response Times (Trento + GM) 16
2.2 Individual Publications Resulting from these Achievements 22
2.3 Interaction and Building Excellence between Partners 25
2.4 Joint Publications Resulting from these Achievements 26
2.5 Keynotes, Workshops, Tutorials 28
Key Note: Plenary Talk at the CPS week in Stockholm, Cyber Physical Systems: the Dream of Dr. Frankenstein 29
Panel: 2010 Design Automation Conference, Designing the Always-Connected Car of the Future 31
Anaheim, California, June 15th, 2010 31

3. Milestones, and Future Evolution 34
3.1 Problem to be Tackled over the next 12 months (Jan 2011 – Dec 2011) 34
3.2 Current and Future Milestones 34
3.3 Main Funding 35

4. Internal Reviewers for this Deliverable 38

1. Overview of the Activity

1.1 ArtistDesign participants and their role within the Activity

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

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

Prof. Tom Henzinger (IST, Austria);
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.

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

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

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

Alberto Sangiovanni-Vincentelli, University of Trento, Italy.
Platform-Based Design, the Metropolis and COSI frameworks, distributed sense and control systems, industrial applications and international activities.

Roberto Passerone, University of Trento (Italy)
Formal analysis of heterogeneous composition, abstract algebra, and meta-modelling..

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

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

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

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

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

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

-- Changes wrt Y2 deliverable --

Affiliations of Tom Henzinger and Alberto Sangiovannic-Vencentelli has changed.

1.2 Affiliated participants and their role within the Activity

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

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

Stavros Tripakis – University of California at Berkeley (USA)
Monitoring and test of real-time properties

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

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

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

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

Dr. Patricia Bouyer, Dr. Nicola Markey and Dr. 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.

Prof. Peter Habermehl – LIAFA (France)
verification of programs with arrays and dynamic data structures

-- Changes wrt Y2 deliverable --

No changes

1.3 Starting Date, and Expected Ending Date

Starting date: January 1st 2008

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

-- Changes wrt Y2 deliverable --

No changes with respect to Year 2.

1.4 Policy Objective

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

-- Changes wrt Y2 deliverable --

No changes with respect to Year 2.

1.5 Background

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

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

-- Changes wrt Y2 deliverable --

No changes with respect to Year 2.

1.6 Technical Description: Joint Research

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

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

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

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

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

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

-- Changes wrt Y2 deliverable --

No changes with respect to Year 2.

1.7 Work achieved in Year 1 (Jan-Dec 2008)

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

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

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

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

-- No changes wrt Y2 deliverable --

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

1.8 Problem Tackled in Year 2 (Jan-Dec 2009)

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

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

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

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

1.9 Problems Tackled in Year 3 (Jan-Dec 2010)

We maintain the division of the validation activities in the following three subactivities:

A. Compositional Validation: aiming at developing validation techniques for establishing properties of composite heterogeneous systems from properties of its components.

B. Quantitative Validation: aiming at developing validation techniques for quantitative system properties including time, resource, hybrid as well as stochastic properties.

C. Cross-layer Validation: aiming at developing methods validating the conformance between designs at different levels of abstraction as well as conformance of executable code and designs.

Within the sub-activity A “Compositional Validation” several partners have worked substantially and collaboratively on compositional design and verification methodologies for functional, timing and stochastic aspect. This methods span assume/guarantee reasoning, interface automata as well as modal transition systems for rich models. Also, theoretical foundations and coordination languages has been developed for heterogeneous systems. Finally, a framework for tool integration based on meta-models and model-transformations has been established.

Within sub-activity B “Quantitative Validation” substantial work has been made on improved schedulabilty analyses supporting multiprocessor and multi-core applications. The improved methods include taking scheduler overhead into account, being power-aware – i.e. exploiting slacks in the system of processes to reduce power consumption while insuring deadlines are met. This work includes combination of abstract interpretation and model-checking for timing and interference analysis of parallel programs on multi-core, and schedulability analysis of Safety Critical Java applications on FPGAs,. Symbolic validation methods for timed automata based formalisms extended with cost/energy information as well as stochastic interpretations has been developed. Also, the work within this sub-activity includes exploitation and implementation of statistical model-checking techniques within the BIP tool.

Within the subactivity C “Cross-Layer Validation” substantial work has been made on improved methods for model-based testing. This work includes incremental testing of composite systems, off-line test generation from timed automata models, model-based test generation for data-intensive systems, as well as runtime monitoring. Work on controller synthesis has continued, focusing on synthesis techniques for timed games, modal specifications, and scenario-based specifications with the purpose of addressing timing properties, multi-objective optimization as well as fault-tolerance. Validation related to executable implementation includes run-time programming, optimal implementation of communication for time-constrained synchronous reactive modules, as well as modular WCET analysis of C-code executing on ARM-processors.

2. Summary of Activity Progress in Year 2

2.1 Technical Achievements

Sub-activity A: Compositional Validation

Causality analysis in contract violation (INRIA) Establishing liabilities in component-based systems is a challenging task, as it requires to establish convincing evidence with respect to the occurrence of a fault, and the causality relation between the fault and a damage. The second issue is especially complex when several faults are detected and the impact of these faults on the occurrence of the failure has to be assessed. In [GLMR10] we have proposed a formal framework for reasoning about logical causality between contract violations. Thus we provide ways to reason on component traces to establish causality properties which go beyond temporal causality and can be used to assess the role of a fault in the occurrence of a failure.

Interface Theories (CISS+INRIA+ITU**)** Nowadays, systems are tremendously big and complex, resulting from the assembling of several components. These many components are in general designed by teams, working independently but with a common agreement on what the interface of each component should be. As a consequence, mathematical foundations that allow to reason at the abstract level of interfaces are needed. Any good interface theory should propose a satisfaction relation (to decide whether a system is an implementation of an interface), a consistency check (to decide whether the specification admits an implementation), a refinement (to compare specifications in terms of inclusion of sets of implementations), logical composition (to compute the intersection of sets of implementations), and structural composition (to combine interfaces).

Most of existing interface theories does not allow to specify timed (scheduling, ...) and/or stochastic (failures, ...) constraints. However, handling at least one of these aspects is often needed to model complex systems such as embedded and heterogeneous systems. Together with Kim Larsen and Andrzej Wasowski, we have proposed the first complete interface theory for timed systems [DLLNW10,DLLNW10b,DLNW10c]. Timed I/O interfaces are timed automata whose transitions are equipped with Input (environment) and Output (system) modalities. We defined satisfaction, refinement, composition, and conjunction. We also proposed an optimistic game-based approach to decide whether a specification admits at least one implementation. The theory comes together with an algorithm to synthesize an interface automaton from two specifications.

Our approach has been implemented as an extension of the well-known UPPAAL toolset in the branch ECDAR. [DLLNW10c]. In Ecdar, a component interface describes both the behavior of the component and the component's assumptions about the environment. The tool supports the important operations of a good compositional reasoning theory: composition, conjunction, quotient, consistency/satisfaction checking, and refinement. The operators can be used to combine basic models into larger specifications to construct comprehensive system descriptions from basic requirements. Algorithms to perform these operations have been based on a game theoretical setting that permits, for example, to capture the real-time constraints on communication events between components. The compositional approach allows for scalability in the verification.

Contracts for Modular Discrete Controller Synthesis (INRIA) In [DMR10], we describe the extension of a reactive programming language (BWR) with a behavioral contract construct. BZR is dedicated to the programming of reactive control of applications in embedded systems, and involves principles of the supervisory control of discrete event systems. Our contribution is in a language approach where modular discrete controller synthesis (DCS) is integrated, and it is concretized in the encapsulation of DCS into a compilation process.

Tool and model integration to support embedded systems analysis (KTH and Volvo) Design models and their respective tools are today not well integrated with analysis tools for example referring to safety analysis and formal methods based analysis. Since these tools are usually disconnected the models may become inconsistent, which hampers understandability of the models and increases the cost of development. KTH has conducted a number of investigations of model-based tool integration approaches, and case studies that involve the integration of modeling with analysis tools. Metamodeling, model transformation technologies and modular adaptors have been developed to build bridges between tools. Examples of case studies include:

- Integration of tools for automotive embedded systems: A systems engineering tool, a safety engineering tool and a simulation tool.
- Integration between a UML tool and the SPIN model checker

Since this work invariably includes work on modeling/meta-modeling as well as mapping to analysis techniques and tool integration, some of this work is also partly reported in the modeling activity.

Model-implemented fault injection to simulate the effect of hardware-related faults in embedded systems (KTH and SP) This work touches upon modeling and simulation, with the goal to support robustness testing and test-case generation for safety related systems. Simulations with fault-injection in models are compared with those at hardware level. This work includes work on modeling/meta-modeling as well as mapping to analysis techniques and tool integration A longer description of the same achievement is available in the Modeling activity.

Incremental component testing (CEA LIST) We have proposed an approch for testing incrementally component oriented systems. The key idea is to see a system Sys as Sys'*Rem where Sys' is the system to be tested and Rem the complementary subsystem. We have defined conformance relations to relate Sys' with its specification but taking into account the fact that the testing architecture interacts with the whole system Sys with various degree of observability concerning messages exchanged between sys' and Rem. We have defined and implemented associated test execution algorithms. We have shown by means of theorems that our approach only reveals non conformance of Sys' even though observability is restricted.

Compositional and Incremental Verification for Component-Based Systems (VERIMAG and INRIA) VERIMAG and INRIA continue the quest for efficient incremental techniques for computing invariants of concurrent systems expressed in BIP. Their work extends the compositional verification technique from [BBSN08] in which system-level invariants are computed as conjunctions of (local) invariants of the individual components with an (global) interaction invariant that takes concurrency and interaction between components into account.

The work in [BLN+10] provides a fixed point characterization for interaction invariants. This characterization leads to a much efficient computation technique: it starts by computing successors for each component location and, at each iteration, constrains the result by using existing interactions and the partially computed information for other locations. The resulting formula represents exactly the same interaction invariant as the one produced by the basic

method in [BBNS08]. However, it provides a much compact representation and is easier to handle than the former.

The work in [BBL+10] reconsiders the computation of invariants during an incremental design process. Incremental design works by adding progressively new interactions to partial system designs, which are, an already existing set of atomic components and interactions. Each time an interaction is added, one may be interested to verify whether the current system design satisfies some given property. Indeed, it is important to report an error as soon as it appears. However, each verification step may be time consuming, which means that intermediary verification steps are generally avoided. The situation could be improved if the result of the verification process could be reused when new interactions are added. Existing techniques, including the one in [BBNS08], do not focus on such aspects.

The new techniques developed in [BBL+10] are based on sufficient conditions that ensure the preservation of invariants through the introduction of new interactions. Moreover, for cases in which these conditions are not met, additional techniques allow for generation of new invariants in an incremental manner, that is, by reusing invariants already computed on the partial design. The reuse of existing invariants reduces considerably the computational effort. These techniques, which rely on finer analysis of the relation between behavior of components and their interactions, is efficient for arbitrary component interconnection topologies (i.e., cyclic or acyclic).

The incremental verification techniques have been implemented in the D-Finder toolset. Among the experiments conducted, VERIMAG has been capable of verifying properties and deadlock-freedom of DALA, an autonomous robot whose behavior in the functional level. This experiment, which is conducted in collaboration with industrial partners, is far beyond the scope of existing academic tools such as NuSMV or SPIN.

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

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

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

Heterogeneous Composition
(TRENTO + IST + CMI + UC Berkeley + UTRC)

We have addressed the problem of heterogeneous composition from a theoretical point of view, starting from a collaboration with IST-Austria, UC Berkeley and the Chennai Mathematical Institute, and later extending it to UTRC to get a better grasp of the actual issues faced by designers when connecting different models of computation. One of the main result of this research is our belief that heterogeneous composition is relative, and depends on the final outcome that the designer wants to achieve. We have proceeded by focusing on the main principles of platform-based design: the models to be connected should strictly maintain their identity in order to 1) preserve their properties that typically lead to efficient analysis methods, and 2) be reusable in different contexts and with other models of interaction. At the same time, to enact any kind of interaction, the models must come together in a domain, which we have called the common semantic domain. The common semantic domain, however, as a common refinement, is unable to preserve identity, and serves the sole purpose of describing the kind of desired interaction. The actual interaction, instead, takes place in a mixed domain, where each model can be embedded separately, and provides a way of describing model adapters. These principles have been applied to the definition of an interface process between an untimed model of computation and a timed one. Here, we have used Khan Process Networks (KPN) as an example for an untimed data flow model, and Finite State Machines (FSM) as a model for synchronous timed communication based on signals. We have used an example provided by UTRC (by Alessandro Pinto) and realized a set of interfaces both in the SystemC language, and in Metro II, showcasing different kinds of interactions between data flow and finite state models.

Compositional Methodology for Stochastic Systems (CISS+INRIA+ITU**)** Notions of specification, implementation, satisfaction, and refinement, together with operators supporting stepwise design, constitute a specification theory. In [CDLLPW10] we construct such a theory for Markov Chains (MCs) employing a new abstraction of a Constraint MC. Constraint MCs permit rich constraints on probability distributions and thus generalize prior abstractions such as Interval MCs. Linear (polynomial) constraints suffice for closure under conjunction (respectively parallel composition). This is the first specification theory for MCs with such closure properties. We discuss its relation to simpler operators for known languages such as probabilistic process algebra. Despite the generality, all operators and relations are computable.

Sub-activity B: Quantitative Validation

Probabilistic Regular Graphs (INRIA) Deterministic graph grammars generate regular graphs, that form a structural extension of configuration graphs of pushdown systems. In [BM10], we study a probabilistic extension of regular graphs obtained by labelling the terminal arcs of the graph grammars by probabilities. Stochastic properties of these graphs are expressed using PCTL, a probabilistic extension of computation tree logic. We present here an algorithm to perform approximate verification of PCTL formulae. Moreover, we prove that the exact model-checking problem forPCTL on probabilistic regular graphs is undecidable, unless restricting to qualitative properties. Our results generalise those of Esparza et al (2006), on probabilistic pushdown automata, using similar methods combined with graph grammars techniques.

Statistical model-checking (INRIA and Verimag) We are primarily interested in the Statistical Model Checking approach (SMC). SMC has recently been proposed as an alternative to avoid an exhaustive exploration of the state-space of a system under verification. The core idea of the approach is to conduct some simulations of the system and then use results from the statistic area in order to decide whether the system satisfies the property with respect to a given probability. The answer is correct up to some confidence. SMC is generally much faster (but less precise) than formal verification techniques.

Within the EU project COMBEST, INRIA and VERIMAG considered the use of SMC to verify applications working within a huge heterogeneous system (more than 23000 states), namely the cabin communication system of an airplane (HCS). Specifications of this system were provided by EADS, our industrial partner in COMBEST. The difficulty in this verification process comes from network communication, which makes all applications interfere, and therefore forces us to explore the full state-space of the system. Unfortunately, SMC was not capable to compete with the size of the case study. This motivated the development of a new simulation-based technique, which we call Stochastic Abstraction. This technique starts by performing simulations of the system in order to learn the context/environment where the application is used. Then, it creates a stochastic abstraction for the application, taking the context information into account. This smaller model can be verified using efficient techniques such as SMC. We have applied this approach to two industrial case studies that are beyond the scope of existing formal techniques: (1) The HCS case study, and (2) an Avionics Full Duplex Switched Ethernet.

Power-aware Temporal Isolation (Salzburg) Salzburg has proposed a higher-level scheduling method for variable-bandwidth servers (VBS) for reducing power consumption while maintaining temporal isolation. This is possible whenever there is slack in a system of processes. There are multiple kinds of slack with different potential for reducing variance in system utilization by slowing down and speeding up process execution temporarily. Less variance in system utilization enables scaling down to and maintaining of lower processor frequencies.

Scheduler Overhead Accounting (Salzburg) Salzburg has proposed a schedulability test for variable-bandwidth servers (VBS) that accounts for non-zero scheduler overhead using either so-called response accounting, or utilization accounting, or a combination of both accounting methods. Response accounting maintains system utilization at the expense of increased response times while utilization accounting maintains response times at the expense of increased system utilization. Previous schedulability tests are typically based on the assumption that scheduling takes zero time and may have therefore flagged systems as in theory schedulable that were in fact in practice not schedulable.

Expressiveness and Tractability of Digraphs as Real-Time Task Models (Uppsala) Models for real-time systems have to balance the inherently contradicting goals of expressiveness and analysis efficiency. Current task models with tractable feasibility tests have limited expressiveness, restricting their ability to model many systems accurately. In particular, they are all recurrent, preventing the modeling of structures like mode switches, local loops, etc. In this work, we advance the state-of-the-art with a model that is free from these constraints. Our proposed task model is based on arbitrary directed graphs (digraphs) for job releases. We show that the feasibility problem on preemptive single-processor systems remains tractable. This even holds in the case of task systems with arbitrary deadlines.

Combining Abstract Interpretation with Model Checking for Timing Analysis of Multi-core Software (Uppsala) In this work, we study a multicore architecture where each core has a local L1 cache and all cores use a shared bus to access the off-chip memory. We use Abstract Interpretation (AI) to analyze the local cache behavior of a program running on a dedicated

core. Based on the cache analysis, we construct a Timed Automaton (TA) to model the precise timing information of the program on when to access the memory bus (i.e. when a cache miss occurs). Then we model the shared bus also using timed automata. The TA models for the bus and programs running on separated cores will be explored using the UPPAAL model checker to find the WECTs for the respective programs.
Based on the presented techniques, we have developed a tool for multicore timing analysis, which allows automatic generation of the TA models from binary code and WCET estimation for any given TA model of the shared bus. Extensive experiments have been conducted, showing that the combined approach can significantly tighten the estimations. As examples, we have studied the TDMA and FCFS buses. In both cases, the WCET bounds can be tightened by up to 240% and 82% respectively, compared with the worst-case bounds estimated based on cache misses and maximal delays for bus access.

Fixed-Priority Multiprocessor Scheduling: Beyond Liu & Layland Utilization Bound (Uppsala) The increasing interests in multicores raise the question whether known results for single-processor scheduling can be generalized to the multiprocessor setting. Recently, in 2009 this has been shown (by Uppsala) for the famous Liu and Layland utilization bound by applying novel task splitting techniques. However, parametric utilization bounds that can guarantee higher utilizations (up to 100%) for common classes of systems are not yet known to be generalizable to multiprocessors as well. In this paper, we solve this open problem for most parametric utilization bounds by proposing new partitioning-based scheduling algorithms. As the second technical contribution, we show that the utilization bound proofs can be established even when exact Response Time Analysis is used for task partitioning. This enables significantly improved average-case utilization in comparison to previous work.

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

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

architecture of a vehicle as well as about its functionality. We provided results that showed our statistical inference allows predicting accurately the distribution of the response time of a CAN message, once its priority has been assigned, from limited information such as the bus utilization of higher priority messages.
This publication obtained the best paper award at the IEEE Symposium on Industrial Embedded Systems.

Abstract Probabilistic Automata (CISS+INRIA + Aachen) Probabilistic Automata (PAs) are a widely-recognized mathematical framework for the specification and analysis of systems with non-deterministic and stochastic behaviors. [CKS+10] proposes Abstract Probabilistic Automata (APAs), that is a novel abstraction model for PAs. In APAs uncertainty of the non-deterministic choices is modeled by may/must modalities on transitions while uncertainty of the stochastic behaviour is expressed by (underspecified) stochastic constraints. We have developed a complete abstraction theory for PAs, and also propose the first specification theory for them. Our theory supports both satisfaction and refinement operators, together with classical stepwise design operators. In addition, we study the link between specification theories and abstraction in avoiding the state-space explosion problem.

Weighted Kripke Structures (CISS) We extend in [FLT10] the usual notion of Kripke structures with a weighted transition relation and generalize the classical Boolean interpretation of CTL to a map which assigns to states and temporal formulae a real-valued distance describing the degree of satisfaction. We describe a general approach to obtaining quantitative interpretations for a generic extension of the CTL syntax and show that, for one such interpretation, the logic is both adequate and expressive with respect to quantitative bisimulation.

Verification and Synthesis of Battery Powered Autonomous Truck (CISS+Mälardalarn) An embedded system is often subject to timing constraints, resource constraints, and it should operate properly no matter how its environment behaves. This paper proposes to use timed game automata to characterize the timed behaviors and the environment uncertainties, and use piecewise constant integer functions to approximate the continuous resources in real-time embedded systems. Based on these formal models and techniques, we employ the real-time model checker UPPAAL to verify a system against a given functional and/or timing requirement. Furthermore, we employ the timed game solver UPPAAL-TIGA to check whether a given control objective can be enforced, and if so, we synthesize a controller for the system. We carry out a case study of this approach on a battery-powered autonomous truck. Experimental results indicate that the method is effective and computationally feasible.

Model Checking of WSAT Protocol (CISS) In [RVS10] we present a formal analysis of the Web Services Atomic Transaction (WSAT) protocol. WS-AT is a part of the WS-Coordination framework and describes an algorithm for reaching agreement on the outcome of a distributed transaction. The protocol is modelled and verified using the model checker UPPAAL. Our model is based on an already available formalization using the mathematical language TLA+ where the protocol was verified using the model checker TLC. We discuss the key aspects of these two approaches, including the characteristics of the specification languages, the performances of the tools, and the robustness of the specifications with respect to extensions.

Model Checking of WS-Business Acitvity Protocol (CISS) WS-Business Activity specification defines two coordination protocols in order to ensure a consistent agreement on the outcome of long-running distributed applications. In [RVS11] we use the model checker UPPAAL to analyse the Business Agreement with Coordination Completion protocol type. Our analyses show that the protocol, as described in the standard specification, violates correct operation by reaching invalid states for all underlying communication media except for the perfect FIFO. Based on this result, we propose changes to the protocol. A further investigation of the modified protocol suggests that messages should be received in the same order as they are sent so that a correct protocol behaviour is preserved. Another important property of

communication protocols is that all parties always reach their final states. Based on the verification with different communication models, we prove that our enhanced protocol satisfies this property for asynchronous, unreliable, order-preserving communication whereas the original protocol does not.

Analysis of Duration Probabilistic Automata (CISS+VERIMAG+CMU**)** In [MLK10] we propose an extension of the zone-based algorithmics for analyzing timed automata to handle systems where timing uncertainty is considered as probabilistic rather than set-theoretic. We study duration probabilistic automata (DPA), expressing multiple parallel processes admittng memoryfull continuously distributed durations. For this model we develop an extension of the zone-based forward reachability algorithm whose successor operator is a density transformer, thus providing a solution to verification and performance evaluation problems concerning acyclic DPA (or the bounded-horizon behavior of cyclic DPA).

Reachability Analysis for Timed Systems (CISS) The model-checker UPPAAL is based on the theory of timed automata and its modeling languague offers additional features such as networks of timed automata, clocks and stop-watches, synchronizing over synchronous and broadcast channels, discrete variables ranging over bounded integers or structured types (arrays and records) as well as user-defined types and functions. In [L10] we give an overview of the development of the datastuctures and algorithms underlying the verification engines of UPPAAL and CORA as well as indicate on-going research directions.

Timed Automata with Energy Constraint (CISS+LSV) In [BFLM10], we study one-clock priced timed automata in which prices can grow linearly or exponentially, with discontinuous updates on edges. We propose EXPTIME algorithms to decide the existence of controllers that ensure existence of infinite runs (or reachability of some goal location) with non-negative observer value all along the run. These algorithms consist in computing the optimal delays that should be elapsed in each location along a run, so that the final observer value is maximized (and never goes below zero).

Schedulability Analysis using UPPAAL (CISS) In [MLRNSPPH10] We propose a modeling framework for performing schedula bility analysis by using Uppaal real-time model-checker [2]. The frame- work is inspired by a case study where schedulability analysis of a satel- ite system is performed. The framework assumes a single CPU hardware where a fixed priority preemptive scheduler is used in a combination with two resource sharing protocols and in addition voluntary task suspension is considered. The contributions include the modeling framework, its application on an industrial case study and a comparison of results with classical response time analysis.¨

Schedulability Analysis for Java Finalizers (CISS) Java finalizers perform clean-up and finalisation of objects at garbage collection time. In real-time Java profiles the use of finalizers is either discouraged (RTSJ, Ravenscar Java) or even disallowed (JSR-302), mainly because of the unpredictability of finalizers and in particular their impact on the schedulability analysis. In [BHRTS10] we show that a controlled scoped memory model results in a structured and predictable execution of finalizers, more reminiscent of C++ destructors than Java finalizers. Furthermore, we incorporate finalizers into a (conservative) schedulability analysis for Predictable Java programs. Finally, we extend the SARTS tool for automated schedulability analysis of Java bytecode programs to handle finalizers in a fully automated way.

Sub-activity C: Cross-layer Validation

Threaded program verification (INRIA) Modern systems involve a complex organization of computational processes sharing access to both processors and resources. The use of threads in programming provides a method in which lightweight processes may be given specific tasks that can be carried out either independently or in cooperation with other threads. The correct and efficient use of shared resources between threads relies on synchronization methods, such as specialized commands or events communicated between threads. Our work demonstrates a semi-automated method of translating cooperatively threaded software to the synchronous programming language SIGNAL in order to verify the correctness of thread synchronizations in the source code

Off-line Test Selection with Test Purposes for Non-Deterministic Timed Automata (INRIA) In [BJSK11] we propose novel off-line test generation techniques for non-deterministic timed automata with inputs and outputs (TAIOs) in the formal framework of the tioco conformance theory. In this context, a first problem is the determinization of TAIOs, which is necessary to foresee next enabled actions, but is in general impossible. This problem is solved in [BSJK11] thanks to an approximate determinization using a game approach, which preserves tioco and guarantees the soundness of generated test cases. A second problem is test selection for which a precise description of timed behaviors to be tested is carried out by expressive test purposes modeled by a generalization of TAIOs. Finally, using a symbolic co-reachability analysis guided by the test purpose, test cases are generated in the form of TAIOs equipped with verdicts.

Automatic Test Generation for Data-Flow Reactive Systems with time constraints (INRIA) In [LMR10] we handle the problem of conformance testing for data-flow critical systems with time constraints. We present a formal model (Variable Driven Timed automata) adapted for such systems inspired from timed automata using variables as inputs and outputs, and clocks. In this model, we consider urgency and the possibility to fire several transitions instantaneously. We present a conformance relation for this model and we propose a test generation method using a test purpose approach, based on a region graph transformation of the specification.

Timed Game Abstractions for Control Systems (CISS) With the aim of enabling automatic controller design for dynamical systems, a method for abstracting control systems by timed game automata is developed and applied in [SW10a,SW10b]. The method is based on partitioning the control and state space, by use of a family of positive and negative invariant sets, which are sub-level sets of Lyapunov functions. The abstraction is based on timed game automata since tools for automatic controller synthesis for such models exist. Controllers for timed game automata are designed to satisfy a Timed Computation Tree Logic (TCTL) specification; hence, in addition to stability temporal requirements can be added. We provide conditions for the Lyapunov functions that are used in the partition, such that sound and complete abstractions of control systems are generated. Finally, an example is provided to illustrate the application of the method.

Supervisory Control for Modal Specifications of Services (INRIA) In [DDM10] we investigate the adaptation of the supervisory control theory of Ramadge and Wonham to enforce a modal specification (with final states marking the ends of the sessions) on a system modelled by a finite LTS. We prove that there exists at most one most permissive solution to

this control problem. We also prove that this solution is regular and we present an algorithm for the effective computation of the corresponding controller.

Multicriteria optimal discrete controller synthesis for fault-tolerant real-time tasks (INRIA) In [DGMR10] we propose a technique for discrete controller synthesis, with optimal synthesis on bounded paths, in order to model, design, and optimize fault-tolerant distributed systems, taking into account several criteria (e.g., the execution costs of the tasks and their quality of service). Different combinations are explored for multi-criteria optimization.

Runtime Programming (Saltzburg) Salzburg in collaboration with the University of Porto continued exploring the fully compositional semantics of HTL and developed a general notion of runtime programming through model-preserving and scalable runtime patches. HTL is used in a case study. The idea of runtime programming is to run two programs of which one implements the actual application and the other supervises the execution of the application, in analogy to a traditional controller-plant model. The controller may modify the plant, i.e., the application, at runtime in a well-defined, modular and thus scalable fashion. Runtime programming aims at introducing flexibility in a well-understood way into complex software systems, which are traditionally inflexible and therefore unable to address uncertainty.

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

Scenario-based Verification and Synthesis of Real-Time Systems (CISS) [LLNP10a] proposes two approaches to tool-supported automatic verification of dense real-time systems against scenario-based requirements, where a system is modeled as a network of timed automata (TAs) or as a set of driving live sequence charts (LSCs), and a requirement is specified as a separate monitored LSC chart. We make timed extensions to a kernel subset of the LSC language and define a trace-based semantics. By translating a monitored LSC chart to

a behavior-equivalent observer TA and then non-intrusively composing this observer with the original TAmodeled real-time system, the problems of scenario-based verification reduce to computation tree logic (CTL) real-time model checking problems. When the real-time system is modeled as a set of driving LSC charts, we translate these driving charts and the monitored chart into a behavior-equivalent network of TAs by using a “one- TA-per-instance line” approach, and then reduce the problems of scenario-based verification also to CTL real-time model checking problems. We show how we exploit the expressivity of the TA formalism and the CTL query language of the real-time model checker UPPAAL to accomplish these tasks. The proposed two approaches are implemented in the UPPAAL tool and built as a tool chain, respectively. We carry out a number of experiments with both verification approaches, and the results indicate that these methods are viable, computationally feasible, and the tools are effective.

In [LLNP10b] We propose an automated, tool-supported approach to scenario-based analysis and synthesis of real-time embedded systems. The inter-object behaviors of a system are modeled as a set of live sequence charts (LSCs), and the scenario-based user requirement is specified as a separate LSC. By translating the set of LSC charts into a behavior-equivalent network of timed automata (TA), we reduce the problems of model consistency checking and property verification to classical CTL real-time model checking problems, and reduce the problem of centralized synthesis for open systems to a timed game solving problem. We implement a prototype LSC-to-TA translator, which can be linked to existing real-time model checker UPPAAL and timed game solver UPPAAL-TIGA. Preliminary experiments on a number of examples show that it is a viable approach.

Modular Worst Case Execution Time Analysis (CISS) Safe and tight worst-case execution times (WCETs) are important when scheduling hard real-time systems. [DOTHL10] presents METAMOC, a path-based, modular method, based on model checking and static analysis, that determines safe and tight WCETs for programs running on platforms featuring caching and pipelining. The method works by constructing a UPPAAL model of the program being analysed and annotating the model with information from an inter-procedural value analysis. The program model is then combined with a model of the hardware platform, and model checked for the WCET. Through support for the pla□orms ARM7, ARM9 and ATMEL AVR 8-bit the modularity and retargetability of the method is demonstrated, as only the pipeline needs to be remodelled. Modelling the hardware is performed in a state-of-the-art graphical modeling environment. Experiments on the Mälardalen WCET benchmark programs show that taking caching into account yields much a tighter WCETs, and that METAMOC is a fast and versatile approach for WCET analysis.

Abstractions for Testing Data-Intensive Embedded Systems (CISS) We present in [OLS10] a new abstraction of embedded systems interacting with databases. This abstraction is intended to be used for model-based testing. We abstract the database into two sets: present set and absent set, and present a proof of this abstraction. We present two extensions of FSM, the DBFSM and PAFSM. DBFSM are a form of FSM incorporating databases. PAFSM are an abstraction of DBFSM using present-absent sets. Depending on what type of testing is to be done, the translation is tailored to fit this purpose. We show how this translation is related to the present/absent abstraction. Finally, we illustrate the approach through a small example and show how this can be used for testing with the model-based testing tool Uppaal TRON.

-- The above is new material, not present in the Y2 deliverable --

2.2 Individual Publications Resulting from these Achievements

INRIA

[GlMR10] G. Goessler, D. Le Métayer and J.-B. Raclet. Causality Analysis in Contract Violation. In Proc. of the 1st International Conference on Runtime Verification (RV'10), Malta, November, 2010. LNCS 6418. pp.270-284. Springer.

[JBGT10] K. Johnson, L. Besnard, T. Gautier, and J.-P. Talpin. A synchronous approach to threaded program verification. In 10th International Workshop on Automated Verification of Critical Systems (AVOCS'10). Düsseldorf, Germany, September 2010.

[LMR10] O. Landry Nguena, H. Marchand, A. Rollet. Automatic Test Generation for Data-Flow Reactive Systems with time constraints (Short paper). In 22nd IFIP International Conference on Testing Software and Systems, Pages 25-30, Natal, Brazil, November 2010.

[BM10] N. Bertrand, C. Morvan. Probabilistic Regular Graphs. In Infinity, EPTCS, Volume 39, Pages 77-90, Singapore, September 2010.

[DDM10] Ph. Darondeau, J. Dubreil, H. Marchand. Supervisory Control for Modal Specifications of Services. In Workshop on Discrete Event Systems, WODES'10, Pages 428-435, Berlin, Germany, August 2010.

[DGMR10] E. Dumitrescu, A. Girault, H. Marchand, E. Rutten. Multicriteria optimal discrete controller synthesis for fault-tolerant real-time tasks. In "Workshop on Discrete Event Systems, WODES'10", August 2010, p. 366-373.

[DMR10] G. Delaval, H. Marchand, E. Rutten. Contracts for Modular Discrete Controller Synthesis. In Conference on Languages, Compilers and Tools for Embedded Systems, LCTES 2010, Pages 57-66, Stockholm, Sweden, April 2010.

[BJSK11] N. Bertrand, T. Jéron, A. Stainer, M. Krichen. Off-line Test Selection with Test Purposes for Non-Deterministic Timed Automata. To appear in TACAS 2011, Saarbrucken, Germany, March 2011.

[BSJK11] N. Bertrand, A. Stainer, T. Jéron, M. Krichen. A game approach to determinize timed automata. To appear in FOSSACS 2011, Saarbrucken, Germany, March 2011.

KTH

[BST10] M. Biehl, C.-J. Sjöstedt, and M. Törngren, A modular tool integration approach - experiences from two case studies. In 3rd Workshop on Model-Driven Tool & Process Integration at the European Conference on Modelling Foundations and Applications, June 2010.

[BDT10] Matthias Biehl, Chen DeJiu, Martin Törngren. Integrating Safety Analysis into the Model-based Development Toolchain of Automotive Embedded Systems.Proceedings of the LCTES 2010, 13-15 April 2010, ACM Press.

Salzburg

[CKS10a] S.S. Craciunas, C.M. Kirsch, and A. Sokolova. Power-aware Temporal Isolation with Variable-Bandwidth Servers. Proc. International Conference on Embedded Software (EMSOFT). ACM, 2010.

[CKS10b] S.S. Craciunas, C.M. Kirsch, and A. Sokolova. Response Time versus Utilization in Scheduler Overhead Accounting. Proc. Real-Time and Embedded Technology and Applications Symposium (RTAS). IEEE, 2010.

CEA LIST

[Escobedo 10] Jose Pablo Escobedo, Christophe Gaston, Pascale Le Gall, and Ana Cavalli, Testing Web Service Compositions in context: a symbolic approach, SEFM 2010, September 13-18 2010, Pisa, Italy.

[Gaston10] Christophe Gaston, Pascale Le Gall, Nicolas Rapin, Assia Touil.Symbolic Execution-Based Techniques for Conformance Testing, In Model Driven Engineering for distributed Real-Time SystemsMARTE modelling, model transformations and their usages Edited by Jean-Philippe Babau, Mireille Blay-Fornarino, Joël Champeau, ENSIETA, Sylvain Robert, LIST, Antonino Sabetta, ISTI CNR, ISBN: 9781848211155. ISTE

UPPSALA

[SENY11] Martin Stigge, Pontus Ekberg, Guan Nan and Wang Yi. The Digraph Real-Time Task Model. Martin. Accepted by RTAS11, the 17th IEEE Real-Time and Embedded Technology and Applications Symposium, Chicago, IL, USA April 11 - 14, 2011.

[LNYY10] Mingsong Lv, Guan Nan, Wang Yi and Ge Yu. Combining Abstract Interpretation with Model Checking for Timing Analysis of Multicore Software. In the proc. of the 31th IEEE Real-Time Systems Symposium, November 30 - December 3, 2010, San Diego, CA, USA.

[GSYY10] Nan Guan, Martin Stigge, Wang Yi and Ge Yu. Fixed Priority Multiprocessor Scheduling: Beyond Layland and Liu's Utilization Bound. In the proc. of RTSS10 Work in Progress, November 30 - December 3, 2010, San Diego, CA, USA.

[AKY10] Parosh Aziz Abdulla, Pavel Krcal, and Wang Yi. Sampled Semantics of Timed Automata. Journal: Logical Methods in Computer Science, vol 6(3), 2010.

[KWDY10] Fanxin Kong, Yiqun Wang, Qingxu Deng and Wang Yi. Minimizing Multi-Resource Energy for Real-Time Systems with Discrete Operation Modes. Proc of ECRTS 2010, the 22nd Euromicro Conference on Real-Time Systems, Brussels, Belgium. July 6-9, 2010.

VERIMAG

[BBSN08] S. Bensalem, M. Bozga, J. Sifakis, and T.-H. Nguyen. Compositional verification for component-based systems and application. In Proceedings of the 6th International Symposium on Automated Technology for Verification and Analysis, pages 64–79, Berlin, Heidelberg, 2008. Springer-Verlag.

[BBL+10] S. Bensalem, M. Bogza, A. Legay, T.-H. Nguyen, J. Sifakis, and R. Yan. Incremental component-based construction and verification using invariants. In Proceedings of Formal Methods for Computer Aided Design FMCAD'10, Lugano, Switzerland, 2010.

[BLN+10] S. Bensalem, A. Legay, T.-H. Nguyen, J. Sifakis, and R. Yan. Incremental invariant generation for compositional design. In Proceedings of 4th International Symposium on

Theoretical Aspects of Software Engineering TASE'10, Taipei, Taiwan, ROC, pages 157-167, 2010.

TRENTO

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

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

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

CISS

[MLRNSPPH10] Marius Mikucionis, Kim Guldstrand Larsen, Jacob Illum Rasmussen, Brian Nielsen, Arne Skou, Steen Ulrik Palm, Jan Storbank Pedersen, and Poul Hougaard. Schedulability analysis using uppaal: Herschel-planck case study. In *4th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation (ISoLA'10)*, Lecture Notes in Computer Science, Crete, Greece, October 2010.

[LLNP10a] Kim Guldstrand Larsen, Shuhao Li, Brian Nielsen, and Saulius Pusinskas. Scenario-based verification of real-time systems using uppaal. Formal Methods in Systems Design (FMSD), July 2010.

[LLNP10b] Kim Guldstrand Larsen, Shuhao Li, Brian Nielsen, and Saulius Pusinskas. Scenario-based analysis and synthesis of real-time systems using uppaal. In Proc. 13th Conf. on Design, Automation and Test in Europe (DATE'10), pages 447–452, Dresden, Germany, March 2010. IEEE.

[DOTHL10] Andreas E. Dalsgaard, Mads Chr. Olesen, Martin Toft, Rene R. Hansen, and Kim G. Larsen. METAMOC: Modular Execution Time Analysis Using Model Checking. In Björn Lisper, editor, 10th International Workshop on Worst-Case Execution Time Analysis (WCET 2010), pages 114–124, 2010.

[SW10a] Christoffer Sloth and Rafael Wisniewski. Proofs for an abstraction of continuous dynamical systems utilizing lyapunov functions. arXiv:1008.3222, 2010.

[OLS10] P. Olsen, K. G. Larsen, and A. Skou. Present and absent sets: Abstraction for testing of reactive systems with databases. In *The 6th Workshop on Model-Based Testing, Cyprus (MBT'10)*, 2010.

[BHRTS10] Thomas Bøgholm, René R. Hansen, Anders P. Ravn, Bent Thomsen, and Hans Søndergaard. Schedulability analysis for java finalizers. In *JTRES '10: Proceedings of the 8th International Workshop on Java Technologies for Real-Time and Embedded Systems*, pages 1–7, New York, NY, USA, 2010. ACM.

Mikkel Larsen Pedersen, and Andrzej Wasowski. Abstract probabilistic automata. In *Proceedings of 12th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI)*, 2011.

[FLT10] Uli Fahrenberg, Kim G. Larsen, and Claus Thrane. A quantitative characterization of weighted K ripke structures in temporal logic. *Computing and Informatics*, 2010.

[RVS10] A.P. Ravn, S. Vighio, and J. Srba. A formal analysis of the web services atomic transaction protocol with uppaal. In *Proceedings of the 4th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation (ISOLA'10)*, LNCS. Springer-Verlag, 2010.

[L10] Kim Guldstrand Larsen. Symbolic and compositional reachability for timed automata. In *Reachability Problems, 4th International Workshop, RP 2010, Brno, Czech Republic, August 28-29, 2010. Proceedings*, pages 24–28, 2010.

[RSV11] Anders P. Ravn, Jiri Srba, and Saleem Vighio: *Modelling and Verification of Web Services Business Activity Protocol.* Accepted for publication in TACAS 2011.

-- The above are new references, not present in the Y2 deliverable --

2.3 Interaction and Building Excellence between Partners

- C. Baïer (U. Dresden) visited INRIA to work with N. Bertrand
- H. Marchand visited CFV (U. Bruxellles) to work with T. Massart.
- Collaboration between INRIA and Verimag on Characterization of testable properties. In [FFJMM10], we characterize the set of testable properties within the Safety-Progress classification. Furthermore, we address automatic test generation for the proposed framework. A protoype tool implementing the results has been developped.
- Salzburg's work on programmable temporal isolation is part of a new initiative in rigorous systems engineering (RiSE) with nine partners in Austria including IST Austria.
- Uppsala is collaborating with ETHZ on interference analysis for multi-core architecture.
- Wang Yi gave a course on model checking of timed systems at Linköping University.
- **CISS + INRIA** (Rennes) are actively collaborating on compositional specification theories for timed as well as stochastic systems. In both cases the theories may be seen as quantitative extensions of modal transition systems with corresponding quantitative notions of refinement. This collaboration has resulted in a number of visits by Axel Legay to Aalborg, extensive stay of Bernoit Delahaye in Aalborg, visit by Benoit Cailoud in Aalborg, as well visits of PhD students from Aalborg to INRIA.
- **CISS + LSV** are actively collaborating on developing a rich theory for priced or weighted timed automata and games. In particular, extended settings with both negative and positive as well as exponential and linear cost-rates have introduced a range of new cost (or energy) bounded problems to be formulated and partially solved. These problems are particularly relevant from the perspective of addressing energy-aware and -optimal schedules for autonomous embedded systems. Collaboration also include work on robustness for timed automata.
- **CISS+Verimag** has collaborated on zone-based analysis of so-called duration probabilistic automata, i.e. networks of one-clock timed automata with a stochastic interpretation. The collaboration was initiated during a 1 month visit to Aalborg by Oded Maler.

- **CISS** is collaborating with **Uppsala** --on the maintenance development and commercialization of Uppaal
- ETHZ, INRIA, OFFIS, Trento and VERIMAG has collaborated within the SPEEDS project lead on the definition of the SPEEDS metamodel HRC which is the basis of an important analysis platform. This collaboration continues for the definition of a verification methodology. From the collaboration in SPEEDS has started a broader collaboration on a general framework for the semantics of communication in distributed systems with INRIA, PARADES and VERIMAG with external collaboration of University of Columbia and Cadence Design Systems [BCC+].
- In the Combest project several joint activities are being carried out. In particular, Verimag and ETHZ collaborate on the combination of analytical performance analysis via performance analysis of a corresponding more precise operational model in order to obtain more precise results.

-- Changes wrt Y2 deliverable --

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

2.4 Joint Publications Resulting from these Achievements

[DLLNW10a] A. David, K.G. Larsen, A. Legay, U. Nyman, and A. Wasowski. Timed I/O automata: a complete specification theory for real-time systems. In International Conference on Hybrid Systems: Computation and Control (HSCC'10), Stockhlom, Sweden, April 2010.

[DLLNW10b] Alexandre David, Kim G. Larsen, Axel Legay, Ulrik Nyman, and Andrzej Wasowski. An interfacetheory for timed systems (abstract). In *Presented at the 20th International Workshop on Algebraic Development Techniques WADT*, 2010. To appear.

[FFJMM10] Y. Falcone, J.-CFernandez, T. Jéron, H. Marchand, L. Mounier. More Testable Properties. In 22nd IFIP International Conference on Testing Software and Systems, Lecture note in Computer Science, Volume 6435, Pages 30-46, Natal, Brazil, November 2010 (Best paper award).

[FCLT10] Lei Feng, DeJiu Chen, Henrik Lönn, and Martin Törngren: Verifying System Behaviors in EAST-ADL2 with the SPIN Model Checker. IEEE International Conference on Mechatronics and Automation. Xi'an, China, August 4-7, 2010. Best conference paper award.

[SEVT10] Rickard Svenningsson, Henrik Eriksson, Jonny Vinter and Martin Törngren. Model-Implemented Fault Injection for Hardware Fault Simulation. Models Workshop on Model-Driven Engineering, Verification and Validation (at the Models Conf., Oct. 3, 2010).

[SVET10b] Rickard Svenningsson, Jonny Vinter, Henrik Eriksson, Martin Törngren. MODIFI: A MODel-Implemented Fault Injection Tool. Safecomp 2010.

[BDGLPY10] Gerd Behrmann, Alexandre David, Kim Guldstrand Larsen, Paul Pettersson and Wang Yi. Developing UPPAAL over 15 years. Journal: Software - Practice and Experience, Wiley Publisher, 2010.

[LDB10] A. Legay, B. Delahaye, and S. Bensalem. Statistical Model Checking: An Overview. International Conference on Runtime Verification, RV'10, LNCS Volume 6418, pp 122-135. Malta, Novembre 2010.

[BBBDLS10] A. Basu, S. Bensalem, M. Bozga, B. Delahaye, A. Legay, and E. Sifakis: Verification of an AFDX Infrastructure Using Simulations and Probabilities. International Conference on Runtime Verification, RV'10, LNCS Volume 6418, pp 330-344. Malta, November 2010.

[BBBCDL10] A. Basu, S. Bensalem, M. Bozga, B. Caillaud, B. Delahaye, A. Legay: Statistical Abstraction and Model-Checking of Large Heterogeneous Systems. IFIP International Conference on Formal Techniques for Distributed Systems, FMOODS/FORTE'10. pp 32-46. Amsterdam, The Netherlands, June 2010.

[CKS+10] Benoit Caillaud, Joost-Pieter Katoen, Falak Sher, Benoit Delahaye, Kim G. Larsen, Axel Legay,

[LP10] Shuhao Li and Paul Pettersson. Verification and controller synthesis for resource-constrained real-time systems: Case study of an autonomous truck. In *Proc. 15th IEEE International Conference on Emerging Techonologies and Factory Automation (ETFA'10)*, Sep. 2010.

[DLLNW10] A. David, K.G. Larsen, U. Nyman, A. Legay, and A. Wasowski. *Methodologies for specification of real-time systems using timed i/o automata.* In Proceedings of FMCO 2009, Lecture Notes in Computer Science. To appear.

[MLK10] O. Maler, K.G. Larsen, and B. Krogh. On zone-based analysis of duration probabilistic automata. In *Proceedings of INFINITY, International Workshop on Verification of Infinite-State Systems*, 2010.

[DLLNW10c] Alexandre David, Kim G. Larsen, Axel Legay, Ulrik Nyman, and Andrzej Wasowski. Ecdar: An environment for compositional design and analysis of real time systems. In *Proceedings of 8th International Symposium on Automated Technology for Verification and Analysis (ATVA)*, 2010.

[BFLM10] Patricia Bouyer, Uli Fahrenberg, Kim G. Larsen, and Nicolas Markey. Timed automata with observers under energy constraints. In *Proceedings of the 13th ACM International Conference on Hybrid Systems: Computation and Control, HSCC 2010, Stockholm*, pages 61–70. ACM, 2010.

[CDLLPW10] Benoit Caillaud, Benoit Delahaye, Kim G. Larsen, Axel Legay, Mikkel Larsen Pedersen, and Andrzej Wasowski. Compositional design methodology with constraint markov chains. In *Proceedings of 7th International Conference on Quantitative Evaluation of SysTems (QEST)*. IEEE Computer, 2010

-- The above are new references, not present in the Y2 deliverable --

2.5 Keynotes, Workshops, Tutorials

A number of workshops have been organized in the framework of ICES (www.ices.kth.se). Some of these relate to analysis tools, for example for systems integration/hardware in the loop simulation. Since these workshops are performed in close cooperation with industry they are reported in the Industrial collaboration activity.

Y. Falcone. You should Better Enforce than Verify (Tutorial). In RV'10: Proceedings of the 1st International Conference on Runtime Verification, Lecture Notes in Computer Science, Volume 6418, Pages 89-105, Malta, November 2010.

Wang Yi, invited talk, the 12th International Conference on Formal Engineering Methods, Shanghai, Nov 16 - 19, 2010.

Wang Yi, invited lectures, Summer School on Model Checking, Chinese Academy of Sciences, Beijing, Oct. 2010.

Wang Yi, Invited lectures, VTSA School on Verification Technology, Systems and Applications, Luxembourg, Sept. 2010

Wang Yi, invited lectures, The 10th International School on Formal Methods for the Design of Computer, Communication and Software Systems: Quantitative Aspects of Programming Languages, Bertinoro, Italy, 21-26 June 2010

Wang Yi, invited lectures, ARTIST Summer School, Europe 2010, Autrans, France, Sept. 2010

Wang Yi, invited lectures, ARTIST Summer School, China 2010, Beijing, July 2010.

Invited Talk: *Systems Verification and Validation*
Kim G. Larsen, Complex Systems Design and Management, Paris, Cite, Universitaire, France, October 27-29, 2010.

Invited Talk: *Symbolic and Compositional Reachability for Timed Automata*
Kim G. Larsen, 4th Workshop on Reachability Problems, Brno, Czech Republic, August 27-29, 2010.

Invited Lectures: *Model-Based Verification and Analysis for Real-Time Systems.*
Kim G. Larsen, Summer School Marktoberdorf, Marktoberdorf, Germany, August 3-15, 2010.

Invited Talk: *Controller Synthesis from Timed Game Automata – from Theory to Practice*
Kim G. Larsen, Synthesis, Verification and Analysis of Rich Models, Edinburgh, Scotland, July 20, 2010.

Invited Talk: *Timing Analysis of Embedded Software Systems*
Kim G. Larsen,International Conference on Formal Verification of Object-Oriented Software, Paris, France, June 28-30, 2010.

Invited Talk: *Verification, Compositionality and Refinements for Real-Time Systems*
Kim G. Larsen, ACSD / PETRI NETS, Braga, Portugal, June 21-25, 2010.

Invited Talk: *Model-Driven Validation of Real-Time and Embedded Systems*

Kim G. Larsen, Dependable Systems ? Who Cares? CTIT Symposium. Twente University, The Netherlands, June 1, 2010.

Invited Lectures: *Extensions of Timed Automata*
Kim G. Larsen, WATA. Weighted Automata: Theory and Applications, May 3-7, 2010, Leipzig, Germany.

Invited Talk: *Verifying LEGO: Validation and Synthesis of Embedded Software*
Kim G. Larsen, BCTCS, 26th British Colloquium for Theoretical Computer Science, 6-9 April 2010, University of Edinburgh, Scotland**.**

Invited Lectures: *Validation, Performance Analysis and Synthesis of Embedded Systems*
Kim G. Larsen, AVACS, Automatic Verification and Analysis of Complex Systems, 1st AVACS Spring School, 15-19 March 2010, Oldenburg, Germany.

Invited Talk and Visit: Validation*, Performance Analysis and Synthesis of Embedded Systems*
Kim G. Larsen, CoSBi, The Microsoft Research-University of Trento, Centre for Computational and Systems Biology, 15-18 February, 2010.

Invited Talk: *Priced Timed Automata: Theory and Tools*
Kim G. Larsen, FSTTCS, IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, December 15 to 17, 2009, IIT Kanpur, India.

Key Note: **DATE 2010, Everything is Connected.**
Dresden, March 9, 2010
Alberto Sangiovanni Vincentelli gave one of the two key notes at DATE, a leading conference in design technology with more than 1,000 attendants. The talk was about the importance of distributed systems in the world of the future, what problems we may have to face in this world and how to design complex distributed systems.

http://www.ecsi.org/date-2010-conference

Key Note: Plenary Talk at the CPS week in Stockholm, Cyber Physical Systems: the Dream of Dr. Frankenstein
Stockholm, April 14, 2010
Alberto Sangiovanni Vincentelli gave one of three Plenary Talks at CPS week 2010 that hosted 5 conferences and several workshops. The talk was about forward looking applications of Cyber Physical Systems and methodology to reduce the complexity of the design.
http://www.kth.se/ees/omskolan/organisation/centra/access/dls/cpsweekplenary-1.58510?l=en_UK

Key Note: 2010 Symposium on Industrial Embedded Systems (SIES) Conference, **Connections, connections and connections. The problems of the embedded systems of the future**
Trento July 7th, 2010
Alberto Sangiovanni Vincentelli gave the key note at the Conference stressing the problems that stem from emerging behavior of widely distributed embedded systems.
http://events.unitn.it/en/sies2010

Key Note: Emerging Technologies and Factory Automation (ETFA) 2010, Distributed System Design: A Nightmare 'in fieri'
Bilbao, September 14, 2010
Alberto Sangiovanni Vincentelli gave a key note at the Conference addressing the nightmares that may ensue from the distributed system design problems.
http://www.etfa2010.org/

Key Note: IEEE System on Chip Conference (SOCC) 2010, SoC Design as an Example of Component-Based Design of Distributed Systems
Las Vegas, September 27, 2010
Alberto Sangiovanni Vincentelli gave the key note at the main conference on systems on chip outlining the need for a rigorous component-based design methodology to address the design of very large chips.
http://www.ieee-socc.org/SOCC2010/Program/program.html

Key Note: IEEE International Behavioral Modeling and Simulation Conference, Away from Plug and Pray towards Plug and Play in Analog-Mixed Signal Design: A Tale of Design Re-use
San Jose', September 24, 2010
Alberto Sangiovanni Vincentelli gave the key note at this mainly analog design conference stressing the need for compositional reasoning in analog design thus enabling a better approach to analog design re-use.
http://www.bmas-conf.org/program.html

Tutorials: Model Based System Engineering at the 2010 Control and Decision Conference (CDC)
Atlanta, Georgia – December 15th-19th, 2010
Alberto Sangiovanni Vincentelli co-organized and co-chaired with John Baras of University of Maryland two tutorial sessions at the CDC 2010 where he also presented two talks on Platform-Based Design and Model Based Design in the context of industrial applications.

Workshop: Green and Smart Embedded System Technology: Infrastructures, Methods and Tools (GREEMBED) at the Cyber-Physical System Week
Organizing committee, general chairs, Alberto Sangiovanni Vincentelli, Huascar Espinoza, Marco Di Natale, Roberto Passerone
Stockholm, Sweden, April 12th, 2010,
Efficient production, transmission, distribution and use of energy are fundamental requirements for our modern society and the challenge of a green, low carbon economy. Embedded systems have an important role to play in increasing the energy efficiency and in reducing carbon emissions to sustainable growth. Indeed, most systems for monitoring and control of energy production, distribution and use are today interconnected and controlled by embedded devices, in areas such as industrial manufacturing, transportation systems, building automation, domestic appliances and more. This offers the opportunity for the creation of new integrated systems offering new products, processes and services with greater efficiency and better situation awareness to end-users and service and infrastructure owners.

Energy-efficient systems offer unique challenges to the embedded system community, from system-level design to dynamic and adaptive controls, optimization of architectures and communication, real-time and reliable services as well as reusable software components and systems.
Energy efficient solutions include both local and global smart solutions. Smart embedded solutions merge ubiquitous computing and the Internet of Things, i.e., the technology integration with sensors, actuators, micro-chips, micro- and nano-embedded systems that allow for

collecting, filtering and producing more and more information locally, to be further consolidated and managed globally according to business functions and services. Locally, embedded systems provide information on energy consumption of every energy consuming appliance in a single location (e.g., home, building, vehicle) to be provided in real-time, in a user friendly way, thereby empowering citizens to take decisions that lead to energy savings. Globally, energy efficient solutions include smart grid concepts, which require dynamic controls for balancing and organizing production from renewable and conventional sources, negotiating, purchasing and routing power requests, but also regulating, balancing and controlling the amount of electrical power that systems consume. From the system-level design perspective, there is a need for simulation, modelling, analysis, and monitoring methods and tools to facilitate an integrated system approach. Today, energy efficient solutions are developed by independent companies whose products or components are tested for individual performance independently of each other. An integrated system approach to the design and implementation, where these components are integrated in a way that they reduce energy consumption through cooperation, is rarely used. This often leads to significant system-level inefficiencies. System design methods and tools, including model-based solutions, must consider the growth and evolvability of hardware and software platforms, to ease the conception, development, validation and integration of new devices and services. The challenge and opportunities not only lie in the integration issue, but also in providing methods and tools for innovative solutions that satisfy government regulations, customer expectations and meet environmental challenges.

http://www.artist-embedded.org/artist/Overview,1928.html

Panel: 2010 Design Automation Conference, Designing the Always-Connected Car of the Future

Anaheim, California, June 15th, 2010

The panel was co-organized and chaired by Alberto Sangiovanni Vincentelli. The automotive industry is introducing novel features, such as seamless vehicle-to-vehicle and vehicle-to-infrastructure connectivity to improve in vehicle driver safety (e.g., forward collision) and comfort (e.g., routing to avoid congestion) while facing stricter government regulations, and shortened time-to-market. As a result, automotive Electronic Control System (ECS) architectures are becoming increasingly complex. To cope with these challenges and opportunities, the entire automotive supply chain is engaged as follows: automotive OEMs are managing complexity by reusing legacy components and enabling new technologies; tier one suppliers are increasingly up-integrating features on the same computing platform; tier two suppliers are providing multicore and other powerful technologies; academic institutions are doing research in new analysis, synthesis and optimization methods; and tool providers are trying to raise the level of abstraction for system modeling, analysis and optimization.

http://www.dac.com/conference+program.aspx

Dagstuhl Seminar on Quantitative Models: Expressiveness and Analysis
Dagstuhl, January 18-22, 2010

The seminar identified three fundamental research areas, each addressing quantitative aspects, namely: weighted automata, timed and hybrids systems, and stochastic systems. The seminar was successful in bringing together 45 researchers from 13 countries discussing their recent research results and developments for quantitative models and their analysis.

Scientific organizer: Kim G. Larsen, Christel Baier, Manfred Droste, Paul Gastin.

PhD School QMC
Quantitative Model Checking PhD School, Copenhagen, February 2-5, 2010
http://qmc.cs.aau.dk/qmc.html

The PhD school on quantivative model checking, **QMC 2010**, is organized by the European Network of Excellence ARTIST Design and the Danish VKR Center of Excellence MT-LAB and takes place at the IT University Copenhagen from 2 to 5 March 2010. It features lectures and other activities by world-renowned experts within the areas of real-time, probabilistic, and hybrid model checking.

Programme Chairs : Kim G. Larsen, Joost-Pieter Katoen
Organizing Chair: Andrzej Wasowski
Publicity Chair: Uli Fahrenberg

Gasics Workshop 2nd Workshop on Games for Design, Verification and Synthesis, 4 September, Paris, 2010, Co-located with CONCUR 2010.
http://www.lsv.ens-cachan.fr/Events/gasics10/

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

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

Organizers: Kim G. Larsen, Nicolas Markey, Jean-François Raskin, Wolfgang Thomas.

ISOLA'10 Track: Quantitative Verification in Practice. 18 October 2010, Heraclion, Krete.
http://isola-conference.org/isola2010/

Model checking has been widely accepted by industry for verifying correctness of hardware and software systems. Temporal logics as PSL have been accepted as IEEE standard, significant shortcomings have been established in standardised protocols, and software of forthcoming NASA missions have been thoroughly checked by tools such as SPIN. Most systems --- embedded systems in particular--- are subject to a multitude of quantitative constraints. These constraints involve

- system's resources (computation resources, power consumption, memory usage, communication bandwidth, etc.),
- assumptions about the environment in which it operates (task arrival rates, signal fluctuations),
- requirements on the services the system has to provide (timing constraints, performance), and
- requirements on the continuity with which these services are delivered (availability, dependability, fault tolerance, etc.).

To meet these challenges quantitative extensions of model checking have emerged. These include timed automata verification, checking models that exhibit random phenomena (such as

Markov-like models), and hybrid systems. Powerful tools such as Uppaal, PRISM, MRMC, PASS and Phaver support this.

The main aim of this track is to show the practical usage of these techniques. What kind of practically relevant questions can be answered by these techniques? How is the practical usage of the tools?, What are their limitations? and so forth.

Track Organizers: Boudewijn Haverkort, Joost-Pieter Katoen, Kim G. Larsen

Tutorial at ESWEEK'2010, October 24, 2010, Scottsdale , Arizona, U.S.A.
EMSOFT Tutorial: Quantitative System Validation in Model-Driven Design, Lectures Holger Hermanns, Kim G. Larsen, Jean-Francois Raskin, Jan Tretmans,

The European Project Quasimodo (http://www.quasimodo.aau.dk/) develops theory, techniques and tool components for handling quantitative constraints in model-driven development of real-time embedded systems, covering in particular real-time, hybrid and stochastic aspects. This tutorial highlights the advances made, focussing on real industrial case studies tackled.

-- The above is new material, not present in the Y2 deliverable --

3. Milestones, and Future Evolution

3.1 Problem to be Tackled over the next 12 months (Jan 2011 – Dec 2011)

INRIA will continue its effort on verification, testing and control synthesis for various models with time, data,probabilities. In particular we expect contributions to the quantitative analysis of timed automata (probability, topology, frequency), and its use for model-based test generation.

KTH (with partners in the iFEST, CESAR and MBAT projects): Assessment of integration of new tools for testing and formal analysis with design tools.

Salzburg intends to continue working on process scheduling techniques for programmable temporal isolation that may eventually provide power isolation as well, or at least enable trading-off temporal and power isolation cost and quality.

CEA will extend its incremental testing framework to take into account timing constraints.

Uppsala will work on Interference and timing analysis for multi-core platforms as well as modelling and mapping of real-time applications onto multi-core platforms.

CISS will work on statistical model checking for extended timed automata models wrt a range of probabilistic temporal properties. The effort on application of real-time model checking for worst-case execution time analysis will continue but extended to establishing bounds on powerconsumption. The notion of energy-game we introduced at FORMATS08 is gaining attention and we aim at settling decidability and complexity of a number of multi-cost problem.

CISS and INRIA will continue their joint effort on compositional specification theories aiming at data-intensive systems.
‘

-- Changes wrt Y2 deliverable --

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

3.2 Current and Future Milestones

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

- **CEA LIST**
  will work on incremental component system testing with timing constraints.
- **IST**
  Austria will continue the work on property-base mixed-signal validation by actively participating in a standardization committee Impact on extensions of System Verilog Assertions (SVA) language with analogue operators.
- **INRIA and CISS**
  will jointly improve and apply the tool ECDAR for compositional development and verification of real-time systems.

- **CISS**
  will provide a first version of UPPAAL supporting statistical model checking for timed-automata based models.
- **UPPSALA and CISS**
  will continue effort on schedulability and timing analysis of embedded multi-core applications using combinations of abstract interpretation and model-checking.

3.3 Main Funding

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

- **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 and VERIMAG and affiliated industrial partners EADS and IAI.
  http://www.speeds.eu.com/
- **COMBEST (funded by European Union IST STREP)**
  COMponent-Based Embedded Systems design Techniques. COMBEST aims at enhancing techniques for the correct design of embedded systems. Combest emerged from collaborations in SPEEDS and ARTIST. Verimag, ETHZ, U. Braunschweig, IST, INRIA, OFFIS, U. Trento are partners.
  http://www.combest.eu
- French **ANR TesTec** project (Test of Real-time and critical embedded System)
- **INRIA** Associate Team grant with Universities of Campina Grande and Recife.
- **CESAR**: www.cesarproject.eu/
- **MAENAD**: www.maenad.eu
- **iFEST**: http:/www.artemis-ifest.eu/
- DFEA2020: www.md.kth.se/RTC
- **VERDE** ITEA project
- **French national ANR project LISE** (Liability Issues in Software Engineering) is a multidisciplinary project funded by ANR under the SeSur 2007 program (ANR-07-SESU-007). The project is led by INRIA and involves two research groups in law and four research groups in ICT.
- **CoDeR-MP - Real-Time Applications on Multicore Platforms**, Supported by the Swedish strategic research foundation: http://www.it.uu.se/research/coder-mp
- **UPMARC**: Uppsala Programming for Multicore Architectures Research Centre, supported by the Swedish Research Council: http://www.it.uu.se/research/upmarc

- **UPMARC:** Uppsala Programming for Multicore Architectures Research Center, supported by the Swedish Research Council

- **CoDeR-MP** - Real-Time Applications on Multicore Platforms, Supported by the Swedish strategic research foundation.
- **CREDO (http://www.cwi.nl/projects/credo/),** Modeling and analysis of evolutionary structures for distributed services, supported by EU
- **Modeling and verification of timed systems supported by the Swedish research council**
- **ANR project TesTec**: Test of Real-time and critical embedded System. Industrial research project that gathers two companies: an end-user (EDF R&D) and one software editor for embedded real-time systems and automation systems (Geensys), and four laboratories from automation engineering and computer science (I3S, INRIA Rennes, LaBRI, LURPA). This project focuses on automatic generation and execution of tests for embedded real-time systems.
- **European Strep Project Combest** (http://www.combest.eu/home/). The aim of this project is to provide a theoretical framework as well as implemented methods and tools for the component-based design of embedded systems. Our role in Combest is to work on timed components, and more precisely develop a theory around timed modal specifications.
- **PHC Procope PIPS**: Partial Information Probabilistic Systems The objective of this bilateral collaboration with the group of Pr. Christel Baier in TU Dresden (Germany) is to study partially observable probabilistic systems.
- **INRIA - DGRST project** with ENIS Sfax in Tunisia (Maher Ben Jemaa and Moez Krichen) on model-based testing of embedded systems.
- **TReaTiES: Test of REAl-TIme Embedded Systems** (http://www.irisa.fr/vertecs/EA-Brazil09.html). INRIA associated team with Federal University of Campina Grande in Brazil (Pr. Patrícia D. L. Machado) and University Pernambuco (Pr. Augusto Sampaio) on test case generation, selection and abstraction for embedded real-time systems
- **The JAviator Project**, IBM Faculty Award 2007 (Helicopter Platform).
- **Concurrent Programming** with Threading by Appointment, Austrian Science Fund (FWF), Grant P18913-N15 (Three PhD students).
- **ArtistDesign, Austrian Federal Ministry of Science and Research**, Grant 651.394/0001-II/2/2009 (Supplemental Support).
- **RNTL project HeCoSim** (http://projet-hecosim.org/) The goal of this project is to study Simulation and validation of heterogeneous virtual platforms of automotive industrial use case, following two different approaches the co-simulation and the global simulation, on the base of existing tools and of generated critical scenarii.
- **ITEA2 project VERDE** (www.itea2.org/public/project_leaflets/VERDE_profile_oct-09.pdf) VERDE will develop and industrialisea solution for iterative, incremental development and validation of realtime embedded systems (RTES) in aerospace, software radio, railway and automotive domains. The project will integrate model-driven engineering (MDE), component-based infrastructures and verification-and-validation (V&V) techniques.
- **ATESST** (Advancing Traffic Efficiency and Safety through Software Technology) ATESST2 is a two-year European project (FP7, Strep), coordinated by Volvo Technology and including OEMs, Suppliers/Tool vendors and Universities. http://www.atesst.org
- **CESAR** - Cost-efficient methods and processes for safety relevant embedded systems. CESAR is an Artemis project three year project resulting from the first call of Artemis.

The project focuses on the gathering, and further development, of methods and tools for safety critical embedded systems. The project has a large number of industrial and academic partners.
https://cesarproject.eu/index.php

- **SPEEDS IP Project**
  The SPEEDS project aims at significant enhancement of model-based systems engineering by semantics-based modelling for complex embedded systems using heterogeneous sub-system models, an by sound integration of existing and new tools using contract-based compositional analysis. Includes the ARTIST partners INRIA, OFFIS, PARADES and VERIMAG and affiliated industrial partners EADS and IAI.
  http://www.speeds.eu.com/
- **COMBEST (funded by European Union IST STREP)**
  COMponent-Based Embedded Systems design Techniques. COMBEST aims at enhancing techniques for the correct design of embedded systems. Combest emerged from collaborations in SPEEDS and ARTIST. Verimag, ETHZ, U. Braunschweig, IST, INRIA, OFFIS, U. Trento are partners.
  http://www.combest.eu
- **ARESA French National ANR project**
  The project aims at modelling energy consumption of Sensor networks with the aim to facilitate research, developments and commercialization of wireless sensor networks. Includes partners VERIMAG and affiliated partner FTRD.
  http://www-verimag.imag.fr/SYNCHRONE/index.php?page=fiche-aresa
- **French RNTL AVERILES Project**
  This project aims at the analysis and verification of embedded software systems with dynamic memory structures. It includes ARTIST partners VERIMAG and LSV, and affiliated partner LIAFA.
  www.lsv.ens-cachan.fr/rntl-averiles/
- **PROSYD IST Project**
  This project aims at the design of a standard, integrated property-based paradigm for the design of electronic systems building upon the emerging standard property specification language PSL/Sugar.
  http://www.prosyd.org/
- **MULTIFORM IST Project**
  This project aims Integrated Multi-formalism Tool Support for the Design of networked Embedded Control Systems. It includes ARTIST partners
  http://www.multiform.bci.tu-dortmund.de/

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

- **DaNES - Danish Network of Embedded Systems**
  DaNES. Danish national project sponsored by the Danish Advanced Technology Foundation. The goal of DaNES is to determine, develop and test a model-driven and component-based development-process for the realization of the intelligent embedded systems of the future, cross-cutting the industrial sectors spanned by the participating partners.
  http://www.danes.aau.dk/

- **MT-LAB: Modeling Information Technology.** Danish national project sponsored by Villum-Kahn Rasmussne Foundation. A collaboration between CISS (Aalborg University), IMM (Denmark Technical University) and ITU (Copenhagen). The scope fo the research centre is to explore and develop methods for formal verification of modern advanced software systems. The aim is to develop new methods and expand the applicability of previous methods in order to formally verify the functionality of complex interacting modern software systems.
  http://www.mtlab.dk/

-- Changes wrt Y1 deliverable --

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

4. Internal Reviewers for this Deliverable

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