IST-214373 ArtistDesign

Network of Excellence

on Design for Embedded Systems

Activity - Progress Report for Year 3

Modeling

Cluster:

Modeling and Validation

Activity Leader:

Susanne Graf (Verimag, Grenoble -- France)

http://www-verimag.imag.fr/~graf/

Policy Objective

Unlike other computer systems, embedded systems are strongly connected with a physical environment. A scientific foundation for embedded systems must therefore deal simultaneously with software, hardware resources, and the physical environment, in a quantitative manner. In order to gain independence from a particular target platform, embedded system design must be model-based. In order to scale to complex applications, embedded system design must be component-based. The overall objective of this activity is develop model and component based theories, methods, and tools that establish a coherent family of design flows spanning the areas of computer science, control, and hardware. The activity brings together the most important teams in the area of model and component based design in Europe.

Versions

number	comment	date
1.0	First version delivered to the reviewers	February 4th 2010

Table of Contents

1. Overview of the Activity

1.1 ArtistDesign Participants and Roles

Susanne Graf (Verimag, France)
modeling taking into account extra-functional properties.

Joseph Sifakis (Verimag, France)
Component-based design, the BIP framework, platform-aware implementation of embedded systems.

Dr. Sébastien Gérard (CEA, France)
Model-based engineering, specific focus on standard modeling (specially OMG UML, SYSML and MARTE standards) and RT/E (Real-Time/Embedded) domains.

Prof. Kim Guldstrand Larsen (CISS, Center for Embedded Software Systems, Denmark)
Timed automata based models with particular emphasis on extensions with cost, probabilities and multiplayer extensions. Verification, synthesis, performance evaluation and model-based testing.

Prof. Dr. Ir. Boudewijn R. Haverkort (Scientific Director of the ESI, The Netherlands)
Quantitative modeling.

Prof. Dr. Jozef Hooman (ESI Research Fellow, The Netherlands)
Component and resource modeling.

Dr. Alain Girault (INRIA, France)
Design and modeling for reliability of safety-critical embedded real-time systems. Protocol conversion techniques and discrete. Controller synthesis for component-based real-time systems. Design and programming of predictable embedded architectures.

Prof. Thomas A. Henzinger (IST, Austria)
Rich interface theory for component-based design. Quantitative properties for the design of reactive systems with resource constraints. Languages and algorithms for specifying, checking and comparing resource-dependent specifications.

Prof. Christoph Kirsch (University of Salzburg, Austria)
Cyber-physical cloud computing for scalable collaborative control. Runtime programming with Giotto-inspired languages and systems.

Prof. Axel Jantsch, KTH, Stockholm, Sweden
Integrated models of behavior, formal analysis and model refinements.

Prof. Martin Törngren (KTH Stockholm, Sweden)
Modeling of embedded systems, in particular multiview modeling, model integration and management.

Prof. Bengt Jonsson (Uppsala University, Sweden)
Component Modeling and Verification.

Prof. Wang Yi (Uppsala University, Sweden)
Component and Resource Modeling, Scalable Analysis, WCET Analysis of Parallel Programs on Multi-core, Multi-Core Real-Time Systems

Prof. Alberto Sangiovanni-Vincentelli (Uni. Trento, Italy)
Platform-Based Design, the Metropolis and COSI frameworks, industrial applications and international activities.

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

-- Changes wrt Y2 deliverable --

No changes

1.2 Affiliated Participants and Roles

Jacques Pulou (France Telecom R&D, France)
Component behaviour modeling, Component Based OS construction.

Prof. Albert Benveniste (INRIA Rennes, France)
Interfaces and modal automata

Prof. Roderick Bloem (TU Graz, Austria))
Game models for the synthesis problem

Bernhard Josko OFFIS, Oldenburg, Germany)
formal design and analysis techniques, regarding safety, real time and deployment

Dr Henrik Lönn, Volvo Technology
System engineering and modeling at Volvo. Leading the effort in developing the EAST-ADL modeling language for automotive embedded systems, through the series of projects EAST-EAA, ATESST and ATESST2.

Dr. Philippe Schnoebelen (LSV, ENS Cachan, France)
Weighted timed automata.

Jean-Francois Raskin (CVF – Belgium);
Synthesis for reactive systems. Timed and hybrid automata.

Sandeep Shukla (Virginia Tech and INRIA)
Modeling of embedded and synchronous systems

-- Changes wrt Y2 deliverable --

The list of affiliate partners has been updated to correspond to the actual contribution of year 3.

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 models and techniques to design systems 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

Unlike other computer systems, embedded systems are strongly connected with a physical environment. A scientific foundation for embedded systems must therefore deal simultaneously with software, hardware resources, and the physical environment, in a quantitative manner. In order to gain independence from a particular target platform, embedded system design must be model-based. In order to scale to complex applications, embedded system design must be component-based. The overall objective of this activity is to develop model and component based theories, methods, and tools that establish a coherent family of design flows spanning the areas of computer science, control, and hardware. The activity brings together the most important teams in the area of model and component based design in Europe.

-- Changes wrt Y2 deliverable --

No changes with respect to Year 2.

1.5 Background

An important class of model-based methodologies is those based on a synchronous execution model. The synchronous languages, such as Lustre, Esterel, and Signal, embody abstract hardware semantics (synchronicity) within different kinds of software structures (functional; imperative). Implementation technologies are available for several platforms, including bare machines and time-triggered architectures. Other model-based approaches are built around a class of popular languages exemplified by Matlab Simulink, whose semantics is defined operationally through its simulation engine. Originating from the design automation community, SystemC also chooses synchronous hardware semantics, but allows for the introduction of asynchronous execution and interaction mechanisms from software (C++). Implementations require a separation between the components to be implemented in hardware, and those to be implemented in software; different design-space exploration techniques provide guidance in making such partitioning decisions. More recent modeling languages, such as UML and AADL, attempt to be more generic in their choice of semantics and thus bring extensions in two directions: independence from a particular programming language; and emphasis on system architecture as a means to organize computation, communication, and constraints.

Model-based design relies on the separation of the design level from the implementation level, and is centered on the semantics of abstract system descriptions (rather than on the implementation semantics). Design often involves the use of multiple models that represent different views of a system at different levels of granularity. Usually design proceeds neither strictly top-down, from the requirements to the implementation, nor strictly bottom-up, by integrating library components, but in a less directed fashion, by iterating model construction, model analysis, and model transformation. Some transformations between models can be automated; at other times, the designer must guide the model construction. While the compilation and code generation for functional requirements is often routine, for non-functional requirements, such as timing, the separation of human-guided design decisions from automatic model transformations is not well understood. Indeed, engineering practice often relies on a trial-and-error loop of code generation, followed by test, followed by redesign (e.g., priority tweaking when deadlines are missed).

We believe that existing model-based approaches will ultimately fall short, unless they can draw on new foundational results to overcome the current weaknesses of model-based design, such as the lack of analytical tools for computational models to deal with physical constraints and quantitative metrics; and the difficulty to automatically and compositionally transform non-computational models into efficient computational ones. This leads us to the key needs for better paradigms for composition modeling, resource modeling, and quantitative modeling.

-- 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.

Sub-activity A: Component Modeling

Large embedded software systems are developed by distributed teams belonging to a number of different organizations. This calls for methods and techniques that split the design into smaller sub-systems and clarify the responsibilities for each participant. Theories of interfaces and contracts are needed to support these requirements and encompass functional, performance, resource, and reliability viewpoints. Additionally, we need to deal with the ability to integrate component-based system engineering within model-driven approaches. That means at least to work on refinement issues with regard to the component paradigm in order to benefit its full power with model-driven processes, which are basically iterative design processes.

We currently have a dichotomy between operational and transformational modeling approaches. Operational means automata-based: these approaches work on a component level, and have been successful in model checking, protocol verification, and code generation. Transformational means stream-based: these approaches work on the system level, and have been successful in performance analysis. While operational approaches have difficulties to scale to systems, transformational approaches suffer a loss of precision. We plan to develop techniques for bridging and combining both approaches.

Sub-activity B: Resource Modeling

Embedded software design differs from other software design in that behavioral properties must be reconciled with resource constraints. This is best done within models that permit the exploration of trade-offs between multiple dimensions, such as functionality, reliability, performance, and resource consumption. This ability must be carefully balanced against the need to separate concerns as much as possible. We expect different formalisms to be appropriate for different purposes, such as time-power trade-offs in power-constrained computing. The relevant dimensions (e.g., time and power) must then be captured within interfaces (sub-activity A) in order to support component-based design.

Complex embedded systems are built around specific distributed architectures and networks (e.g., Arinc, CAN, and FlexRay). Efforts have been undertaken to abstract such architectures as Models of Computation and Communication (MoCC): time-triggered, event-triggered, loosely time-triggered, etc. Research must further study and generalize these MoCCs to clarify their relationships, invent new ones with new interesting features, identify their basic building blocks, and find out how generic services can be built on top of them.

Sub-activity C: Quantitative Modeling

Classical specifications are typically of Boolean nature: a temporal specification is either satisfied or not; a real-time deadline is either met or not. This type of worst-case reasoning is not helpful in practical situations, where a system designer has to choose from a number of alternatives, none of them perfect, but some better than others. We propose to further develop quantitative theories of executable systems, together with rational criteria for making design decisions. In such theories, Boolean-valued system properties are replaced by real-valued rewards (or costs), and Boolean-valued refinement relations are replaced by real-valued similarity metrics.

Quantitative models are also required for modeling stochastic behavior, real-time behavior, and hybrid (mixed discrete-continuous) behavior. Our current models for such systems (Markov processes; timed automata; hybrid automata) tend to be brittle and overly sensitive towards arbitrarily small numeric perturbances. We need robust models for stochastic, timed, and hybrid systems. Moreover, the properties of interest are often application dependent; for this reason, we consider different application domains and the corresponding property classes.

-- Changes wrt Y1 deliverable --

No changes with respect to Year 1.

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

Within the sub-activity A “Component Modeling”, we focus on defining and composing models with heterogeneous semantics. We considered models with rich semantics (e.g. multi-priced timed automata), and combination of models with different semantics (e.g. object-oriented and component-based, modal automata and interface automata, functional and non-functional specifications).

Within the sub-activity B “Resource Modeling”, we study the design of resource-constrained systems, where the resource can be quantitative (e.g. energy consumption) or not (e.g. shared memory access). We have considered applications such as hardware design for embedded systems, transactional memory, performance and reliability modeling.

Within the sub-activity C “Quantitative Modeling”, we specifically focus on design frameworks for quantitative modeling (mainly timing and resource consumption). We proposed a quantitative generalization of classical languages; we worked on timed automata and timed Petri nets, and on improving adaptativity of systems.

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

Sub-activity A (Component Modeling)

CEA investigates the ability of MARTE, and especially its High-Level Application Modeling sub-profile, to denote various MoCC on a UML-based composite structure model (i.e., component in the UML2 terminology). More precisely, CEA is redesigning its methodology called Accord/UML that is by nature an Object-oriented approach to migrate towards a component-based methodology fostering the model-based engineering paradigm and relying on the MARTE standard.

CISS has worked on multi-priced timed automata with emphasis on Pareto-optimal reachability and optimal infinite scheduling, and on the class of one-clock priced timed automata with emphasis on model checking as well as optimal strategies.

CISS and ***EPFL*** are working on modal transition systems as interface specifications.

INRIA is working on convertibility verification for component-based embedded systems. Protocol conversion deals with the automatic synthesis of an additional component or glue logic, often referred to as an adaptor or an interface, to bridge mismatches between interacting components, often referred to as protocols. A formal solution, called convertibility verification, has been recently proposed, which produces such a glue logic, termed as a converter, so that the parallel composition of the protocols and the converter also satisfies some desired specification. A converter is responsible for bridging different kinds of mismatches such as control, data, and clock mismatches. Mismatches are usually removed by the converter (similar to controllers in supervisory control of discrete event systems) by disabling undesirable paths in the protocol composition.

KTH in cooperation with Volvo Technology and ***CEA*** have been further developing the EAST-ADL modeling language. The partner together have also together been OFFIS been part in setting up the new Artemis project CESAR where the EAST-ADL provides one important input. As part of this work, transformations between EAST-ADL and domain tools have been investigated.

KTH in cooperation with Volvo, and involving interactions with ***Aveiro***, ***MDH***, ***LTH*** and ***CEA,*** have been developing models for describing self-configuring embedded systems.

KTH has further developed ForSyDe as a framework for modeling, verifying and analyzing heterogeneous systems. In particular the framework has been enhanced to include dynamically reconfigurable systems.

OFFIS together with ***INRIA*** and ***VERIMAG*** have specified a tool-independent meta-model for heterogeneous rich components. Rich components are specification entities which combine several, otherwise often separately represented aspects, like functionality, safety or timing. The meta-model has to be rich enough to express formally specification of contracts for components in terms of assumptions/promises containing functional and non-functional viewpoints. The semantic foundation of the meta-model should allow its usage as a basis for analysis techniques.

Parades, in collaboration with UC Berkeley worked on design frameworks for system level design based on meta-models for heterogeneous systems. Metropolis has been analyzed and compared to other meta-modeling approaches. In addition, heterogeneous composition based on conservative approximations has been studied. The models of complex interconnects have been developed in the COSI modeling, analysis and synthesis framework.

VERIMAG has worked on the expressiveness of BIP and defined a new notion of expressiveness for components. VERIMAG has applied BIP to modeling of architectures of autonomous robots.

Sub-activity B (Resource Modeling)

CEA is working on the usage of the Hardware Resource Modeling sub-profile of MARTE combined with other modeling parts in order to enable simulation of embedded systems.

CISS is working on energy-constrained infinite runs in priced timed automata, on timed games with partial observability with emphasis on synthesis of strategies for reachability and safety objectives.

EPFL has worked on transactional memory, a new paradigm for concurrent programs. It allows a programmer to require a piece of code in the program to execute atomically. We have built a verification technique for various transactional memory implementations that exist in the literature.

ESI has worked on performance modeling. The problem that ESI addresses in this activity is modeling for various sub-domains in embedded systems, such as an electron microscope and warehouses. Modeling allows the analysis and prediction of system qualities and therefore will help to get to the optimal product at lower costs and shorter lead times. Next to this, models will be needed as part of the complex system control.

INRIA is working on design and modeling for reliability of safety-critical embedded real-time systems. All the existing heuristics for the (length, reliability) bi-criteria static multiprocessor scheduling problem suffer from three major drawbacks: first, the length criterion overpowers the reliability criterion; second, it is very tricky to control precisely the replication factor of the operations onto the processors, from the beginning to the end of the schedule (in particular, it can cause a funnel effect); and third, the reliability is not a monotonous function of the schedule. We wanted to propose a new framework for this problem, in order to avoid the aforementioned drawbacks.

KTH has studied resource allocation for delivering high performance and QoS. This work has included case studies in a variety of applications and systems.

Parades, in collaboration with Scuola di Sant'Anna, General Motors and UC Berkeley has investigated models for distributed interconnections including standard protocols such as FlexRay and has developed architecture exploration methods for the optimal choice of communication parameters based on these resource models.

VERIMAG has worked on a distributed semantics for BIP and enhanced the BIP execution engines to multithreaded execution.

Sub-activity C (Quantitative Modeling)

CEA is defining transformations of models to link models using the MARTE's extensions contained in its High-Level Application Modeling sub-profile towards a model using the extensions provided in the sub-profile for schedulability analysis.

CISS is working on timed automata versus timed Petri nets, and on probabilistic timed automata.

EPFL has defined a quantitative generalization of classical languages, and studied the expressive power of such languages, as well as natural generalization of decision problems such as emptiness, universality, and language inclusion.

ESI has worked on improving system evolvability, i.e. the ability to easily adapt systems in response to evolution of technology, competition, and/or customer expectations. The systems we look at are, a.o.: maritime information systems, medical devices and copiers. A challenge is gaining flexibility, adaptability and evolvability while retaining reliability at the same time.

Parades, with Scuola di Sant'Anna and General Motors are working on quantitative evaluation of designs for mapping and architectural exploration. The quantities modeled involve timing, power, cost and other less obvious quantities such as extensibility and flexibility. In particular, precise definitions of these concepts are investigated together with ways of computing their value.

VERIMAG has worked on the modeling of quantitative extra-functional properties for software-intensive embedded product lines.

-- Changes wrt Y2 deliverable --

This section was already presented in the Y2 deliverable, in section 1.7.

1.8 Work achieved in Year 2 (Jan-Dec 2009)

We maintain the division of the modeling activities into the three subactivities:

A. Component Modeling", where we focus on defining and composing models with heterogeneous semantics.

B. Resource Modeling", where we study the design of resource-constrained systems, where the resource can be quantitative (e.g. energy consumption) or not (e.g. shared memory access).

C. Quantitative Modeling", where we specifically focus on design frameworks for quantitative modeling (mainly timing and resource consumption).

Sub-activity A (Component Modeling)

According to the section 3.1 of the Y1 deliverable, **CEA** was planning for year 2 to refine and experiment its component-based design pattern for supporting MoCC as defined in the MARTE specification, and especially its High-Level Application Modeling sub-profile. This has not been achieved completely due to some delay in the definition of the formal final version of the MARTE standard itself, but the results are very promising. The limitations of our results are related to the scope covered by our work with respect to the MARTE standard. For the moment, our work only account for one specific MoCC defined in MARTE. According to that limitation, we get a first prototype of our new tool. This latter is going to be finalized in Year 3 in order to cover the full possible MoCC defined in the HLAM of MARTE (Technical Achievement 1, 2).

ESI progressed on the formalization of the Y-chart paradigm in the POOSL modeling language, respecting the Y-chart modularity. Modeling patterns have been defined for dataflow applications and platform resources using standardized model component interfaces for scalability (Technical Achievement 10).

ESI worked on modeling the behavior of systems and subsystems in industrial case studies, particular in connection with medical imaging devices and car entertainment systems. The relationship between data flow and control was investigated in cooperation with the University of Twente. Dynamically capturing the behavior of systems during actual use was studied in cooperation with the University of Groningen. Together with the Technical University of Eindhoven, ESI studied expressing system requirements in compositional dynamic models for the purpose of validation and supervisory control generation (Technical Achievements 11 and 13).

INRIA has developed the foundations for a contract-based theory of components amenable to multi-viewpoint modeling. INRIA and the University of Trento have interacted on some aspects of this topic (Technical Achievement 16).

INRIA also investigated the state of the art to modeling multi-clocked synchronous embedded system (Technical Achievement 17).

IST Austria worked on a theory of relational interfaces (Technical Achievement 19).

KTH worked on extending achievements of Y1 with respect to embedded systems modeling with the EAST-ADL. (Technical Achievement 28, 29)

Salzburg in collaboration with UC Berkeley began working on a higher-level, collaborative flight control system for the Salzburg helicopter platform, which now consists of ten identical vehicles. The system is based on the jointly developed collaborative sensing language CSL, which incorporates in many ways the experience from developing HTL and the Exotask system (Technical Achievement 31).

Salzburg, in collaboration with the University of Porto and IST explored the fully compositional semantics of HTL defined in year 1 with respect to language modularity. HTL is now mostly modular with respect to all key properties such as race freedom and schedulability. Modularity is important for scalability and fast runtime modifications through runtime patching (Technical Achievement 33).

Uni. Trento and UC Berkeley, **OFFIS**, **Verimag** and **INRIA** studied how to use meta-models such as the Heterogeneous Rich Component and the Metropolis meta-model for the representation of complex heterogeneous systems (see achievement 37).

Uni. Trento and UC Berkeley worked on the development of design frameworks for complex systems ranging from automobiles, buildings and airplanes to systems on chip. A new framework that evolved from Metropolis, Metro II, was also applied to the design of a UMTS system (see achievement.35)

VERIMAG has worked on translating synchronous languages into BIP, this work provides a deep understanding of the nature of synchronous computation as opposed to asynchronous computation. We identified synchronous systems as a subset of the BIP language. Furthermore, this work opens the way for meaningful integration of synchronous and asynchronous systems such as GALS (Technical Achievement 46).

VERIMAG worked on source-to-source architecture transformation (BIP2BIP), this work bridges the gap between component-based and corresponding monolithic programming. The former allows incremental description, readability, code reuse while the latter may lead to much more efficient implementations on a single processor. The experimental results show the interest of the approach (Technical Achievement 44).

VERIMAG has worked on distributed BIP, which complements already existing work on translating BIP with multiparty interaction and distributed BIP, the sublanguage encompassing only asynchronous message passing. This year's work allows computing more efficient schedulers and several approaches for distributed implementation of priorities (Technical Achievement 45).

VERIMAG has developed a general framework for **contract-based reasoning** allowing circular reasoning and proposed some instances of it (Technical Achievement 47).

Sub-activity B (Resource Modeling)

ESI developed modeling patterns in the POOSL modeling language for a diversity of resource types (including switched networks, processors, memory and, energy) and preemptive and non-preemptive scheduling mechanisms (Technical Achievement 10).

Together with Philips Healthcare and Philips Research, ESI has worked on the modeling of the thermal behavior of an MRI scanner, involving the imaging parameters, the power dissipation, and the coolant flow. Together with the University of Delft, ESI worked on modeling the workflow for complicated clinical procedures and its relationship to spatial constraint. (Technical Achievement 13)

IST Austria has pursued the work on transactional memory, a new paradigm for concurrent programs (Technical Achievement 23).

KTH and their partners worked on extensions of Y1 reported achievements in the domain of modeling of a middleware for self-configuring embedded systems (Technical Achievement 27). Salzburg began working on a real-time programming model called workload-oriented programming, which is inspired by HTL but more flexible and applicable to other applications than control such as multimedia applications (Technical Achievement 34).

Salzburg in collaboration with IBM Research improved the performance of the Exotask system by tackling priority inversion in the underlying virtual machine implementation (Technical Achievement 32).

Uni. Trento, Scuola di Sant'Anna, UC Berkeley and General Motors developed modeling and design methodologies for automotive parameter selections where communication protocols, periods and task allocations are concurrently adjusted to optimize delays, reliability and extensibility of unified architectures (see achievement 40)

Uppsala worked on schedulability analysis for multiprocessor platforms. The main focus has been on timing analysis of multi-core processors with shared caches, and multiprocessor scheduling (Technical Achievement 41 - 43).

VERIMAG has worked on the translation of the architecture description language AADL into BIP as a first step for efficient analysis architecture properties (Technical Achievement 48).

Sub-activity C (Quantitative Modeling)

CISS provided substantial work on the development of sound semantic basis for various component-based frameworks. Also, work on the formalism of modal transitions underlying several emerging component-based frameworks (for time and stochastic behavior) has been made, closing a number of long-standing open complexity problems (Technical Achievement 8).

A number of problems have been investigated for priced (or weighted) extensions of timed automata, which provide natural formalisms allowing for analysis and optimization of quantitative resources. In particular, so-called allowing negative as well as negative prices allow for a number of energy-bounded questions to be addressed, such as the existence of infinite runs within given energy constraints (Technical Achievements 4, 5).

CISS has worked towards the development of quantitative theories of executable systems, where Boolean-valued system properties are replaced by real-valued rewards (or costs), and Boolean-valued refinement relations are replaced by real-valued similarity metrics (Technical Achievement 9).

ESI has continued its work on performance modeling. The problem that ESI addresses in this activity is modeling for various sub-domains in embedded systems. Year 2 activities mainly focused on professional printers and wafer steppers (Technical Achievements 10 and 12)

IST Austria pursued its work on quantitative generalizations of classical languages, studying their expressiveness and closure properties, as well as their alternating and probabilistic extensions (Technical Achievement 20).

IST Austria and **TU Graz** worked on synthesis of optimal controllers from quantitative high-level specifications and on synthesis of robust systems from high-level specifications (Technical Achievement 21).

IST Austria, **INRIA** and **CVF** collaborated on studying robustness of sequential circuits (Technical Achievement 23).

Uni. Trento, United Technologies and UC Berkeley developed quantitative communication models and synthesis methods for energy efficient buildings and systems on chip (see achievement..)

-- Changes wrt Y2 deliverable --

This section was already presented in the Y2 deliverable, in sections 1.8 and in detail in 2.1

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

We maintain the division of the modeling activities into the three sub-activities:

A. Component Modeling”, where we focus on defining and composing models with heterogeneous semantics.

B. Resource Modeling”, where we study the design of resource-constrained systems, where the resource can be quantitative (e.g. energy consumption) or not (e.g. shared memory access).

C. Quantitative Modeling”, where we specifically focus on design frameworks for quantitative modeling (mainly timing and resource consumption).

Sub-activity A (Component Modeling)

CEA intended to continue to refactor its existing framework for designing real-time systems in order to apply component-based design pattern for supporting MoCC as defined in the MARTE specification, and especially its High-Level Application Modeling sub-profile. This framework called EC3M has been refactored and included in the new version of the UML tool Papyrus. The current version of EC3M is used for validation in a project consisting in proposing a component-based approach based on a set of specific design patterns for designing safety system with Alstom. (Technical Achievement 1).

CISS has worked on timed game abstractions from continuous dynamical systems using Lyapunov functions (Technical Achievement 6)

ESI investigated the modeling of components in the Healthcare domain addressing the problem of validating a global Healthcare architecture with respect to a number of use cases. Another topic is the improvement of the quality of the design process by relating multiple models in several formalisms to each other in such a way that communication over disciplines is improved, design errors are discovered in earlier phases, and the quality of the design is increased. In addition, ESI studied the use of models in the very early phases of product development, which many things have not been decided yet or are even not known (Technical Achievement 13).

INRIA has continued to develop the foundations for a contract-based theory of components amenable to multi-viewpoint modeling, in particular incorporating probabilities in component-based design frameworks. INRIA and the University of Trento have continued to develop the theory of Modal Interfaces initiated in Y2 (Technical Achievements 14, 15).

IST Austria, **VERIMAG** and **TU Graz** continued their work on robust synthesis, by developing a method for robust synthesis of components from high-level specifications in presence of liveness (Technical Achievement 23).

KTH in cooperation with Volvo devoted further work on embedded systems modeling, in particular the integration of architecture and safety modeling concepts, extending achievements of Y2 with respect to embedded systems modeling with EAST-ADL (Technical Achievements 27, 29, 30).

KTH studied how design decisions could be represented using model-driven techniques. **KTH** started a larger scale investigation on model and tool integration challenges and solutions (Technical Achievement 56).

KTH in collaboration with Volvo investigated how formal behavioral models could be integrated with architecture description languages.

KTH in collaboration with SP developed tools for fault-injection at model level as an approach for early robustness testing and test case generation (Technical Achievement 55).

OFFIS, KTH, **VOLVO** and others have worked within the ARTEMIS Project CESAR, on a common meta-model extending the approaches of SPEEDS and ATESST with the aim to combine several meta-models in a common framework (Technical Achievement 59).

Salzburg in collaboration with UC Berkeley began working on a higher-level, collaborative flight control system for the Salzburg helicopter platform (Technical Achievement 31).

Salzburg, in collaboration with the University of Porto, UC Berkeley, Trento and **IST** explored the fully compositional semantics of HTL defined in year 1 with respect to language modularity (Technical Achievement 33).

Uni. Trento and UC Berkeley worked on the development of design frameworks for complex systems ranging from automobiles, buildings and airplanes to systems on chip. A new framework that evolved from Metropolis, Metro II, was also applied to the design of a UMTS system (see achievement.35)

VERIMAG worked on source-to-source architecture transformation, this work bridges the gap between component-based and corresponding monolithic programming. We have continued working on this topic by taking into account architectural constraints (Technical Achievement 44).

VERIMAG has continued working on a general framework for **contract-based reasoning** allowing circular reasoning and proposed some instances of it (Technical Achievement 47).

VERIMAG has continued to work on distributed BIP, which complements already existing work on translating BIP with multiparty interaction and distributed BIP, the sublanguage encompassing only asynchronous message passing (Technical Achievement 62).

Sub-activity B (Resource Modeling)

CEA aimed at exploring the possibility to model resources using MARTE and account for this modeling within analysis-aware processes. This work has been concretized into a tool called Optimum. This latter enable to use MARTE to model functional systems including their resources usages and to analyze this latter using schedulability analysis tools such MAST (Technical Achievement 2).

ESI addressed the large scale applicability of the Y-chart approach in an industrial context. Main problem is that the performance has to predict of large amounts (thousands) of concurrent tasks which are represented in some domain specific language. Also optimization is complicated for such large numbers of tasks (Technical Achievement 10).

ESI developed modeling and tooling support for design-space exploration (DSE) in the form of the Octopus DSE toolset. The toolset intends to leverage the strengths of existing analysis and DSE tools in a common framework, aiming at reuse of tools and modeling effort, and aiming at synergy between different analysis methods in DSE. The toolset is centered around an intermediate representation that follows the Y-chart paradigm (Technical Achievement 12).

IST Austria developed a flexible framework for cloud computing (Technical Achievement 54). **IST** Austria has pursued the work on transactional memory, a new paradigm for concurrent Programs (Technical Achievement 24).

Uni. Trento, Scuola di Sant'Anna, UC Berkeley, United Technology and General Motors developed modeling and design methodologies for automotive and smart building parameter selections where communication protocols, periods and task allocations are concurrently adjusted to optimize delays, reliability and extensibility of unified architectures (see achievement 61)

Uppsala worked on Multi-Core Scheduling, Expressiveness and Tractability of Real-Time Task Models, Combining Abstract Interpretation and Model Checking for Timing and Interference Analysis of Parallel Programs on Multi-Core. (Technical Achievements 41 - 43).

VERIMAG has continued the work on implementing prioritized global specifications on distributed platforms (Technical Achievement 45).

VERIMAG has started work on real-time modeling and implementation with BIP which relies on two models of a given application (Technical Achievement 63).

Sub-activity C (Quantitative Modeling)

CISS has – in an intense collaboration with ITU Copenhagen and INRIA Rennes – continued work towards a fully compositional specification theories for timed and stochastic systems, allowing specifications to be combined with respect to both structural (e.g. parallel composition) and logical operators (e.g. conjunction) (Technical Achievement 3). The work has additionally resulted in the tool ECDAR for compositional development of timed systems (Technical Achievements 3 and 64)

CISS has – partly in collaboration with LSV Cachan – worked on priced (or weighted) extensions of timed automata, allowing for analysis and optimization of a number of quantitative resource problems to be formulated in a natural way. The introduction *Energy Timed Automata and Games* has been introduced allowing for modeling of both the consumption as well as the harvesting of resources. Work on linearly and exponentially growing cost functions as well as multiple cost functions has been addressed. (See Technical Achievement 5)

CISS has -- partly in collaboration with LSV Cachan – worked on quantitative theories of executable systems, where Boolean verdicts are replaced by real-valued outcomes – e.g. Boolean-valued refinement relations are replaced by real-valued similarity metrics. In particular the relationship between metrics and notions of robustness has been addressed (See Technical Achievements 8 and 9).

CISS has worked on scenario-based verification of timed systems and on the use of timed automata for analyzing probabilistic durational properties (See Technical Achievements 8 and 9).

ESI investigated the modeling of complex applications, where a full model with all details is infeasible, but appropriate abstractions and a combination of suitable models have to be found (Technical Achievement 13).

INRIA has studied, partly with Aachen, stochastic and quantitative logics and contract frameworks (Technical Achievements 57, 58).

IST Austria, together with **CVF** and **VERIMAG**, continued to study probabilistic systems, in particular, synthesis in presence of a probabilistic environment, the role of randomness in games and the qualitative analysis of the partially-observable Markov decision processes (Technical Achievement 50, 51).

IST Austria, **CVF** and **ULB** developed analysis and synthesis methods for quantitative systems, represented as mean-payoff and energy automata (Technical Achievement 21).

IST Austria studied simulation distances as a way to capture a finer and more quantitative view of the relationship between boolean specifications and systems (Technical Achievement 49).

Uni. Trento, United Technologies and UC Berkeley developed quantitative communication models and synthesis methods for energy efficient buildings and systems on chip (Technical Achievement 60)

-- Changes wrt Y2 deliverable --

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

2. Summary of Activity Progress

2.1 Technical Achievements

1. EC3M, a component-based framework for model-based design of embedded systems (CEA)

xMARTE constitutes a major achievement of CEA in 2009. It is designed as a plug-in for Papyrus, and it provides support for MARTE-based modeling of real-time and embedded systems, as well as model-based execution of MARTE-based specifications. Model-based execution is supported via code generation. The code generation process is put into practice using eC3M (developed by CEA, available at www.ec3m.net), a generic tool chain for the generation of execution infrastructures for component-oriented specifications. eC3M is generic in the sense that it can be parameterized by design patterns, describing how a given component-oriented specification (such as the one defined in MARTE) must actually be realized (i.e., in terms of executable code). Here, the usage of eC3M therefore leverages on works presented last year from CEA (concerning the definition of a component-oriented realization pattern of MARTE's Real-Time Units). CEA has also started evaluating an alternative strategy for the execution of MARTE-based specification. The approach is based on model interpretation (as opposed to code generation), and it relies on a specialization of the UML Execution Model, which is currently being standardized by the OMG.

2. OPTIMUM, a model-based approach for software architectural evaluation against non-functional requirements (CEA)

In Year 1, we have defined and prototyped a first model-based analysis tool connected to the RT-Druid tool for performing scheduling analysis. The goal of this preliminary work was to conclude on the feasibility of this kind of approach. Because this step was a success, we decided to continue and defined this year a new architecture for our tool in order to be able to integrate different analysis tools and be able to combine their results. Today, the current version of our model-based analyzer tool is integrated in our modeling tool Papyrus (www.eclipse.org/papyrus). It consists of three parts: a generic part that drives the user to build well-formed models ready for analysis and to use MARTE profiles dedicated to scheduling analysis, and two other plug-ins that make the link respectively with the MAST tool and the RT-Druid tool. Both aforementioned tools are used here for performing the scheduling analysis of the previously mentioned MARTE model dedicated to scheduling analysis.

3. An Interface Theory for Timed Systems (CISS+INRIA)

A specification theory combines notions of specifications and implementations with a satisfaction relation, a refinement relation and a set of operators supporting stepwise design. We develop a complete specification framework for real-time systems using Timed I/O Automata as the specification formalism, with the semantics expressed in terms of Timed I/O Transition Systems. We provide constructs for refinement, consistency checking, logical and structural composition, and quotient of specifications—all indispensable ingredients of a compositional design methodology. The theory is implemented on top of an engine for timed games, and illustrated with a small case study.

We also present Ecdar a new tool for compositional design and verification of real time systems. 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 the scalability of the verification.

5. Exponentially Priced Timed Automata (CISS+LSV Cachan)
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 compute 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).

6. Abstracting Continuous Systems by Timed Automata and Timed Games (CISS)
The development of the method for abstracting dynamical systems by timed automata was initiated during the visit of Oded Maler at Aalborg University, August, 2009. With the aim of enabling automatic controller design for dynamical systems, we have proposed this year a method for abstracting control systems by timed game automata. 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.

8. Weighted Kripke Structures and Temporal Logics (CISS)
We extend 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 for 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.

9. Robustness for Timed Automata (CISS+LSV Cachan)
We report on a development within robust verification of timed automata, and its relation to quantification of correctness. As it has been pointed out in a series of papers [Puri98, De Wulf et.al.08] concerning robustness of timed automata, the classic semantics as defined by Alur and Dill, unfortunately does not relate well to real world applications. The reason is that this semantics is based on the assumption that clocks do not drift, and in general exhibit perfect precise behaviour, and that reactions are instantaneous and without delay. It is well-known that this is not a viable assumption of digital hardware clocks, and clearly, the fixed speed of CPUs means we cannot implement the infinitely precise behaviour of the semantics on existing hardware. With this in mind, it has been shown in [De Wulf et.al.08] that systems exist, which are not robust, i.e., where any (however small) imprecision in the reaction time, will admit behaviour, which is (only) avoided by the ideal semantics, meaning that any attempt to implement the model will fail to preserve all (safety) properties of the model. The inherent weakness of using the ideal semantics for verification of real-world systems has led to the investigation of alternative semantics such as the Almost-ASAP semantics. This semantics, which aims at establishing properties of models using more realistic assumptions, is captured by the robust verification paradigm, which allows a very strong notion of

correctness. Our contribution is a construction of robust timed automata, which to some extent circumvents the need for robust verification.

10. Performance Prediction and Optimization for High-Tech Embedded Control (ESI)

Embedded control is a key product technology differentiator for many of the high-tech industries. The strong increase in complexity of embedded control systems, combined with the occurrence of late changes in control requirements, results in many timing performance problems showing up only during the integration phase. This results in extremely costly design iterations, severely threatening the time-to-market and time-to-quality constraints. In the ESI Wings project, this integration problem is attacked systematically through the construction of formal models. The key approach is to separate the logic of the embedded control application from the execution platform on which it is deployed, following the Y-chart approach. Modeling patterns with standardized interfaces were developed for reasons of scalability and distributed and multi-domain model development. To allow large-scale applicability in an industrial context, domain-specific models have been developed to formalize the Y-chart applications, mappings and platforms. These domain-specific models are generated mostly automatically from the available design and configuration files. In turn, the formal models are generated by weaving the domain-specific models together. Through an approach combining simulation (with POOSL) with exhaustive computations (with SDF3), both stochastic and worst-case timing properties can be analyzed in tandem. The ESI Wings project has demonstrated the effectiveness of the performance prediction and optimization method by applying it to an execution platform for process control of a wafer scanner. The method has shown to support the analyses of the full platform on which more than 30000 concurrent tasks are deployed. The application of the method within ASML has resulted in more than a dozen improvement proposals. In addition, the method is planned to become an integral platform facility for performance prediction and optimization.

12. Model-driven Design-space Exploration (ESI)

Several ongoing activities are aiming at developing model-driven design-space exploration (DSE) support for embedded systems, following up on the activities done over the last two years. We are working with dataflow, Petri nets, and timed automata, targeting multi-objective trade-off analysis, simulation, and schedule optimization, respectively. We have integrated CPNTools (Petri nets), Uppaal (timed automata), and SDF3 (dataflow) into a design-space exploration framework, called Octopus. The framework is centered around the intermediate representation DSEIR (DSE Intermediate Representation) that follows the Y-chart paradigm. DSEIR and the translations from DSEIR models to the analysis tools allow static task-to-resource bindings and dynamic resource allocation (pre-emption, bus throttling). All model transformations are fully automated. The analysis and simulation speed for the automatically generated models is similar to, and sometimes even better than, the analysis and simulation speed for handcrafted models. Modelling efforts are reduced substantially, because models need to be made only once, and models are guaranteed to be consistent between tools. Initially the toolset targets professional printers, but it is intended to be retargetable to other embedded systems. More information about the Octopus toolset can be found in [BBG+2010] and through http://dse.esi.nl.

13. Behavior modeling for complex software-intensive systems (ESI)

A simple simulator concept has been developed in the Falcon project. This concept is based on autonomous objects traveling over a system topology. The concept was used to model an existing retail warehouse. The results showed that the simulator, which can be configured within days, had the same performance as the existing detailed simulation, which took many weeks. Moreover, the running time of the new simulation concept (less than a minute) is much smaller than that of the existing detailed simulation (hours). This allows the new concept to be used for design-space exploration and sensitivity analysis.

In the Multiform project, a first prototype of a design framework has been realized, intended to support system architects in industry in their main process, i.e., developing systems. It is a generic, but highly extendible framework that aims at minimizing overhead in terms of additional tasks to be done, and at the same time maximizes the benefits in terms of keeping oversight of the process, the views on the system, and the collection of models that have been made to answer certain design issues. Conflict detection and parameter-based exploration are some of the main features of the design framework. It is going to be tested in a number of companies, starting with Vanderlande, followed by ASML.

In collaboration with Vanderlande, a number of design models and performance models were made in order to study different aspects of a system under development. Preliminary results indicate that the two types of models could be connected at a cost that may be well under control, and which coupling would lead to a higher degree of consistency in the development process.

Together with the University of Delft it has been studied how systems architecting can be supported by system modeling in such a way that the different architectural views are connected through different models containing shared components. Such a unified model scheme leads to the possibility of supporting reasoning in design space whilst suggesting alternative solutions. This work is being based on case studies within Océ which have not been completed yet.

In the Care4Me project, an executable architectural model has been made of a global healthcare cycle using the POOSL language. By means of simulation, it has been validated that the architecture supports a number of use cases for medical innovations. Related work has been done in the Darwin project, where a new patient communications system of an MRI scanner was modeled to validate the requirements. Furthermore, from the models, a supervisory controller was derived that realized the requirements while having other desirable properties like liveliness and being deadlock free. Moreover, we have modeled the cooling system of an MRI scanner family. Many variation points, such as the number of gradient amplifiers and the number of receive channels, exist in the family. Still, the low-end members of the family have to be cost-effective, and hence cannot be over-dimensioned. To obtain an appropriate solution, many different models were made, ranging from behavioral to thermal models and from functional decompositions to physical models. These models have been validated by measurements on an actual MRI scanner.

14. A Modal Interface Theory for Component-based Design (INRIA + Trento)

Complex systems are built by combining subsystems possessing dissimilar alphabets for referencing ports and variables. It is thus important to properly handle those different alphabets when combining interfaces (via product, conjunction or quotient). In [RBBCLP'10] locality is addressed as a fundamental requirement in interface-based design. The approach developed relies on alphabet equalization operations, where modalities play a crucial role. The paper [RBBCLP'10] also addresses some considerations about architectural design, namely "component-centric" design vs. "viewpoint-centric" design.

15. A Compositional Approach on Modal Specifications for Timed System (INRIA)

During Y2, INRIA defined a timed extension of modal specifications and built, for the subclass of modal event-clock automata, an entire interface theory for real time systems with conjunction, product, and quotient. It thus promoted efficient incremental design techniques and enabled us to reason in a compositional way about timed system. This theory is now surveyed in [BLPR'10]. New results on how to extend our past results to interfaces with arbitrary resets of clocks are also presented.

21. Quantitative analysis and synthesis (IST Austria + CVF + ULB)

Quantitative languages are an extension of boolean languages that assign, to each word, a real number. Mean-payoff automata are finite automata with numerical weights on transitions that assign, to each infinite path, the long-run average of the transition weights. We introduce in [CDEH+10] a new class of quantitative languages, defined by mean-payoff automaton expressions, which is robust and decidable: it is closed under the four pointwise operations, and we show that all decision problems are decidable for this class. Mean-payoff automaton expressions subsume deterministic mean-payoff automata, and we show that they have expressive power incomparable to nondeterministic and alternating mean-payoff automata. We also present, for the first time, an algorithm to compute the distance between two quantitative languages, and in our case the quantitative languages are given as mean-payoff automaton expressions. In mean-payoff games, the objective of the protagonist is to ensure that the limit average of an infinite sequence of numeric weights is nonnegative. In energy games, the objective is to ensure that the running sum of weights is always nonnegative. We study in [CDHR10] generalized mean-payoff and energy games that replace individual weights by tuples, and the limit average (resp. running sum) of each coordinate must be (resp. remain) nonnegative. These games have applications in the synthesis of resource-bounded processes with multiple resources. We prove the finite-memory determinacy of generalized energy games and show the inter-reducibility of generalized mean-payoff and energy games for finite-memory strategies.

23. Robust Synthesis in Presence of Liveness (IST Austria + VERIMAG + TU Graz)

Current verification and synthesis approaches consider the functional correctness of a system as a Boolean question: either the specification is fulfilled, or it is not. This approach is unsatisfactory in many situations. In particular, many specifications consist of environment assumptions and system guarantees. For such specifications, the classical approach does not impose any restrictions on the behavior of the system when the environment assumptions are not fulfilled. We believe that systems ought to behave reasonably even in circumstances that are not anticipated in their specifications, as reported in Deliverable 5-(3.1)-Y2. We propose a definition of robustness for liveness specifications which prescribes, for any number of environment assumptions that are violated, a minimal number of system guarantees that must still be fulfilled. This notion of robustness can be formulated and realized using a Generalized Reactivity formula. We present an algorithm for synthesizing robust systems from such formulas. This work is the continuation of our study of robust synthesis of systems that was presented in Deliverable 5-(3.1)-Y2, and was published in [BCG+10].

24. Transactional Memories (IST Austria and EPFL)

In [GHKS10], we have proposed a correctness condition for transactional memories (TMs), parameterized opacity, to formally capture the now folklore notion of strong atomicity by stipulating the two following intuitive requirements: first, every transaction appears as if it is executed instantaneously with respect to other transactions and non-transactional operations, and second, non-transactional operations conform to the given underlying memory model. We investigate the inherent cost of implementing parameterized opacity. We first prove that parameterized opacity requires either instrumenting non-transactional operations (for most memory models) or writing to memory by transactions using potentially expensive read-modify-write instructions (such as compare-and-swap). Then, we show that for a class of practical relaxed memory models, parameterized opacity can indeed be implemented with constant-time instrumentation of non-transactional writes and no instrumentation of non-transactional reads. We show that, in practice, parameterizing the notion of correctness allows the development of more efficient TM implementations.

27. Model-integration in embedded systems development and model evolution (KTH + Volvo)

Model-driven development provides a partial solution to dealing with the increasing complexity of embedded systems development, but it also introduces new challenges. Several models and views are used to describe an embedded system in different life cycle stages and from the viewpoints of the involved disciplines. To create the various models, a number of specialized development tools are used. These tools are usually disconnected, so the models cannot be transferred between different tools. Thus, models may become inconsistent, which hampers understandability of the models and increases the cost of development. We have proposed a model-based tool integration approach that uses a common meta model in combination with model transformation technology to build bridges between development tools. We have applied this approach in a case study and integrated several tools for automotive embedded systems development: A systems engineering tool, a safety engineering tool, and a simulation tool.

28. Automatic allocation of safety integrity levels to components (**KTH + Volvo**)
A concept has been developed for the automatic allocation of general Safety Integrity Levels (SILs) to subsystems and components of complex hierarchical networked architectures that deliver sets of safety critical functions. The concept is generic and can be adapted to facilitate the safety engineering approach defined in several standards that employ the concept of integrity or assurance levels including ISO 26262, the emerging automotive safety standard. SIL allocation is facilitated by HiPHOPS, an automated safety analysis tool, and can be performed in the context of development using EAST-ADL2, an automotive architecture description language. The process rationalizes complex risk allocation and leads to optimal/economic allocation of SILs.

29. Adding precise semantics to the EAST-ADL2 architecture description language to support formal analysis (**KTH + Volvo**)
KTH, in cooperation with Volvo has developed a behavior extension to the EAST-ADL2 language. This extension enhances the behavior modeling capability of EAST-ADL2, so that the model is precise and susceptible to the SPIN model checker. An algorithm was provided to convert (transform) an EAST-ADL2 behavior model to a SPIN model. The corresponding paper was awarded a best paper award at the IEEE. Conference on Mechatronics and Automation, August 4-7, 2010.

30. Model-based Safety Engineering of Interdependent Functions (KTH and Volvo)
For systems where functions are distributed but share support for computation, communication, environment sensing, and actuation, it is essential to understand how such functions can affect each other. Preliminary Hazard Analysis (PHA) is the task through which safety requirements are established. This is usually a document-based process where each system function is analyzed alone, making it difficult to reason about the commonalities of related functional concepts and the distribution of safety mechanisms across a system-of-systems. This work explored a model-based approach to PHA with the EAST-ADL2 language and in accordance with the ISO/DIS 26262 functional safety standard.
The language explicitly supports the definition and handling of requirements, functions and technical solutions, and their various relations and constraints as a coherent whole with multiple views. We have shown in particular the engineering needs for a systematic approach to PHA and the related language features for precise modeling of requirements, management of functions and their interdependencies, and the reasoning of safety mechanisms.

31. Cyber-Physical Cloud Computing (Salzburg + UC Berkeley)
Salzburg, in collaboration with UC Berkeley, continued working on a higher-level, collaborative flight control system for the Salzburg helicopter platform. The goal is to enable scalable multi-vehicle, multi-user, and multi-mission control. The approach is to deploy virtualized versions of vehicles operating on possibly fewer, heterogeneous real vehicles. Vehicle virtualization enables information-acquisition-as-a-service of cyber-physical rather than traditional cloud computing.

33. Runtime Programming (Salzburg + **U. Porto)**
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. We have used HTL in a case study. The idea of runtime programming is to run two programs, one of which implements the actual application and the other supervising 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.

35. Platform-Based Design and Frameworks: Metropolis and Metro II (Uni. Trento, UC Berkeley, UTC, National Instruments and Intel)

System-Level Design (SLD) means many different things to many different people. In our view, system-level design is about the design of a whole that consists of several components where specifications are given in terms of functionality with additional:

- constraints on the properties the design has to satisfy and on the components that are available for implementation and
- objective functions that express the desirable features of the design when completed.

This contribution was about principles and how a unified methodology together with a supporting software framework, as challenging as it may seem, can be developed to bring the embedded electronics industry to a new level of efficiency. We developed Metropolis, a software framework supporting the methodology and Metro II, a second generation framework built to alleviate the problems we encountered when applying Metropolis to industrial test cases. We continued the work by applying the framework and the corresponding methodology in several diverse domains: semiconductor chips (a UMTS single-chip design), energy efficient buildings (an indoor air quality control system), and synthetic biology.

36. COSI: A Modeling and Design Framework for Communication Design (Trento and United Technologies Corporation)

COSI (Communication Synthesis Infrastructure) is a software framework for interconnecting infrastructure modeling, analysis and synthesis. It is depicted in Figure 1.

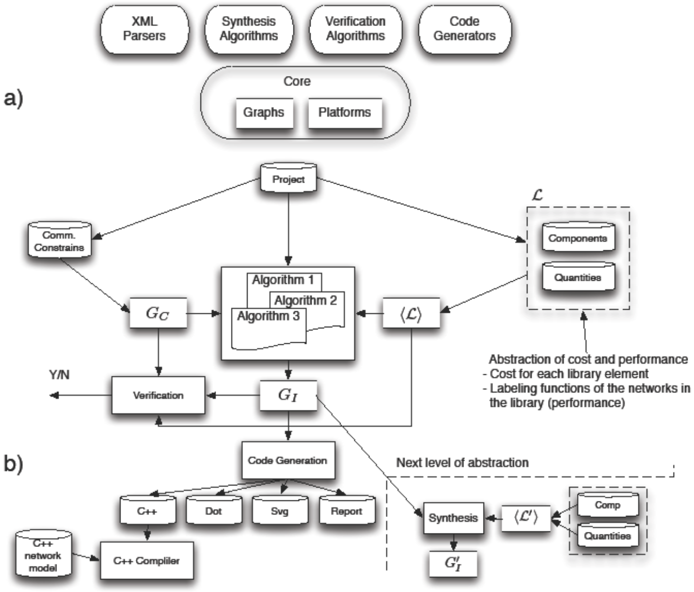
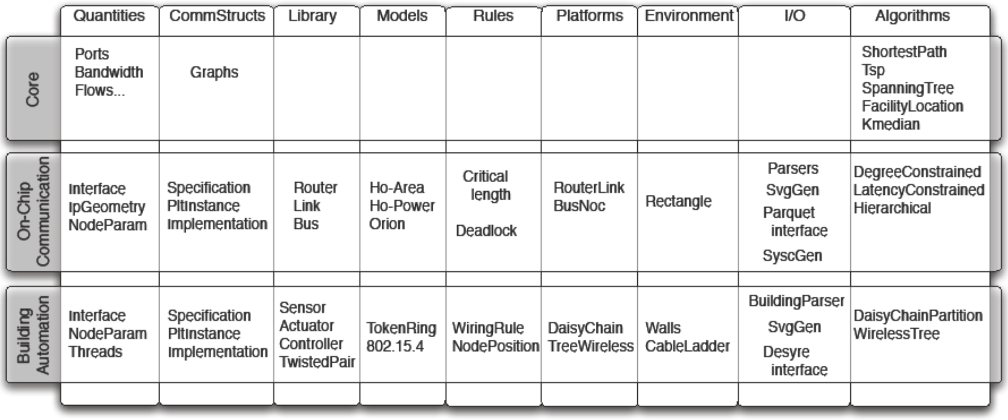


Figure 1. The COSI Platform-Based Design-like structure

The COSI framework allows the development of specialized flows and tools for communication synthesis, as exemplified by the release of COSI-NOC (Communication Synthesis Infrastructure for Network-on-Chips), a software toolkit for the automatic synthesis of synchronous networks-on-chip based on the platform-based design paradigm, and by COSI-BAD, for building automation design (see Figure 2).



	Quantities	CommStructs	Library	Models	Rules	Platforms	Environment	I/O	Algorithms
Core	Ports Bandwidth Flows...	Graphs							ShortestPath Tsp SpanningTree FacilityLocation Kmedian
On-Chip Communication	Interface IpGeometry NodeParam	Specification PltInstance Implementation	Router Link Bus	Ho-Area Ho-Power Orion	Critical length Deadlock	RouterLink BusNoc	Rectangle	Parsers SvgGen Parquet interface SyscGen	DegreeConstrained LatencyConstrained Hierarchical
Building Automation	Interface NodeParam Threads	Specification PltInstance Implementation	Sensor Actuator Controller TwistedPair	TokenRing 802.15.4	WiringRule NodePosition	DaisyChain TreeWireless	Walls CableLadder	BuildingParser SvgGen Desyre interface	DaisyChainPartition WirelessTree

Figure 2. Use of COSI framework to generate specific synthesis tools.

We have continued to work towards expanding COSI capabilities, including better models for router delays, bus models, and support for the generation of synthesizable RTL description of the synthesized on-chip interconnection network. In this domain, we are integrating Metro II with COSI. Meanwhile, we also plan to continue our work on the extension of the communication synthesis approach to the design of large-scale network for distributed embedded systems, such as avionics systems including autonomous vehicles.

40. Optimizations of an application-level protocol for enhanced dependability in FlexRay (Uni Trento, UC Berkeley, and GM)

FlexRay is an automotive standard for high-speed and reliable communication that is being widely deployed for next generation cars. The protocol has powerful error detection mechanisms, but its error-management scheme forces a corrupted frame to be dropped without any notification to the transmitter. In [ZNGZSV10], we analyze the feasibility of and proposed an optimization approach for an application-level acknowledgment and retransmission scheme, for which transmission time is allocated on top of an existing schedule. We formulated the problem as a Mixed Integer Linear Programming one. The optimization consists of two stages. The first stage optimizes a fault tolerance metric; the second improves scheduling by minimizing the latencies of the acknowledgment and retransmission messages. We demonstrated the effectiveness of our approach on a case study based on an experimental vehicle designed at General Motors.

41. 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. We have improved 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 have shown that the feasibility problem on preemptive single-processor systems remains tractable. This even holds in the case of task systems with arbitrary deadlines.

42. Combining Abstract Interpretation with Model Checking for Timing Analysis of Multi-core Software (Uppsala)

We have studied a multi-core 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 TA. 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 multi-core timing analysis, which allows the automatic generation of the TA models from binary code and the 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.

43. Fixed-Priority Multiprocessor Scheduling: Beyond Liu & Layland Utilization Bound (Uppsala)

The increasing interests in multi-cores 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. We have solved this open problem for most parametric utilization bounds by proposing new partitioning-based scheduling algorithms. As the second technical contribution, we have shown 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.

44. Source-to-Source Transformations in BIP: Integrating Architectural Constraints in Application (VERIMAG, ETHZ):

Performance of embedded applications strongly depends on features of the hardware platform on which they are deployed. A grand challenge in complex embedded systems design is developing methods and tools for modeling and analyzing the behavior of an application software running on a given hardware architecture. There exist performance evaluation techniques applied on very abstract system models. DOL provides system level performance analysis based on formal analysis techniques using Real Time Calculus. It also offers multi-objective mapping and optimizations. The proposed methodology in BIP provides a global system model, which is analyzable by using formal methods, and which faithfully characterizes the behavior of a mixed hardware/software system from a model of its software application and a model of its underlying hardware architecture. The methodology consists of a sequence of translations and transformations as it is illustrated in Figure 3. Firstly, we consider an input specification in DOL that consists of a description of the software application, a description of the hardware architecture, and a mapping of the software application to the given hardware architecture. Secondly, we translate the software application into an equivalent BIP software model. This model is to be simulated and checked for functional correctness. Thirdly, we specify the mapping and we integrate into the BIP software model the BIP System components and the performance observers. The integration is realized through a sequence of correct-by-construction transformations, guaranteeing the functional equivalence and integrating non-functional architectural properties. The generated system model can be analyzed by the BIP tool chain, as following:

1. Code generation for simulation/validation on a real platform.
2. Functional correctness using the D-Finder tool, checking for deadlocks.
3. Further transformations for code generation that uses send/receive primitives, for execution on distributed architectures.
4. Optimal analysis of delay bounds, based on simulation and statistical model checking facility integrated with BIP.

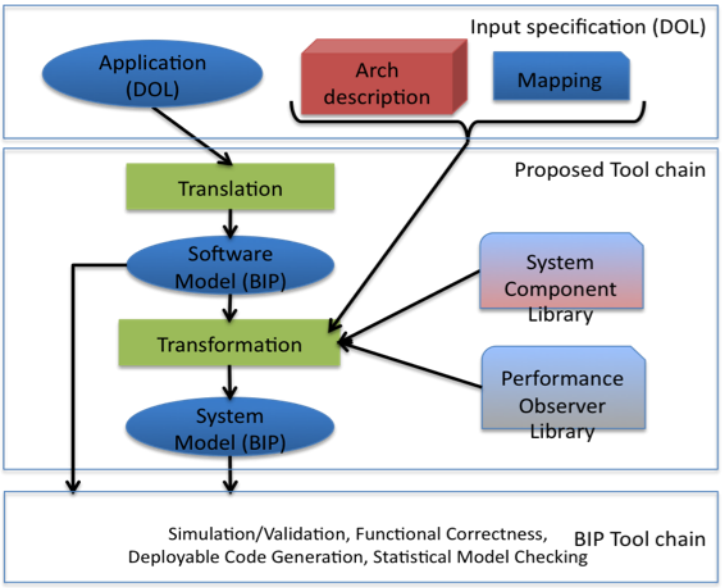


Figure 3. DOL to System - BIP Method

A key point in the proposed tool chain is the development of a tool that translates DOL application to BIP software model. The translation is completely automatic and supports complex DOL applications producing a synthesizable BIP model. Each process of the KPN is directly translated into a BIP component, while each software channel is modeled by using a predefined BIP component. The connections are modeled by BIP connectors. Although the translation to BIP is straightforward, it is not trivial. An important part of the procedure we follow is the translation of the C/C++ code. To achieve this, we assume a subset of the C/C++ language which should restrict the use of global variables, “goto” statements, multiple return statements and declarations placed not at the start of the executable code.

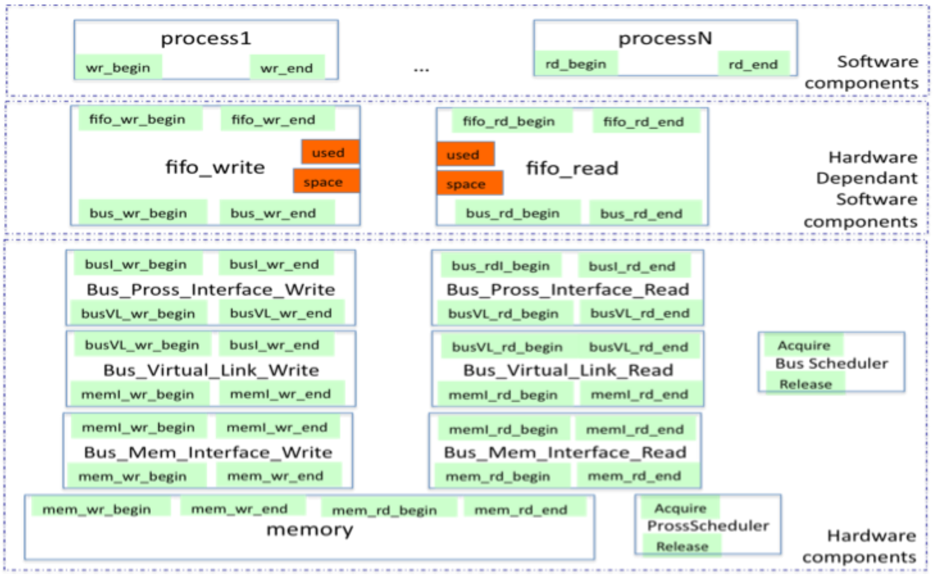


Figure 4. BIP Atomic Components Library

The construction of the BIP System model uses a set of generic components provided as a library of system components listed in Figure 4. The generation of the mixed hardware / software system considers the application software, the description of the hardware architecture, and the mapping. The method is completely automated and supported by tools. The system model is obtained by refining the application software model and composing it with the hardware architecture model. The composition is defined by the mapping.

The final system model is not an ad-hoc model. It is obtained by a series of low-level BIP source-2-source transformations which transform the initial BIP software model. They transform the system by modifying the BIP atomic component behavior, the BIP connectors, and the instantiation of the BIP System model which is enriched with the system library components. The transformations are guaranteed to provide a correct-by-construction result and to introduce no deadlocks.

The generated system model contains components in 3 layers: a) hardware layer, containing the processor, the memory, and the bus (architecture specification), b) software layer (process network) and c) hardware dependant software components which glue layers (a) and (b) together. Properties such as total delay, computational delay and processor idle time, communication overhead, bus and memory conflict can be measured with the deployment of performance observers [BBB*10,BBB*10a].

45. Distributing priorities (VERIMAG)

In a distributed system, it can be quite nontrivial to implement distributed communication; for example, once one process decides that it is willing to communicate with a second process, this communication might not be available anymore, as the second process has meanwhile communicated with a third process. For this reason, concurrent programming languages may restrict the choice of communication. For example, Hoare has initially restricted his programming language CSP to commit to a single output, where choice is allowed between inputs.

The use of a "synchronizing" communication model and priorities is an abstract, yet powerful, means for expressing memoryless controllers of distributed systems. For efficiency reasons, one wants to avoid the use of a centralized global controller. We have studied different approaches for distributing such a controller.

One approach considered the use of "knowledge" that can be constructed using verification techniques (reachability analysis) and used by local components to decide whether to execute some interaction and which one, if more than one of them is locally enabled. In [BPS10], we compute such knowledge by using an algorithm similar to one suggested by Van der Meyden. This analysis checks which processes possess "knowledge" about having a maximal priority transition enabled at the current state. This knowledge is then used as a basis for producing a new program without priorities, which implements (or at least approximates) the prioritized behavior of the original program. This transformation does not introduce any new executions or deadlocks and preserves the linear temporal logic properties, but it allows the choice of unfair executions. We have proposed an optimization by computing the knowledge from the controlled rather than the uncontrolled system [BBJ*10].

We have also developed a method combining knowledge and message passing [GPQ10], where we provide an algorithm that computes an optimal communication strategy for collecting sufficient knowledge to take a decision about whether or which next step to execute. Here, we try to minimize the number of processes required to obtain the information required.

We have also considered an implementation based on message passing which does not minimizes, as usually, the number of messages, but privileges short sequences of message exchanges. This algorithm handles some forms of confusion (and ignores others) and it also handles arbitrary conflicts [BQG10, BGK10].

47. Contract-based verification for rich interaction models (Verimag and Trento):

We have continued the work on a general notion of contract framework that we had started in year 1. A contract-framework is defined on top of a component framework and defines 3 related notions of refinement: ***conformance*** is refinement between closed components (that is properties, e.g., the closed system defined by a contract), ***dominance*** is refinement between contracts, and ***satisfaction*** is refinement under context and relates a component and a contract. This year, we have provided more reasoning rules for dominance, handling multiple contracts on one hand, and component frameworks with weaker properties on the other hand.

In the context of the SPEEDS project, we have used and refined the general framework for contract-based reasoning developed in Year 1. We had made some proposals for the expression of proper encapsulation in BIP and had given a proof rule for dominance in the resulting framework. We have generalized the contract-related concepts defined in HRC and achieved a notion of contract framework that has the notion of composition as an explicit parameter. We have shown, for several existing contract and interface theories, that they can be considered as instances of this general framework. In particular, we have provided special reasoning rules for proofs provided by verification engines based on different verification tools using possibly different notions of refinement (work submitted for publication)

49. Simulation Distances (IST Austria)

Standard verification systems return a Boolean answer that indicates whether a system satisfies its specification. However, not all correct implementations are equally good, and not all incorrect implementations are equally bad. It is a natural question whether it is possible to extend the standard specification frameworks and verification algorithms to capture a finer and more quantitative view of the relationship between boolean specifications and systems. Intuitively, a system which behaves undesirably repeatedly is worse than a system that behaves undesirably once. It is valid to ask if this notion can be quantified. Another instance where a quantitative measure of system desirableness is necessary is to compare the robustness of various implementations. During Year 3, we have captured these measures of system behaviors using directed distances between systems as a generalization of the simulation preorder.

We have extended the notion of simulation to the quantitative setting. We have extended the simulation preorder to a distance function that, given two systems, returns a real-valued distance between them. In the 2-player simulation game used for computing the simulation relation, we allow each player to “cheat". However, each player pays a certain price for “cheating". By varying the nature of “cheating" and the costs, we are able to capture various notions of desirability of systems. For example, allowing the specification player to cheat by taking erroneous transitions allows us to compute the degree of correctness of implementations. We have been able to compute various other system properties, like coverage and robustness, by using other schemes of cheating. These three simulation distances were presented in [CHR10a]. Two case studies have been treated which showthat the error tolerance of error correction systems and the degree of environment restrictions imposed by an implementation of a reactive system can be computed using the robustness and coverage distances respectively.

The simulation preorder helps in the analysis of large systems thanks to its properties (compositionality, transitivity, etc.). In [CHR10b], we examined the analogous properties for the simulation distances. We were able to show the quantitative version of transitivity (triangle inequality) for all three distances. In addition, the correctness and coverage distances are directed metrics as the distance they assign from a system to itself is zero. Also, we were able to show that all three metrics are well-behaved with respect to abstraction and composition.

50. Systems in Probabilistic Environments (IST Austria + VERIMAG + IIT Bombay)

Often, one has a preference order among the different systems that satisfy a given specification. Under a probabilistic assumption about the possible inputs, such a preference order is naturally expressed by a weighted automaton, which assigns to each word a value, such that a system is preferred if it generates a higher expected value. We have solved the following optimal-synthesis problem: given an omega-regular specification, a Markov chain that describes the distribution of inputs, and a weighted automaton that measures how well a system satisfies the given specification under the given input assumption, synthesize a system that optimizes the measured value. For safety specifications and measures that are defined by mean-payoff automata, the optimal-synthesis problem amounts to finding a strategy in a Markov decision process (MDP) that is optimal for a long-run average reward objective, which can be done in polynomial time. For general omega-regular specifications, the solution rests on a new, polynomial-time algorithm for computing optimal strategies in MDPs with mean-payoff parity objectives. We have presented some experimental results showing optimal systems that were automatically generated in this way. This work was published in [CHJS10] and the algorithms were implemented in the tool QuaSy.

51. Qualitative Analysis of Partially-observable Markov Decision Processes (IST Austria + CVF)

We have studied in [CDH10] observation-based strategies for partially-observable Markov decision processes (POMDPs) with omega-regular objectives. An observation-based strategy relies on partial information about the history of a play, namely, on the past sequence of observations. We consider the qualitative analysis problem: given a POMDP with an omega-regular objective, whether there is an observation-based strategy to achieve the objective with probability ~1 (almost-sure winning), or with positive probability (positive winning). Our main results are twofold. First, we present a complete picture of the computational complexity of the qualitative analysis of POMDPs with parity objectives (a canonical form to express omega-regular objectives) and its subclasses. Our contribution consists in establishing several upper and lower bounds that were not known in literature. Second, we present optimal bounds (matching upper and lower bounds) on the memory required by pure and randomized observation-based strategies for the qualitative analysis of POMDPs with parity objectives and its subclasses.

52. Randomness in Games (IST Austria + CVF + LaBRI)

We study in [CDGH10] two-player zero-sum games on graphs. These games can be classified on the basis of the information of the players and on the mode of interaction between them. On the basis of information, the classification is as follows: (a) partial-observation (both players have partial view of the game); (b) one-sided complete-observation (one player has complete observation); and (c) complete-observation (both players have complete view of the game). On the basis of mode of interaction, we have the following classification: (a) concurrent (both players interact simultaneously); and (b) turn-based (both players interact in turn). The two sources of randomness in these games are randomness in transition function and randomness in strategies. In general, randomized strategies are more powerful than deterministic strategies, and randomness in transitions gives more general classes of games. We have proposed a complete characterization for the classes of games where randomness is not helpful in: (a) the transition function probabilistic transition can be simulated by deterministic transition; and (b) strategies (pure strategies are as powerful as randomized strategies). As consequence of our characterization, we have obtained new undecidability results for these games.

53. Parity Games (IST Austria + EPFL + UC Santa Cruz)

We have studied two player concurrent games played on a finite state space for an infinite number of rounds. In each round, the two players choose their moves independently and simultaneously; the current state and the two moves determine the successor state. We consider winning conditions specified as parity objectives on the resulting infinite state sequence. We first consider timed parity games, where each player, together with an action, also chooses a time delay. We present an efficient reduction of these games to turn-based (i.e., non-concurrent) finite-state (i.e., untimed) parity games. The states of the resulting game are pairs of clock regions of the original game. Our reduction improves the best known complexity for solving timed parity games. Additionally, we consider two restricted classes of strategies for the player that represents the controller in a real-time synthesis problem, namely, limit-robust and bounded-robust strategies. Using a limit-robust strategy, the controller cannot choose an exact real-valued time delay but must allow for some non-zero jitter in each of its actions. If there is a given lower bound on the jitter, then the strategy is bounded-robust. We provide algorithms for the synthesis of robust real-time controllers [CHP10]. Secondly, we have studied qualitative concurrent parity games where both players are allowed to use randomization when choosing their moves. We study the computation of the limit-winning set of states, consisting of the states where player 1 can ensure a probability of winning arbitrarily close to 1. We show in particular that, although they have the same complexity, our algorithms are considerably more involved than those for turn-based games. This is because concurrent games violate two of the most fundamental properties of turn-based parity games. First, in concurrent games limit-winning strategies require randomization; and second, they require infinite memory [CdAH10].

54. Cloud computing (IST Austria)

We have studied and developed in [HSS+10a,HSS+10b] a flexible framework for cloud computing, which is called FlexPRICE (Flexible Provisioning of Resources in a Cloud Environment) and works as follows. A user presents a job to the cloud. The cloud finds different schedules to execute the job and presents a set of quotes to the user in terms of price and duration for the execution. The user then chooses a particular quote and the cloud is obliged to execute the job according to the chosen quote. FlexPRICE thus hides the complexity of the actual scheduling decisions from the user, but still provides enough flexibility to meet the users' actual demands. We implemented FlexPRICE in a simulator called PRICES that allows us to experiment with our framework. We observe that FlexPRICE provides a wide range of execution options —from fast and expensive to slow and cheap— for the whole spectrum of data-intensive and computation-intensive jobs. We also observe that the set of quotes computed by FlexPRICE do not vary as the number of simultaneous jobs increases.

55. Model-implemented fault injection to simulate the effect of hardware-related faults in embedded systems (KTH and SP)

In work at SP in Sweden in cooperation with KTH (as part of the Mogentes project), modeling libraries and hardware fault abstractions together with a tool was developed to support model-based fault-injection. The fault injection environment enables the comparison of experiments at model level and hardware level using Simulink and a microcontroller respectively. Experiments at model level, leading to safety requirement violations, are automatically repeated at hardware level to compare the fault effects.

Artifacts in a Simulink model (e.g., block output ports) are automatically mapped to memory addresses obtained from a linker generated map. Thus, the same variable can be manipulated by the fault injection environment at both model and hardware level. For the automotive application evaluated, experiments show that the effects of data errors at model level and hardware level are similar excluding the experiments leading to exceptions.

56. An approach towards capturing design decisions through model transformations (KTH)

Models do not remain static, but they change over time and evolve. KTH investigated support for various aspects of model evolution. When models are changed, the design decisions and the justification for the change are usually neither captured nor documented in a systematic way. As a result, important information about the model is lost, making the model more difficult to understand, which hampers model evolution and maintenance.

To support model evolution, design decisions need to be captured explicitly using an appropriate representation. This representation reduces the overhead of capturing design decisions, keeps the model and the design decision documentation consistent, and links the design decision documentation to the model. As a result, the captured design decisions provide a record of the model evolution and the rationale of the evolution.

57. Generalization of Constraint Markov Chains with non-determinism (INRIA + Aachen)

In [CDLLPW10], we proposed Constraint Markov Chain (CMC), a new specification theory for Markov Chains (MC). This new model permits rich constraints on probability distributions and thus generalizes prior abstractions such as Interval MCs. This is the first specification theory for MCs with such closure properties. In a very recent effort (in collaboration with Joost-Pieter Katoen), our CMC theory was generalized to also handle non-determinism. The new model, which we call Abstract Probabilistic Automata (APA), is a specification theory for Markov Decision Processes. Alternative models of timed and stochastic interfaces have also been considered.

58. Quantitative Logics and probabilistic contracts (INRIA)

Temporal logic is two-valued: a property is either true or false. When applied to the analysis of stochastic systems, or systems with imprecise formal models, temporal logic is therefore fragile: even small changes in the model can lead to opposite truth values for a specification. In 2004, de Alfaro has proposed DCTL, a quantitative version of CTL. The logic has been extended for the case of transitions systems, Markov Chains, and Markov Decision Processes. Together with David Jansen (who visited INRIA Rennes), Axel Legay has extended the logic to continuous timed Markov Chains.

In the same direction, we have defined a probabilistic contract framework for describing and analyzing component-based embedded systems, based on the theory of Interactive Markov Chains (IMC). A contract specifies the assumptions a component makes on its context and the guarantees it provides. Probabilistic transitions allow for uncertainty in the component behavior, e.g., to model observed black-box behavior (internal choice) or reliability. An interaction model specifies how components interact. We provide the ingredients for a component-based design flow, including (1) contract satisfaction and refinement, (2) parallel composition of contracts over disjoint, interacting components, and (3) conjunction of contracts describing different requirements over the same component. Compositional design is enabled by congruence of refinement [XGG10].

59. A common meta-model approach supporting interoperability of models and tools (OFFIS, KTH, Volvo)

In the ARTEMIS project CESAR, a common meta-model that should improve data handling in embedded system engineering projects with heterogeneous tool and model environments is currently under development. This common meta-model is compliant to existing standards such as UML / SysML and is based on recent meta-models like HRC (developed within the SPEEDS project) and EAST-ADL2 (developed within ATESST).

When developing an embedded system various modeling tools and models based on different meta-models are used along the development process. Such tools and meta-models support process steps like requirement elicitation, structural component design, simulation, analysis techniques etc. During the development process, model information has to be exchanged and traceability between a heterogeneous set of artifacts from various models is required. Since in general the meta-models of the respective tools are different, it is needed to perform transformation techniques to address artifacts in other models. Creating transformations between a large set of meta-models means high effort which costs time and money. Furthermore, it is not always possible to transform one model completely into another.

Having *one* meta-model covering every element from every meta-model is an intuitive solution to provide data interoperability between tools. But this is not the right approach. Having a common meta-model is a solution which provides a view to address common concepts and artifacts on various abstraction levels with different viewpoints from such a heterogeneous set of meta-models used in a development process.

For the usage of a common meta-model in the context of various heterogeneous meta-models, common concepts have to be identified in the respective meta-models. During the identification process, for each meta-model, a mapping to the common meta-model is defined. In such a mapping table, meta-model artifacts and relationships are mapped to those defined in the common meta-model. The result is a projection of a set of elements of the regarded meta-models to a set of elements of the common meta-model. A mapping between meta-models and the common-meta model can be used in several ways. Since the common-model provides generic concepts, elements of the common-meta-model can generalize mapped elements of other meta-models. Such generalizations allow addressing elements of foreign meta-models based on elements of the common meta-model. Furthermore, based on the mapping, transformations can be created which translate instances of other meta-models into an instance of the common meta-model.

The usage of a common meta-model for tool interoperation can be different. It is considerable to use a common meta-model as an exchange format, as a native format of tools, i.e., for analysis techniques or for common understanding of elements from different kinds of models and as a common model data interface. A common view on a heterogeneous set of model artifacts from different kinds of models can be compared to the view provided by file navigation tools. When connecting several tools with different meta-models, the common meta-model provides a common view on elements of instances of different meta-models.

The common meta-model approach is evaluated in the CESAR project in scenarios of various industrial partners from different domains such as avionics, automotive and rail. In one scenario, structural models defined in EAST-ADL2 and HRC contracts defining requirements on the structural models were connected using the common meta-model approach. A mapping between EAST-ADL2 structure and HRC components as well as EAST-ADL Requirements and HRC contracts was defined and a transformation description was created using QVT (Query/View/Transformation).

60. Moving from Federated to Integrated Architectures in Automotive: The Role of Standards, Methods and Tools (Scuola di Sant'Anna, University of California at Berkeley, Trento)

Cost pressure, flexibility, extensibility and the need for coping with increased functional complexity are changing the fundamental paradigms for the definition of automotive and aeronautics architectures. Traditional designs are based on the concept of a Federated Architecture in which integrated hardware/software components [Electronic Control Units (ECUs)] realize mostly independent or loosely interconnected functions. These components are connected by bus and cooperate by exchanging messages. This paradigm is now being replaced by the Integrated Architecture (the concept comes from Integrated Modular Avionics (IMA) introduced by the avionics community (see C. B. Watkins and R. Walter, Transitioning from federated avionics architectures to integrated modular avionics, in Proc. 26th Digital Avionics Syst. Conf., Oct. 2007) but it is certainly general and applicable to other fields and in particular, automotive, in which software components can be supplied from multiple sources, integrated on the same hardware platform or physically distributed and possibly moved from one CPU to another without loss of functional and time correctness, and providing a guaranteed level of reliability. This shift will decouple software design from the hardware platform design and provide opportunities for the optimization of the architecture configuration, increased extensibility, flexibility and modularity. However, the integration of software components in a distributed system realizing a complex functional behavior and characterized by safety, time and reliability constraints requires a much tighter control on the component model and its semantics, new methods and tools for analyzing the results of the composition, whether by simulation or formal methods, and methods for exploring the architecture solution space and optimizing the configuration.

In [NSV10], an invited paper in a special issue of the Proceedings of the IEEE on Automotive Software, we have provided a general overview of existing challenges and possible solutions to the design and analysis problem, with special focus on the automotive domain. The development of such methods and tools must necessarily consider the compatibility with existing modeling languages and standards, including UML, AUTOSAR and synchronous reactive models, on which the widely used commercial products Simulink and SCADE are based.

61. A Design Flow for Building Design Automation (Berkeley+Trento+UTC+Intel)

The building stock in the US accounts for 40% of total energy consumption and 70% of electricity consumption. Limits on carbon emissions are driving new regulations that will require buildings to be energy efficient according to standards that are likely to be more stringent than the ASHRAE 90.1. The design of low energy buildings – zero energy in the ideal case – is challenging but not impossible. There are today examples of zero energy buildings, but they are the results of ad-hoc designs that are not easy to generalize.

The design methodology used today for large buildings is top-down. Different sub-systems (e.g., mechanical and electrical) are designed in isolation by domain experts following design documents flown down after the bid process. This methodology is not suitable for low energy buildings that require interaction among architects, mechanical engineers and control engineers. Consider for instance adopting low energy solutions such as natural ventilation and active facade. In this case, the architectural design (e.g., the building orientation), the design of the mechanical equipment of the HVAC system and the design of the control algorithms cannot be done in isolation. In this new context, the design of the building automation system (i.e., the embedded processors and networks supporting the building operations, and the software running on them) is non-trivial. Control algorithms become multi-input, multi-output, hybrid and predictive, as opposed to single-input single-output controllers coordinated by simple switching conditions as today (and mainly dictated by standards). Moreover, several sub-systems such as HVAC, lighting, vertical transportation and fire and security will interact through the network to allow information sharing.

In [YPSVZ10], we have focused on a design flow for building automation systems, which bridges the gap between a desirable design entry point – at a high abstraction level using model-based design tools such as Simulink – and the available back-end tools able to generate low-level code.

It enables the integration of models from different high-level languages, allowing the interaction between domain experts. Furthermore, it automatically optimizes the implementation of the control algorithms on a distributed platform by selecting computation and communication resources, and by performing code generation while meeting the specification.

62. Distributed BIP (Verimag)

We have investigated and implemented methods for generating efficient distributed implementations from BIP and related models [BBJ*10a, BBJ*10b].

To generate distributed implementations from BIP models, it is necessary to transform these models into S/R-BIP models. These are a subclass of models where multi-party interaction is replaced by protocols using S/R (Send/Receive) primitives. Then, from the S/R-BIP models and a mapping of atomic components into the processing elements of a platform, it is possible to generate efficient C/C++ or MPI-code.

The method uses the following sequence of correct-by-construction transformations, which preserve observational equivalence:

1. Given a user-defined partition of its interactions, a BIP system model is transformed into an S/R-BIP system model such that (i) atomicity of transitions in the original model is broken by separating interaction and computation, and (ii) multi-party interactions of the source model are replaced by protocols using send/receive primitives. Moreover, the target S/R-BIP model is structured in three layers:
   a. The *component layer* consists of the atomic components in the original model, where each port involved in strong interactions is replaced by a pair of corresponding S/R ports.
   b. The *interaction protocol layer* consists of a set of components, each managing a class of interactions of the partition. This protocol detects the enabledness of interactions, and executes them after resolving conflicts either locally or assisted by the third layer.
   c. The *conflict resolution protocol layer* resolves conflicts requested by the interaction protocol layer. This protocol resolves a committee coordination problem using one distributed algorithm amongst (i) fully centralized, (ii) token-ring, and (iii) dining philosophers.
2. We generate from the obtained 3-layer S/R-BIP model and a mapping of its atomic components on processors, either an MPI program, or a set of plain C/C++ programs that use TCP/IP communication. The generation consists in statically composing atomic components running on the same processor to obtain a single observationally equivalent component, and consequently reduced coordination overhead at runtime.

We have conducted a set of experiments in [BBJ+10a,BBJ+10b] to analyze the behavior and performance of the generated code using different scenarios (i.e., different partitioning of interactions, choice of committee coordination algorithm, mapping). Experimental results allow performance estimation for different partitions of the interactions and different mappings.

For example, the following table (taken from [BBJ+10a]) shows results obtained for different distributed implementations of a bitonic sorting algorithm. It reports the total sorting time for different implementations (handwritten or generated, with or without optimization) deployed on different execution platforms (*m* x *c* denotes *m* interconnected machines with *c* cores each) on unsorted arrays of *k* x 10^4 elements.

	MPI (handwritten)			Plain C/C++ with TCP/IP (generated)				MPI (generated)	
Optimized				no	No	yes	No	no	Yes
m x *c*	1 x 1	2 x 2	4 x 1	1 x 1	2 x 2	2 x 2	4 x 1	2 x 2	2 x 2
k=20	80	14	14	96	23	24	24	63	24
k=40	327	59	60	375	96	96	100	271	96
k=60	1368	240	240	1504	390	391	397	964	394
k=80	5605	1007	958	6024	1539	1548	1583	4158	1554

63. Real-Time BIP (Verimag)

Verimag had developed a model-based implementation method for real-time applications in BIP relying on two models of the application. The *abstract model* is based on timed automata. It takes into account platform-independent timing constraints expressing user requirements. The actions of the abstract model are assumed to be timeless. We also had introduced the notion of *physical model*, which describes the behavior of the abstract model when it is executed on a target platform. It is obtained from the abstract model by assigning execution times to its actions. Under some time-robustness assumption for WCET, the Real-Time Engine implementing this method respects the semantics of the abstract model. We improved this method in two directions [ACS10].

We first improved the real-time scheduling policy used by the Real-Time Engine. This policy is based on earliest deadline first (EDF). The Real-Time Engine associates to each enabled interaction, a timing constraint (i.e., a time interval and an urgency type: lazy, delayable or eager) computed from the timing constraints associated to the corresponding transitions of the atomic components. Interactions are chosen according to the deadlines computed from their timing constraint. The problem with this approach is that deadlines are computed considering only transitions that can be executed at the next step, i.e., using a single step planning horizon mechanism. We improved our scheduling policy by using the following principle: if an interaction ***I1*** precedes another interaction ***I2*** and ***I2*** has a deadline ***D2***, then ***I1*** should be also completed before ***D2***. This principle has been applied both at the level of transitions (inside atomic components) and at the level of interactions. We implemented a prototype that performs the backward propagation of timing constraints for each timed automaton (i.e., for each atomic component). We are also working on algorithms for timing constraints propagation between those atomic components.

We also introduced the notion of environment ports in BIP models. They allow a clean description and implementation of the interactions of a BIP model with its execution environment. The execution environment can be, for instance, the physical environment, the hardware platform, or another software application running on the platform but not written in BIP. An environment port is implicitly associated to events coming from the environment. Transitions of an atomic component labeled by an environment port require the presence of an event to be executed. In the proposed implementation of the Real-Time Engine, the *Event Handler* is responsible for updating the status of environment ports depending on the presence of events. Updating the events is achieved by drivers that are the interfaces between the *Engine* and the environment. Waiting for new events can be implemented in the *Drivers* using techniques such as active waits, processes signals, or interruptions. Experimental results on a robot application implemented in BIP show that using environment ports drastically increases the reactivity of the application with respect to its environment. Moreover, the CPU usage has been also reduced due to the fact that active waits in the model have been replaced by simple transitions involving environment ports.

64. Interface Theories for Probabilistic Systems (CISS+INRIA+Aachen)

Notions of specification, implementation, satisfaction, and refinement, together with operators supporting stepwise design, constitute a specification theory. We have built 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 have studied its relation to simpler operators for known languages such as probabilistic process algebra. Despite the generality, all operators and relations are computable.

Probabilistic Automata (PAs) are a widely-recognized mathematical framework for the specification and analysis of systems with non-deterministic and stochastic behaviours using a novel abstraction model for PAs. In PAs, 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 have also proposed the first specification theory for them. Our theory supports both satisfaction and refinement operators, together with classical stepwise design operators. In addition, we have studied the link between specification theories and abstraction in avoiding the state-space explosion problem.

65. Scenario-based verification of real-time systems using UPPAAL (CISS)

We have proposed 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 have provided timed extensions to a kernel subset of the LSC language and have defined 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 TA modeled 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 have shown how to 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 have carried 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.

66. Durational Probabilistic Automata (VERIMAG+CISS+CMU)

We have proposed 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 have studied duration probabilistic automata (DPA), expressing multiple parallel processes admitting memoryful continuously distributed durations. For this model, we have developed 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).

-- Changes wrt Y2 deliverable --

This is new text, not present in Y2 deliverables. We have kept the numbering scheme from last year: items with number below 48 are continuations of earlier work, items with higher numbers correspond to new work lines, and missing number to lines of work on which no new progress has been achieved this year

2.2 Individual Publications Resulting from these Achievements

CEA

[BCTTBG10] A. Benyahia, A. Cuccuru, S. Taha, F. Terrier, F. Boulanger and S. Gérard, "Extending the Standard Execution Model of UML for Real-Time Systems", in Proceedings of the 7th IFIP Conference on Distributed and Parallel Embedded Systems (DIPES 2010), Brisbane, Australia, September 20-23, 2010.

[BDTTF10] M. Brun, J. Delatour, Y. Trinquet, F. Thomas and S. Gérard, "Étude comparative pour la modélisation de plates-formes d'exécution: Application au temps réel embarqué", Technique et Science Informatiques, Hermès Science, volume 29, 2010.

[CRGT10] W. E. H. Chehade, A. Radermacher, S. Gérard and F. Terrier, "Detailed Real-time Software Platform Modeling", in Proceedings of the 17th Asia Pacific Software Engineering Conference (APSEC 2010), Sydney, Australia, 30 November - 3 December, 2010.

[CRCGT10] W. E. H. Chehade, A. Radermacher, A. Cuccuru, S. Gérard and F. Terrier, "Automating the Generation of Platform Specific Models," in Proceedings of the 15th IEEE International Conference on Engineering of Complex Computer Systems, IEEE Computer Society, pp. 383-388, St. Anne's College, University of Oxford, 2010.

[CRCGT10] W. E. H. Chehade, A. Radermacher, A. Cuccuru, S. Gérard and F. Terrier, "Automating the Generation of Platform Specific Models," in Proceedings of the 15th IEEE International Conference on Engineering of Complex Computer Systems, IEEE Computer Society, pp. 383-388, St. Anne's College, University of Oxford, 2010.

[FRGT10] M. Fredj, A. Radermacher, S. Gérard, F. Terrier, A Developer-Oriented View of Component-Based Embedded Systems, in Proceedings of 36th EUROMICRO Conference on Software Engineering and Advanced Applications (SEAA 2010), Lille, France, September, 2010

[GETTGNS10] S. Gérard, H. Espinoza, F. Terrier, F. Tufo, G. Gentille, M. Di Natale and B. Selic, "Modeling Languages for Real-time and Embedded Systems: Requirements and Standards-Based Solutions", chapter of book MBEERTS, Springer, LNCS Volume 6100, 2010.

[RMTG10] A. Radermacher, C. Mraidha, S. Tucci-Piergiovanni and S.Gérard, Generation of Schedulable Real-Time Component Implementations, 15th IEEE International Conference EFTA'2010, Bilbao, Spain, September 13-16, 2010 .

CISS

[LLNP10] 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.

[SW10] Christoffer Sloth and Rafael Wisniewski. Proofs for an abstraction of continuous dynamical systems utilizing Lyapunov functions. arXiv:1008.3222, 2010.

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

ESI

[BBG+2010] T. Basten, E. van Benthum, M. Geilen, M. Hendriks, F. Houben, G. Igna, F. Reckers, S. de Smet. L. Somers, E. Teeselink, N. Trcka, F. Vaandrager, J. Verriet, M. Voorhoeve, Y. Yang. Model-Driven Design-Space Exploration for Embedded Systems: The Octopus Toolset. In T. Margaria and B. Steffen, editors, 4th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation, ISoLA 2010, Proceedings, Part I, pages 90-105. Heraclion, Crete, 18-20 October 2010. Lecture Notes in Computer Science 6415. 2010.

[LH10] L. Li and J. Hooman: Connecting Technical and Non-Technical Views of System Architectures. In the proceedings of the 3rd IEEE/ACM International Conference on Cyber, Physical and Social Computing (CPSCom2010), 2010

[PGB2010] P. Poplavko, M. Geilen, T. Basten. Predicting the Throughput of Multiprocessor Applications under Dynamic Workload. In 28th International Conference of Computer Design, ICCD 2010, Proceedings, pages 282-288. Amsterdam, Netherlands, 3-6 October 2010. IEEE Computer Society Press, Los Alamitos, CA, USA, 2010.

[SGB2010] S. Stuijk, M.C.W. Geilen, T. Basten. A Predictable Multiprocessor Design Flow for Streaming Applications with Dynamic Behaviour. In Digital System Design, 13th EUROMICRO Conference, DSD 2010, Proceedings, pages 548-555. Lille, France, 1-3 September 2010. IEEE Computer Society Press, Los Alamitos, CA, USA, 2010.

[VFH+10] J. Voeten, O. Florescu, J. Huang and H. Corporaal. Error Computation for Predictable Real-Time Software Synthesis. TIn: Simulation - Transactions of the Society for Modeling and Simulation International, March 12, Simulation OnlineFirst, 2010

[WBG+2010] M. Wiggers, M.J.G. Bekooij, M.C.W. Geilen, T. Basten. Simultaneous Budget and Buffer Size Computation for Throughput-Constrained Task Graphs. In Design, Automation and Test in Europe, DATE 2010, Proceedings, pages 1669-1672. Dresden, Germany, 8-12 March, 2010. IEEE, 2010.

[XTL+10] J. Xing, B Theelen, R. Langerak, J. van de Pol, J. Tretmans and J. Voeten. (2010). UPPAAL in Practice: Quantitative Verification of a RapidIO Network. In: ISoLA 2010 - 4th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation, 18-20 Oct 2010, Amirandes, Heraclion, Crete. MNCS 6416, pp. 160-174, 2010. Springer-Verlag, Berlin-Heidelberg, 2010

[XTR+10] J. Xing, B. Theelen, R. Langerak, J. van de Pol, J. Tretmans and J. Voeten. From POOSL to UPPAAL: Transformation and Quantitative Analysis. In: Proceedings of the International Conference on Application of Concurrency to System Design (ACSD), pp. 47-56, ISBN 978-0-7695-4066-5, IEEE Computer Society, 2010.

[YGB+2010] Y. Yang, M.C.W. Geilen, T. Basten, S. Stuijk, H. Corporaal. Automated Bottleneck-Driven Design-Space Exploration of Media Processing Systems. In Design, Automation and Test in Europe, DATE 2010, Proceedings, pages 1041-1046. Dresden, Germany, 8-12 March, 2010. IEEE, 2010.

INRIA

[BLPR'10] N. Bertrand, A. Legay, S. Pinchinat and J.-B. Raclet. Modal event-clock specifications for timed component-based design. Submitted to an international journal.

[XGG10] D. Xu, G. Goessler, and A. Girault. Probabilistic Contracts for Component-Based Design. In 8th International Symposium on Automated Technology for Verification and Analysis (ATVA'10). Pp 325-340, vol 6252 of LNCS, Springer Verlag. Singapore, September 2010.

IST

[CHR10a] P. Cerny, T. Henzinger, and A. Radhakrishna. Quantitative simulation games. In Essays in Memory of Amir Pnueli, pages 42-60, 2010.

[CHR10b] P. Cerny, T. Henzinger, and A. Radhakrishna. Simulation distances. In CONCUR, pages 253-268, 2010.

[HSS+10a] Thomas A. Henzinger, Anmol V. Singh, Vasu Singh, Thomas Wies, and Damien Zufferey, “FlexPrice: Flexible provisioning of resources in a cloud environment," Proceedings of the Third International Conference on Cloud Computing (CLOUD), IEEE Computer Society Press, 2010.

[HSS+10b] Thomas A. Henzinger, Anmol V. Singh, Vasu Singh, Thomas Wies, and Damien Zufferey, “A marketplace for cloud resources," Proceedings of the Tenth Annual Conference on Embedded Software (EMSOFT), ACM Press, 2010.

KTH

[BDT*10] 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.

[Bie10] Matthias Biehl. Supporting Model Evolution in Model-Driven Development of Automotive Embedded Systems. Licentiate thesis - ISBN 978-91-7415-723-9, Royal Institute of Technology, Stockholm, Sweden, November 2010.

[Bie10a] Matthias Biehl. Documenting Stepwise Model Refinement using Executable Design Decisions. Proceedings of the International Workshop on Models and Evolution (ME 2010), October 3 2010, Oslo, Norway

[BT10] Matthias Biehl and Martin Törngren. An Executable Design Decision Representation using Model Transformations. 36th EUROMICRO Conference on Software Engineering and Advanced Applications (SEAA2010), September 1-3 2010, IEEE, Lille, France

[QDT10] Qamar A., During C., Wikander J., Torngren M. Integrating multi-domain models for the design and development of mechatronic systems. EuSEC 2010 - 7th bi-annual European Systems Engineering Conf. May 23-26, 2010, Stockholm.

OFFIS

[Bau10] Andreas Baumgart: A common meta-model for the interoperation of tools with heterogeneous data models; ECMFA 2010 - 3rd Workshop on Model-Driven Tool & Process Integration.

[BRR*10] A. Baumgart, P. Reinkemeier, A. Rettberg, I. Stierand, E. Thaden, R. Weber: A Model-Based Design Methodology with Contracts to Enhance the Development Process of Safety-Critical Systems; The 8th IFIP Workshop on Software Technologies for Future Embedded and Ubiquitous Systems (SEUS 2010)

Salzburg

[KLMS10] C.M. Kirsch, L. Lopes, E.R.B. Marques, and A. Sokolova. Runtime Programming through Model-Preserving, Scalable Runtime Patches. Technical Report 2010-08, Department of Computer Sciences, University of Salzburg. December, 2010.

[CHKPRRSTLS10] S.S. Craciunas, A. Haas, C.M. Kirsch, H. Payer, H. Roeck, A. Rottmann, A. Sokolova, R. Trummer, J. Love, and R. Sengupta. Information-Acquisition-as-a-Service for Cyber-Physical Cloud Computing. Proc. Workshop on Hot Topics in Cloud Computing (HotCloud). USENIX, 2010.

Trento

[CPV*10] Daniela Cancila, Roberto Passerone, Tullio Vardanega, Marco Panunzio: Ensuring Correctness in the Specification and Handling of Non-Functional Attributes in High-Integrity Real-Time Embedded Systems. IEEE Trans. Industrial Informatics 5(2): 181-194 (2010)

[NSV10] M. Di Natale and A. Sangiovanni Vincentelli, Moving from Federated to Integrated Architectures in Automotive: The Role of Standards, Methods and Tools, *Proceedings of the IEEE*, Volume 98, n. 4, pp. 603-620, April 2010, Invited Paper

[NGGSVZS10] M. Di Natale, A. Ghosal, P. Giusto, A. Sangiovanni-Vincentelli, H. Zeng and S. Seshia, Special Issue on Automotive Embedded Systems, Guest Editorial, Volume 2, n. 2*, IEEE Embedded Systems Letters*, pp. 21-23, June 2010

[ZNGSV10] Haibo Zeng, Marco Di Natale, Paolo Giusto, and Alberto Sangiovanni - Vincentelli. Using Statistical Methods to Compute the Probability Distribution of Message Response Time in Controller Area Network *IEEE Transactions on Industrial Informatics*, Special Issue on Real-Time and (Networked) Embedded Systems (TII),Volume 6,N. 4, pp.621-636,November 2010.

[ZZZNSV10] Qi Zhu, Haibo Zeng, Wei Zheng, Marco Di Natale, and Alberto Sangiovanni-Vincentelli. Optimization of Task Allocation and Priority Assignment in Hard Real-time Distributed Systems. *ACM Transactions in Embedded Computing Systems (TECS*), special issue on the Synthesis of Cyber-Physical Systems, 2010.

[ZNGZSV10] Haibo Zeng, Marco Di Natale, Arkadeb Ghosal, Wei Zheng, and Alberto Sangiovanni-Vincentelli. Schedule Optimization of Time-Triggered Systems Communicating over the FlexRay Static Segment. *IEEE Transactions on Industrial Informatics* (TII) 2010.

[ZNGSV10] H. Zeng, M. Di Natale, P. Giusto and A. Sangiovanni Vincentelli, Using Statistical Methods to Compute the Probability Distribution of Message Response Time in Controller Area Networks, *IEEE Transactions on Industrial Informatics* (TII) Volume 6,N. 4, pp.678-691,November 2010

[NGZSV10] Marco Di Natale, Liangpeng Guo, Haibo Zeng, and Alberto Sangiovanni-Vincentelli. Synthesis of Multi-task Implementations of Simulink Models with Minimum *IEEE Transactions on Industrial Informatics* (TII) Volume 6,N. 4, pp.637-651,November 2010.

[ZYNSSV10] Q. Zhu, Y. Yang, M. Di Natale, E. Scholte and A. Sangiovanni-Vincentelli, Optimizing the Software Architecture for Extensibility in Hard Real-Time Distributed Systems, Delays *IEEE Transactions on Industrial Informatics* (TII) Volume 6,N. 4, pp.621-636,November 2010, Invited Paper.

[WNSV10] G. Wang, M. Di Natale and A. Sangiovanni Vincentelli, Optimal Synthesis of Communication Procedures in Real-Time Synchronous Reactive Models, Delays IEEE Transactions on Industrial Informatics (TII) Volume 6,N. 4, pp729-743,Nov, 2010

[MLVSV10] Mozumdar, M.M.R. Lavagno, L. Vanzago, L.Sangiovanni-Vincentelli, A.L., , HILAC: A framework for Hardware In the Loop simulation and multi-platform Automatic Code Generation of WSN Applications*, Proceedings of Symposium on Industrial Embedded Systems, pp. 88-97, July 2010*

[SV10a] Corsi e Ricorsi: Alberto Sangiovanni Vincentelli and the Birth of EDA, Solid-State Circuits Magazine, IEEE, Vol. 2, Issue:3 , Summer 2010.

[SV10b] Corsi e Ricorsi: Alberto Sangiovanni Vincentelli and the Evolution of EDA., Solid-State Circuits Magazine, IEEE, Vol. 2, Issue:4 , Fall 2010.

[DSDP09] D. Densmore, A. Simalatsar, A. Davare, R. Passerone, and A. Sangiovanni-Vincentelli. *UMTS MPSoC design evaluation using a system level design framework*. In Proceedings of the Conference on Design, Automation and Test in Europe (DATE09), Nice, France, April 20-24, 2009.

[NSWDBSV10] P. Nuzzo, X. Sun, C.-C. Wu, F. De Bernardinis, A. Sangiovanni-Vincentelli, “A Platform-Based Methodology for System-Level Mixed-Signal Design*,” Eurasip Journal of Embedded Systems*, vol. 2010, Article ID 261583, 2010.

[YPSVZ10] Yang Yang, Alessandro Pinto, Alberto Sangiovanni-Vincentelli, and Qi Zhu. A Design Flow for Building Automation and Control Systems*, Proceedings of the 31st IEEE Real-Time Systems Symposium*, pp. 105-116, December 2010.

Uppsala

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

[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.

[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.

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

[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.

VERIMAG

[ACS10] T. Abdellatif, J. Combaz and J. Sifakis. Model-Based Implementation of Real-Time Applications. In Proceedings of the 10th ACM International Conference on Embedded Software (EMSOFT 2010) Scottsdale, Arizona, USA.

[BBB*10] A. Basu, S. Bensalem, P. Bourgos, M. Bozga and J. Sifakis. Integrating Architectural Constraints in Application Software by Using Model Transformations in BIP. IEEE International High-Level Design Validation and Test Workshop Collocated with DAC 2010, Anaheim, California, June 10-12, 2010

[BBB*10a] P. Bourgos, A. Basu, S. Bensalem, K. Huang, J. Sifakis. Integrating Architectural Constraints in Application Software by Source-to-Source Transformation in BIP. Verimag Research Report.

[BBBS10] Ananda Basu, Borzoo Bonakdarpour, Marius Bozga, Joseph Sifakis: Systematic Correct Construction of Self-stabilizing Systems: A Case Study. SSS 2010: 4-18

[BBJ*10] Saddek Bensalem, Marius Bozga, Susanne Graf, Doron Peled, Sophie Quinton: Methods for Knowledge Based Controlling of Distributed Systems. ATVA 2010: 52-66

[BBJ+10a] B. Bonakdarpour, M. Bozga, M. Jaber, J. Quilbeuf, J. Sifakis : Automated Conflict free Distributed Implementation of Component-Based Models. In Proceedings of Intl. Symposium on Industrial Embedded Systems, SIES'10, July 2010.

[BBJ+10b] B. Bonakdarpour, M. Bozga, M. Jaber, J. Quilbeuf and J. Sifakis: From High Level Component-Based Models to Distributed Implementation. In Proceedings of Intl. Conference on Embedded Software, EMSOFT'10, October 2010.

[BGK10] Imene Ben Hafaiedh, Susanne Graf, Hammadi Khairallah: Implementing Distributed Controllers for Systems with Priorities FOCLASA 2010: 31-46

[BPS10] Saddek Bensalem, Doron Peled, Joseph Sifakis: Knowledge Based Scheduling of Distributed Systems. Essays in Memory of Amir Pnueli 2010: 26-41

[BGQ10] Imene Ben Hafaiedh, Susanne Graf, Sophie Quinton: Reasoning about Safety and Progress Using Contracts. ICFEM 2010: 436-451

[GPQ10] Susanne Graf, Doron Peled, Sophie Quinton: Achieving Distributed Control through Model Checking. CAV 2010: 396-409

[MJS10] Marius Bozga, Mohamad Jaber, Joseph Sifakis: Source-to-Source Architecture Transformation for Performance Optimization in BIP. IEEE Trans. Industrial Informatics 5(4): 708-718 (2010)

-- Changes wrt Y2 deliverable --

This is new text, not present in Y2 deliverables.

2.3 Interaction and Building Excellence between Partners

CEA + VOLVO: within ATESST2, its continuation MAENAD, and ADAMS an action support for the dissemination of MARTE, both are collaborating on modeling automotive system with EAST-ADL in the context of other standards such as MARTE, SysML and AUTOSAR.

ESI + KTH Twan Basten acted as opponent in the defense of Jun Zhu from KTH for his Licentiate degree. Prof. Dr. Ir. Twan Basten is guest editor, together with Prof. Dr. Rolf Ernst of TU Braunschweig, for the special issue of ACM Transactions in Embedded Computing Systems (TECS). This special issue was initiated during the 2nd Artist Workshop on Models of Computation and Communication, held in Eindhoven, July 3-4, 2008. Submission for the special issue was open to everyone and 32 papers were submitted. The review process is almost complete and the special issue is expected to appear in 2010.

ESI + TU Braunschweig. Prof. Dr. Ir. Twan Basten is guest editor, together with Prof. Dr. Rolf Ernst of TU Braunschweig, for the special issue of ACM Transactions in Embedded Computing Systems (TECS) on Model-driven Embedded System Design. This special issue was initiated during the 2nd Artist Workshop on Models of Computation and Communication, held in Eindhoven, July 3-4, 2008. Submission for the special issue was open to everyone and 32 papers were submitted. The review process is complete, 9 papers were accepted, and the special issue is scheduled to appear in December 2010.

CEA + KTH and Volvo : within the ATESST2 project (http://www.atesst.org) and its continuation MAENAD (www.maenad.eu) the partners are working on the further development of the EAST-ADL language, a UML-based extension for enabling full model-based design of automotive embedded systems.

INRIA + Aachen: Joost-Pieter Katoen (U. Aachen) visited INRIA Rennes to work with Axel Legay on the generalization of Constraint Markov Chains with non-determinism.

INRIA + Nijmegen: David Janssen (Radboud U. Nijmegen) visited INRIA Rennes to work with Axel Legay on quantitative logics. Temporal logic is two-valued: a property is either true or false. When applied to the analysis of stochastic systems, or systems with imprecise formal models, temporal logic is therefore fragile: even small changes in the model can lead to opposite truth values for a specification. de Alfaro has proposed DCTL that is a quantitative version of CTL. The logic has been extended for the case of transitions systems, Markov Chains, and Markov Decision Processes. Together with David Jansen, Axel Legay has extended the logic to continuous timed Markov Chains.

IST Austria + CVF are actively collaborating on quantitative and probabilistic analysis and synthesis of systems

IST Austria + VERIMAG are collaborating on the robust synthesis

IST Austria + INRIA are actively collaborating on further development of interface theories. This resulted in a visit of Dejan Nickovic from IST Austria to INRIA-Rennes and a visit of Benoit Delahaye from INRIA-Rennes to IST Austria.

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 Caillaud in Aalborg, as well as 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 includes work on robustness for timed automata.

CISS+Verimag have 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.

KTH + Volvo: Cooperation within both the ATESST2 and CESAR projects. This has also involved mobility of personnel. PhD Lei Feng has continued to work both at KTH and Volvo, acting as an industrial post-doc and bridge between Volvo and KTH.

KTH + CESAR partners (including EADS, Airbus, AVL, INRIA, CNRS, ABB and CRF): longer term work in defining the CESAR reference technology platform (https://cesarproject.eu/) including work towards a common meta-model (see technical achievement 59), tool interoperability (an extension of the work reported in technical achievement 27) and case studies.

INRIA + Trento: INRIA and the University of Trento have interacted on the topic of modal interfaces for component-based design.

Salzburg + IST Our work on virtualization technology 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.

Uni. Trento + Scuola Superiore di Sant'Anna have been collaborating for years on the development of a comprehensive approach to mapping of functional descriptions to computing architectures in collaboration with a number of industrial partners including GM, National Instruments and UTC.

Important interaction and collaborative work happens in collaborative research projects with participation of several cluster partners. Examples of such projects are

- **INRIA +OFFIS + Uni. Trento + VERIMAG** have been collaborating intensely in the SPEEDS project where for developing a modeling framework, a design methodology and system level validation techniques.
- In the COMBEST project, almost all partners of this cluster collaborate for developing a design theory for complex embedded systems, fully covering heterogeneity, interface specifications, composability, compositionality, and refinement for functional and extra-functional properties. In one line of work, **INRIA + IST + Uni. Trento** are together involved in further developing studies on *Interface Theories*. The objective is to allow for new services to be offered by such theories, in addition to substitutability that was offered from the beginning in original de Alfaro-Henzinger framework. **ETHZ** and **Verimag** continue collaborating on a connection between DOL and BIP.
- **CEA** and **KTH** collaborate in the ATESST and ATESST2 project.
- The ARTEMIS project CESAR is a platform project aiming at the integration and enhancement of techniques developed the French OpenEmBeDD, in ATESST2 and in SPEEDS, and gathers most cluster participants.

-- Changes wrt Y2 deliverable --

This is new text, not present in Y2 deliverables.

2.4 Joint Publications Resulting from these Achievements

[AJL*10] Andreas Abele, Rolf Johansson, Henrik Lönn, Yiannis Papadopoulos, Mark-Oliver Reiser, David Servat, Martin Törngren and Matthias Weber. The CVM Framework - A Prototype Tool for Compositional Variability Management. VAMOS'2010, 4th Int. Workshop on Variability Modelling of Software-intensive Systems, Linz, Austria, ICB report 37:101-108, ISSN 1860-2770

[BCG+10] Roderick Bloem, Krishnendu Chatterjee, Karin Greimel, Thomas A. Henzinger, Barbara Jobstmann: Robustness in the Presence of Liveness. CAV 2010: 410-424

[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.

[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] B. Caillaud, B. Delahaye, K.G. Larsen, A. Legay, M.L. Pedersen, and A. Wasowsk. Compositional Design Methodology with Constraint Markov Chains. In International Conference on Quantitative Evaluation of SysTems (QEST'10), Williamsburg, Virginia, USA, September 2010.

[CKSDLLLW11] Benoit Caillaud, Joost-Pieter Katoen, Falak Sher, Benoit Delahaye, Kim G. Larsen, Axel Legay, Mikkel Larsen Pedersen, and Andrzej Wasowski. Abstract probabilistic automata. In *Proceedings of 12th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI)*, 2011

[BJ10] Simon Bliudze, Joseph Sifakis: Causal semantics for the algebra of connectors. Formal Methods in System Design 36(2): 167-194 (2010)

[CdAH10] Krishnendu Chatterjee, Luca de Alfaro, and Thomas A. Henzinger, “Qualitative concurrent parity games," ACM Transactions on Computational Logic, in press.

[CDEH+10] Krishnendu Chatterjee, Laurent Doyen, Herbert Edelsbrunner, Thomas A. Henzinger, and Philippe Rannou, Mean-payoff automaton expressions," Proceedings of the 21st International Conference on Concurrency Theory (CONCUR), Lecture Notes in Computer Science 6269, Springer, 2010, pp. 269-283.

[CDGH10] Krishnendu Chatterjee, Laurent Doyen, Hugo Gimbert, and Thomas A. Henzinger, “Randomness for free," Proceedings of the 35th International Symposium on Mathematical Foundations of Computer Science (MFCS), Lecture Notes in Computer Science 6281, Springer, 2010, pp. 246-257.

[CDH10] Krishnendu Chatterjee, Laurent Doyen, and Thomas A. Henzinger, “Qualitative analysis of partially observable Markov decision processes," Proceedings of the 35th International Symposium on Mathematical Foundations of Computer Science (MFCS), Lecture Notes in Computer Science 6281, Springer, 2010, pp. 258-269.

[CDHR10] Krishnendu Chatterjee, Laurent Doyen, Thomas A. Henzinger, and Jean-Francois Raskin, Generalized mean-payoff and energy games," Proceedings of the 30th Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS), Lecture Notes in Computer Science, Springer, 2010.

[CHJS10] K. Chatterjee, T. A. Henzinger, B. Jobstmann, R. Singh: Measuring and Synthesizing Systems in Probabilistic Environments. CAV 2010: 380-395

[CHP10] Krishnendu Chatterjee, Thomas A. Henzinger, and Vinayak S. Prabhu, “Timed parity games: Complexity and robustness," Logical Methods in Computer Science, in press.

[CFJ*10] Philippe Cuenot, Patrik Frey, Rolf Johansson, Henrik Lönn, Yiannis Papadopoulos, Mark-Oliver Reiser, Anders Sandberg, David Servat, Ramin Tavakoli Kolagari, Martin Törngren, Matthias Weber (invited paper, under review). The EAST-ADL Architecture Description Language for Automotive Embedded Software. Invited chapter in the book Model-Based Engineering of Embedded Real-Time Systems. Holger Giese, Bernard Rumpe, Bernard Schätz (eds). LNCS 6100. 2010

[DLLNWb10] Alexandre David, Kim G. Larsen, Axel Legay, Ulrik Nyman, and Andrzej Wasowski. Timed i/o automata: a complete specification theory for real-time systems. In *Proceedings of the 13th ACM International Conference on Hybrid Systems: Computation and Control, HSCC 2010, Stockholm, Sweden, April 12-15, 2010*, pages 91–100, 2010

[DLLNWc10] 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

[DLNLW10] 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.

[GHKS10] Rachid Guerraoui, Thomas A. Henzinger, Michal Kapalka, and Vasu Singh, “Transactions in the jungle," Proceedings of the 22nd Annual Symposium on Parallel Algorithms and Architectures (SPAA), ACM Press, 2010, pp. 263-272.

[GIKHS10] A. Ghosal, D. Iercan, C.M. Kirsch, T.A. Henzinger, and A. Sangiovanni-Vincentelli. Separate Compilation of Hierarchical Real-Time Programs into Linear-bounded Embedded Machine Code. Science of Computer Programming, 2010.

[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

[PWR*10] Papadopoulos Y. Walker M., Reiser M-O, Weber M., Servat D., Abele A., Johansson R., Lonn H., Torngren M., Sandberg A. Automatic Allocation of Safety Integrity Levels, 8th European Dependable Computing Conference – CARS workshop, Valencia, Spain, April, ACM Publications, 2010.

[SCL*10] Anders Sandberg, DeJiu Chen, Henrik Lönn, Rolf Johansson, Lei Feng, Martin Törngren, Sandra Torchiaro, Ramin Tavakoli-Kolagari, Andreas Abele. Model-based Safety Engineering of Interdependent Functions in Automotive Vehicles Using EAST-ADL2. Safecomp 2010.

[SEV*10] 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).

[SVE*10] Rickard Svenningsson, Jonny Vinter, Henrik Eriksson, Martin Törngren. MODIFI: A MODel-Implemented Fault Injection Tool. Safecomp 2010.

-- Changes wrt Y2 deliverable --

This is new text, not present in Y2 deliverables.

2.5 Keynotes, Workshops, Tutorials

Keynote: Computational Models for Concurrent Streaming Applications
Twan Basten - ASCI Winterschool on Embedded Systems 2010, Soesterberg, Netherlands, Soesterberg, Netherlands*, 17 March 2010*
http://www.asci.tudelft.nl/pages/events.php?event_id=1

Keynote: Kahn Process Networks and a Reactive Extension
Twan Basten - IEEE Summer School on Models for Embedded Signal Processing Systems, Leiden, Netherlands, 1 September 2010
http://www.lorentzcenter.nl/lc/web/2010/427/info.php3?wsid=427

Keynote: ***Building tomorrow's systems with industry as a laboratory***
Michael Borth - ICT Delta 2010, Rotterdam, Netherlands, 18 March 2010

Keynote: Architecture of Systems-of-Systems
Michael Borth - ESI Symposium, Eindhoven, Netherlands, 2 December 2010

Keynote: Performance prediction and design-space exploration for wafer scanners
MMB & DFT 2010, Essen, Germany, March 15, 2010.

Keynote: Predicting timing performance of wafer scanners
Bits and chips conference, Eindhoven, The Netherlands, November 11, 2010.

Keynote: System Architecting & Modeling
Roelof Hamberg - ESI Symposium, Eindhoven, The Netherlands, December 2 2010

Keynote: Model based design
Roelof Hamberg - Special Interest Group (ASML, Océ, Vanderlande, Philips Healthcare, ESI), Eindhoven, April 28, 2010

Keynote*:* Linking Healthcare Architecture to Requirements
Jozef Hooman - Care4Me workshop, Barcelona, 6 October 2010

Keynote: Time predictability from system-level design to task implementations in automotive applications,
Paolo Gai, Marco Di Natale, Huascar Espinoza, Francois Terrier, Sébastien Gérard, Reinhold Heckmann, Christian Ferdinand, Giacomo Gentile and Nicola Ariotti
SAE 2010 World Congress & Exhibition within the session System Level Architecture Design Tools and Methods, Detroit, MI, USA, 2010.

Key Note: DATE 2010, Everything is Connected.
Alberto Sangiovanni Vincentelli Dresden, March 9, 2010
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
Alberto Sangiovanni Vincentelli Stockholm, April 14, 2010
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
Alberto Sangiovanni Vincentelli July 7th, 2010
http://events.unitn.it/en/sies2010

Key Note: Emerging Technologies and Factory Automation (ETFA) 2010, Distributed System Design: A Nightmare 'in fieri'
Alberto Sangiovanni Vincentelli ,Bilbao, September 14, 2010
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

Alberto Sangiovanni Vincentelli Las Vegas, September 27, 2010
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
Alberto Sangiovanni Vincentelli, *San Jose', September 24, 2010*
http://www.bmas-conf.org/program.html

Invited Lecture: Thomas A. Henzinger,
The Quantitative Agenda in System Analysis, First International Workshop on Logics for System Analysis (LfSA), Edinburgh, United Kingdom, July 2010.

Invited Lecture: Thomas A. Henzinger
From Boolean to Quantitative Theories of Reactive Systems, Third International Workshop on Interaction and Concurrency Experiences (ICE), Amsterdam, The Netherlands, June 2010.

Invited Lecture: Thomas A. Henzinger
Quantitative Modeling and Verification, Amir Pnueli Memorial Symposium, New York, New York, May 2010.

Invited Lecture: Thomas A. Henzinger
From Boolean to Quantitative Notions of Correctness, 37th Annual Symposium on Principles of Programming Languages (POPL), Madrid, Spain, January 2010.

Keynote: Thomas A. Henzinger
Weighted Automata on Infinite Words, Highlights of AutomathA Conference, Vienna, Austria, November 2010.

Keynote: Thomas A. Henzinger
A Marketplace for Cloud Resources, Embedded Systems Week, Scottsdale, Arizona, October 2010.

Invited Lecture: Thomas A. Henzinger
Beyond Finite Automata, Eighth International Symposium on Automated Technology for Verification and Analysis (ATVA), Singapore, September 2010.

Invited Tutorial: Thomas A. Henzinger
Interface-based Design and Verification, Eighth International Symposium on Automated Technology for Verification and Analysis (ATVA), Singapore, September 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, Edinburgh.

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

Invited Lecture: Alberto Sangiovanni Vincentelli
Research in Advanced Topics: Energy and Health,, Kick Off Meeting of the European Technology Institute for Information Technology, Trento, July 2010

Invited Lecture: Alberto Sangiovanni Vincentelli
Start-up and Innovations, Uni Roma 3, June 2010

Invited Lecture: Alberto Sangiovanni Vincentelli
How the Innovation System works in Silicon Valley, Italian National Research Council (CNR), October 2010.

Invited Lecture: Alberto Sangiovanni Vincentelli
Distributed System Design: A Nightmare Waiting to Happen, The Smith Distinguished Lecture, November 2010

Invited Lecture: *Multicore Embedded Systems: Challenges and Perspectives*
Wang Yi – the 12th International Conference on Formal Engineering Methods, Shanghai, Nov 16 - 19, 2010

Invited Lecture: *Modeling and Analysis of Timed Systems*
Wang Yi – Summer School on Model Checking, Chinese Academy of Sciences, Beijing, Oct. 2010.

Invited Lecture: *Model Checking of Real-Time Systems*
Wang Yi – VTSA School on Verification Technology, Systems and Applications, Luxembourg, Sept. 2010

Invited Lecture: *A UPPAAL Tutorial*
Wang Yi – 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

Invited Lecture: *Towards Real-time Applications on Multi-core Platforms: the Timing Problem and Possible Solutions*
Wang Yi – ARTIST Summer School, Europe 2010, Autrans, France, Sept. 2010

Invited Lecture: *Towards Real-time Applications on Multi-core Platforms: the Timing Problem and Possible Solutions*
Wang Yi – ARTIST Summer School, China 2010, Beijing, July 2010

Conference: The 8th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS 2010), IST Austria, Klosterneuburg, Austria
8-10 September 2010
Timing aspects of systems from a variety of computer science domains have been treated independently by different communities. Researchers interested in semantics, verification and performance analysis study models such as timed automata and timed Petri nets, the digital design community focuses on propagation and switching delays while designers of embedded controllers have to take account of the time taken by controllers to compute their responses after sampling the environment. Timing-related questions in these separate disciplines do have their particularities. However, there is a growing awareness that there are basic problems that are common to all of them. In particular, all these sub-disciplines treat systems whose behaviour depends upon combinations of logical and temporal constraints; namely, constraints on the temporal distances between occurrences of events. The aim of FORMATS is to promote the study of fundamental and practical aspects of timed systems, and to bring together researchers from different disciplines that share interests in modelling and analysis of timed systems. Typical topics include (but are not limited to):
Foundations and Semantics: Theoretical foundations of timed systems and languages; comparison between different models (timed automata, timed Petri nets, hybrid automata, timed process algebra, max-plus algebra, probabilistic models).
Methods and Tools: Techniques, algorithms, data structures, and software tools for analyzing timed systems and resolving temporal constraints (scheduling, worst-case execution time analysis, optimisation, model checking, testing, constraint solving, etc.).
Applications: Adaptation and specialization of timing technology in application domains in which timing plays an important role (real-time software, hardware circuits, and problems of scheduling in manufacturing and telecommunication).
The conference was chaired by Thomas A. Henzinger and Krishnendu Chatterjee from IST Austria.
http://pub.ist.ac.at/formats2010/

Workshop: Formalisms for Description and Visualization of Embedded Systems Architectures, April 2010 as part of the CPS week at KTH in Stockholm

This workshop had the overall goal to provide the following discussion points and insights:

- What key formalisms, ADL's and visual languages, for design of embedded systems are there and what are the trends?
- What is the maturity (languages, tools) and industrial adoption of such formalisms?
- What are the key outstanding research issues to pave way for larger scale industrial adoption?

The workshop also provided for hands-on experiences with selected formalisms including AADL, EAST-ADL (a UML profile for embedded systems), Transaction level hardware design; SystemC/VHDL, and Domain specific ADL's, using a meta-modeling environment where different formalisms can be created.
http://www.artist-embedded.org/artist/Overview,1937.html

Workshop: Green and Smart Embedded System Technology: Infrastructures, Methods and Tools
Associated with the Cyber-Physical System Week (Stockholm, Sweden, April 12, 2010), Organizing committee, general chairs, Alberto Sangiovanni Vincentelli, Huascar Espinoza, Marco Di Natale, Roberto Passerone
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.
http://www.artist-embedded.org/artist/Overview,1928.html

Workshop: Software Synthesis
October 2010, as part of ESWEEK, at Phoenix, US, co-organized by A. Sangiovanni Vincentelli and P. Marvedel
An increasing amount of software is not written manually any more. Rather, software is synthesized from abstract models of the required functionality. As a result, the effort of generating software is reduced and software verification typically becomes easier. Software synthesis has been implemented in various disperse communities.
The workshop aims at bringing these communities together and at identifying research problems which should be addressed by the scientific community.
http://www.esweek.org/

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

Workshop: IWBDA: International Workshop on Bio-Design Automation
Associated with DAC 2010, co-organizer and panel moderator, Alberto Sangiovanni Vincentelli,
The Second International Workshop on Bio-Design Automation (IWBDA) at DAC brought together researchers from the synthetic biology, systems biology, and design automation communities. The focus is on concepts, methodologies and software tools for the computational analysis of biological systems and the synthesis of novel biological systems. Still in its early stages, the field of synthetic biology has been driven by experimental expertise; much of its success has been attributable to the skill of the researchers in specific domains of biology. There has been a concerted effort to assemble repositories of standardized components. However, creating and integrating synthetic components remains an ad hoc process. The field has now reached a stage where it calls for computer-aided design tools. The electronic design automation (EDA) community has unique expertise to contribute to this endeavour. This workshop offered a forum for cross-disciplinary discussion, with the aim of seeding collaboration between the research communities. Topics of interest included:

- Design methodologies for synthetic biology;
- Standardization of biological components;
- Automated assembly techniques;
- Computer-aided modelling and abstraction techniques;
- Engineering methods inspired by biology

http://cctbio.ece.umn.edu/wiki/index.php/IWBDA:International_Workshop_on_Bio_Design_Automation

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 quantitative model checking, QMC 2010, is organized by the European Network of Excellence ARTIST Design and the Danish VKR Centre 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

Workshop: Gasics,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
- Games with 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, Crete.
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, focusing on real industrial case studies tackled.

Workshop: Second IEEE International workshop UML and Formal Methods (UML&FM'2010) held in conjunction with the 12th International Conference on Formal Engineering Methods, ICFEM 2010
November 16th, 2010 Shanghai, China

The UML and formal methods communities have been working for a number of years to produce a practical (via UML) and rigorous (via formal methods) approach to software engineering. UML is the de facto standard for modeling various aspects of software systems in both industry and academia, despite the inconvenience that its current specification is complex and its syntax imprecise. This third workshop has encouraged new initiatives of building bridges between informal, semi-formal and formal notations.
http://www.artist-embedded.org/artist/Overview,2099.html

Workshop: 1st international workshop on Model Based Engineering for Robotics (RoSym'10), co-located with MODELS'2010 and supported by Robotics Task Force at OMG.
Current engineering approaches for robotic systems have indeed been demonstrated to be insufficient to bypass following constraints that robotics embedded systems are currently facing: (i) the problem space is huge: as uncertainty of the environment and the number and type of resources available to the robot increase, the definition of the best matching between current situation and correct robot resource exploitation becomes overwhelming even for the most skilled robot engineer; (ii) the solution space is huge: in order to enhance robustness of complex robotic systems, existing cognitive methods and techniques need to exploit robotic-specific resources adequately. This means that the robotic system engineer should master highly heterogeneous technologies in order to integrate them in a consistent and effective way. One ideal process for developing robotic software components is to enable the design and implementation of highly complex and robust robotic systems to involve as less effort as possible. Robotics systems are complex and embedded ones; thanks to MBE that has already demonstrated its efficiency on complex and embedded systems. We expect MBE to be a real promising solution for the development process of robotics software & systems. This workshop will bring together robotics community and MBE community to discuss about techniques and solutions to improve current engineering for robotics systems.
http://www.artist-embedded.org/artist/RoSym-2010,2158.html

Workshop: MoBE-RTES 2010
May 4th, 2010, organized in conjunction with ISORC 2010)
Model-Based Engineering (MBE) is evolving into a fully-fledged engineering discipline, with well-established standards, industrial-strength tools, and emerging theoretical foundations. Models are being used to specify the artifacts, structure, and behavior of complex and mission-critical systems in various domains. MBE provides the ability to, design, analyze, validate, and implement such systems using much higher levels of abstraction and computer-based automation than traditional approaches to software development. One of the most challenging domains for which MBE is a natural fit is the development of Real-time and Embedded Systems (RTES). The focus of this workshop is identifying the critical challenges in the RTES domain and how MBE techniques and standards can be used to overcome them.
The primary objective of the workshop was to bring together experts, researchers, and practitioners, from the embedded and real-time systems community as well from other relevant disciplines (e.g., hardware and systems designers), who are interested in the industrial application of MBE to embedded systems.
http://www.artist-embedded.org/artist/Overview,1896.html

-- Changes wrt Y2 deliverable --

This is new text, not present in Y2 deliverables.

3. Milestones, and Future Evolution

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

Within each sub-activity, the partners will continue to develop and extend the results obtained in the first 2 years. We are also working on implementations of our previous results, and we plan to make new tool developments (either extensions of existing tools, or new prototypes) in the next year. This should trigger new research directions, and enhance the dissemination of the results. We give below a short list of the problems that will be addressed in Year 4.

Sub-activity A (*Component Modeling)*

CEA will investigate issues related to reconfiguration and auto-adaptability of component-based systems and will complete its component-based framework EC3M with related features. In addition CEA is also investigating the safety domain, and will integrate within EC3M design patterns dedicated to safety design.

CISS will in collaboration with INRIA (Rennes) improve the collaboration on the tool ECDAR supporting compositional development of timed systems using a specification theory based on timed I/O automata.

CISS will with INRIA (Rennes) work on tool support for the stochastic specification theories based on Constraint Markov Chains and Abstract Probabilistic Processes using the decision procedures of Z3 for quantifier elimination for linear arithmetic.

ESI will investigate which type of models are most fruitful to support early design processes, how they relate to each other, and how they can be used in the transient to the next phase of development. A few industrial experiments will be conducted with a design framework to manage multiple models and their relations. This should provide feedback on the prototyped concept, which will lead to a next iteration that is even better tuned to the needs of development teams. Moreover, we expect the first extensions to the framework to be made in order to fit more specific environments. ESI will also study models that can be used to validate component-based architectures with respect to system-wide use cases. In this context, also formal techniques to support component-based development will be investigated.

INRIA is investigating several extensions of the modal interface algebra to capture: (i) dynamically reconfigurable software architectures, such as those of telecommunication systems, service architectures, or systems of systems; and (ii) termination properties, which are important for the design of web-based services or work-flows.

IST will continue to develop interface theories in collaboration with INRIA. We plan to study in particular real-time synchronous interfaces based on top of the model of reactive modules..

KTH with partners in the iFEST and CESAR projects: Systematic approaches for model and tool integration for embedded systems will be evaluated and developed as part of the iFEST and CESAR projects. The goal is to lower the threshold for developing and maintaining tool-chains for embedded systems. State of the art technologies will be investigated and contrasted with industrial needs that will be elicited from the participating industrial companies.

KTH with partners in the CESAR and Maenad projects: Architecture exploration tools for architecture design are today scarce at the system and subsystem level (cmp. vehicle, and its networked subsystems). Models and techniques for embedded systems architecture design will be characterized and challenges investigated, with the goal to propose approaches that are viable for industrial adoption.

KTH with partners: EAST-ADL (UML/SysML) KTH is also together with partners including **Volvo**, **CEA** and **OFFIS** further consolidating the support for formalized requirements expression and behavior modeling capabilities of the EAST-ADL and that of the CESAR meta-model. Most of these above mentioned KTH activities relate both to component modeling and to resource modeling.

OFFIS: Within CESAR, **OFFIS** together with other project partners will continue the work on a common meta-model towards an interoperability standards for the development of safety relevant embedded systems.
Within the new ARTEMIS project MBAT, we will study models for efficient combination of analysis and testing methods.

Salzburg intends to work on developing the notion of cyber-physical cloud computing further. There is already a hardware-in-the-loop setup for running multiple virtual vehicles on server hardware, which will eventually develop into a distributed system of virtual vehicles running on real helicopters. The implementation requires further work on virtualization technology and temporal isolation of concurrent processes, in addition to work on collaborative control done by our collaborators at UC Berkeley.

Uni Trento will continue its work on design frameworks for large and small-scale systems based on meta-modeling and quantity management. In addition, the COSI framework will be extensively leveraged in applications such as avionics and energy efficient buildings

VERIMAG will continue to investigate and experiment thoroughly the spectrum of distributed implementations for BIP components. Particularly efficient solutions are foreseen for different classes of systems e.g., without conflicts on interactions, using shared-memory, distributed etc.

VERIMAG will continue to develop a contract-based design methodology, in particular, we will propose and apply instances for quantitative properties.

Sub-activity B (Resource Modeling)

CEA will improve its OPTIMUM tool dedicated to model-based analysis of real-time systems. The focus will be put on architectural exploration and improvement of results analysis. The idea is to better exploit the results provided by schedulability analysis to enable correct-by-construction modeling of embedded systems.

CISS will – within UPPAAL – develop tool support for statistical model checking of priced probabilistic timed automata allowing for performance analysis and optimization of a wide variety of resource problems.

CISS will continue work on the formalism of Time-Arc Petri Nets as a means of modeling Boolean resources.

ESI will further develop the multi-disciplinary design methodology for embedded mechatronic control systems that satisfy stringent resource constraints and performance requirements. The focus next year will be on design-space exploration platform technologies for high-performance mechatronic control systems and the incorporation of networked and distributed control, allowing the development of optimal networked and distributed control algorithms.

Uni Trento will explore how to evaluate architectures for distributed systems with particular attention to energy efficient buildings, avionics and automotive.

Uppsala will work on

- WCET analysis of parallel software on multi-cores,

- resource modeling and schedulability analysis of multiprocessor systems, and
- expressiveness and tractability of real-time task models.

VERIMAG will further develop the BIP for real time and the associated implementations.

Sub-activity C (Quantitative Modeling)

CISS will together with LSV continue work on a number of open problems concerning energy-bounded games for priced timed automata with negative and positive rates as well as linear and exponential rates. In particular synthesis of energy timed games under partial observability will be considered.

CISS will continue work on developing and applying the general metric-based theory for weighted transition systems, and study the relationship to robustness for timed automata.

ESI will further develop its work on model-driven design-space exploration support for high-tech embedded systems. Now that the Octopus toolset has reached the minimally required level of maturity in modeling support, focus will shift towards methodological and exploration support. We also plan to evaluate the toolset, in particular the expressiveness of the intermediate representation and the scalability of the approach, in at least one case study outside the printer domain.

INRIA, **Uppsala**, **Aalborg**, **Nijmegen**, and teams in Germany have applied to EU funding. Our overall objective is to continue our recent collaboration on statistical model checking and learning for embedded systems.

INRIA maintains a strong collaboration with **Verimag**. Our common topics are invariant generation and statistical model checking. Over the next three years, we will co-supervise one PhD student that will implement new results on statistical model checking in the BIP toolset.

INRIA and **IST** are currently working together to propose a new theory for timed reactive modules. This collaboration started in October 2010 with a visit of Delahaye in Austria. The exchanges will continue in 2011. As an example, Dejan Nickovic will visit INRIA in February 2011.

IST plans to continue studying the properties of quantitative languages in the context of quantitative modeling, analysis and synthesis. This will in particular involve solving open problems regarding basic questions about certain classes of quantitative languages, including their determinizability and universality.

-- Changes wrt Y2 deliverable --

This is new text, not present in Y2 deliverables.

3.2 Current and Future Milestones

- **CEA**
  will extend its EC3M framework for dealing with safety-concerns design and reconfigurations. CEA will also improve its OPTIMUM tool-set dedicated to model-based schedulability analysis.
- **CISS**
  will – in collaboration with INRIA Rennes - improve the implementation of the ECDAR tool.

Also initial effort on tool support for Constraint Markov chains and Abstract Probabilistic Automata will be made using the decision procedures of Z3.

- **ESI**
  will further develop its work on design-space exploration of high-tech embedded systems. The goal is to integrate CPNTools, Uppaal, and SDF3 into a common design-space exploration framework, to make those tools available for design-space exploration of high-tech embedded systems.
- **INRIA and Uni. Trento**
  will continue to study extensions of contract-based design approaches by considering modal specifications, extension to quantitative and dynamic aspects and methodological aspects.
- **OFFIS, INRIA and Uni Trento**
  are working on a comprehensive framework for contract-based design including a new meta-theory of contracts.
- **IST**

  developed in year 3 a flexible framework for cloud computing with promising results that we will exploit and develop further in the future.
- **IST**

  intends to further study modeling frameworks for design of robust and predictable systems, as we believe that such systems are increasingly becoming essential in embedded system design.
- **IST and INRIA**
  will continue to study extensions of contract-based design approaches by considering modal specifications, extension to quantitative and dynamic aspects and methodological aspects.
- **KTH**
  KTH and its partners in the iFEST and CESAR projects will during 2011 develop a first version of a tool integration framework for systematically realizing tool chains for embedded systems. By 2011, a first implementation of the framework and a one (or more) partial tool-chains will be finalized.
- **Salzburg** intends to demonstrate multiple virtual vehicles running on and migrating across real helicopters. The goal is to show that process isolation is effective and scalable. Future work will focus on supporting heterogeneous platforms and incorporating collaborative control technology developed at UC Berkeley. .
- **Uni Trent**o will continue its work on design frameworks for large and small-scale systems based on meta-modeling and quantity management. In addition, the COSI framework will be extensively leveraged in applications such as avionics and energy efficient buildings.
- **Uppsala**
  will continue to work on the extension of UPPAAL and TIMES for multiprocessor scheduling.

-- Changes wrt Y2 deliverable --

This is new text, not present in Y2 deliverables.

3.3 *Main Funding*

Funding for the scientific activities is provided by the following collaborative or industrial projects. New projects are underlined.

- **ACROSS ARTEMIS Project**
  It is the objective of the ACROSS project to develop and implement an ARTEMIS cross-domain reference architecture for embedded systems based on the architecture blueprint developed in the European FP7 project GENESYS. The ACROSS reference architecture will implement a *stable set of core services* cost- and energy efficiently in hardware as a foundation for the development of applications.

- **ADAMS**
  The main objective of the ADAMS project is to promote the industrial exploitation and enhancement of the MARTE and other relevant standards for the development of real-time and embedded systems using both, model and component design paradigms.
  http://www.adams-project.org

- **ArtistDesign**, Austrian Federal Ministry of Science and Research, Grant 651.394/0001-II/2/2009 (Supplemental Support).

- **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. The project finished June 2010 and the work is continued in the MAENAD project (see below).

  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

- **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

- **Concurrent Programming with Threading by Appointment**
  Austrian Science Fund (FWF), Grant P18913-N15 (three PhD students).

- **Condor project**
  The Condor project is partially supported by the Dutch Ministry of Economic Affairs under the BSIK program. It concentrates in system performance and evolvability. Case studies are based on electron microscopes of FEI Company. Partners are ESI, Eindhoven University of Technology, Delft University of Technology, Katholieke Universiteit Leuven and University of Antwerp. Second participating industrial partner is Technolution, an SME company on technical automation and embedded systems. http://www.esi.nl/condor/.

- **CoDeR-MP** - Real-Time Applications on Multicore Platforms, Supported by the Swedish strategic research foundation
  http://www.it.uu.se/research/coder-mp

- **CREDO** (http://www.cwi.nl/projects/credo/), Modeling and analysis of evolutionary structures for distributed services, supported by EU

- **DaNES - Danish Network of Embedded Systems**
  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/

- **Darwin project.**
  The Darwin project addresses system evolvability, using MRI scanners of Philips Healthcare as sources for cases studies. Other partners are ESI, Philips Research, Delft University of Technology, Eindhoven University of Technology, University of Groningen (RuG), University of Twente, and the Vrije Universiteit Amsterdam. Partially supported by the Dutch Ministry of Economic Affairs under the BSIK program.
  http://www.esi.nl/darwin/.

- **DFEA2020:** stands for Dependable and Flexible Electrical Architecture 2020, and is a collaborative project between Volvo car (coordinator), KTH, Chalmers and a number of suppliers and consultancy companies in Sweden. The project has the goal to develop the next generation of automotive embedded system architectures for Volvo car.
  www.md.kth.se/RTC

- **Dynamically Self-Configuring Automotive Systems (FP6)**
  DySCAS is a research project funded by the European Commission within FP6. The project started June 1 2006 and will end in February 2009. A Final Workshop will be arranged in Brussels February 18, 2009. The main objective of the DySCAS project is the elaboration of fundamental concepts and architectural guidelines, as well as methods and tools for the development of self-configurable systems in the context of embedded vehicle electronic systems.
  http:/www.dyscas.org

- **Falcon project**
  The Falcon project focuses on system performance and reliability of a new generation of distribution centers. It is partially supported by the Dutch Ministry of Economic Affairs under the BSIK program. The carrying industrial partner is Vanderlande Industries. Other partners are ESI, Eindhoven University of Technology, Delft University of Technology and University of Twente.
  http://www.esi.nl/falcon/.

- **GASICS**
  European Project sponsored by European Science Foundation (ESF).
  This project studies game theoretic formalizations of interactive computational systems and algorithms for their analysis and synthesis. Our aim is to extend the existing notions of games played on graphs introduced by computer scientists. Currently, most of the games played on graphs are of the sort "two players-zero sum", we aim to extend them to "multiple players non-zero sum", and show the applicability of the new theory to the analysis and synthesis of interactive computational systems.
  Sponsors: European Science Foundation with Danish participation sponsored by Danish Agency for Science Technology and Innovation.
  Partners: Centre Fédéré en Vérification, Belgium (project leader Jean-Francois Raskin), Aachen University, Germany, (principal investigator Wolfgang Thomas), CISS Aalborg University, Denmark (principal investigator: Kim G. Larsen), French IP containing LIAFA, LSV with Jean-Eric Pin and Nicolas Markey being principal investigator, University of Warwick, United Kingdom, Marcin Jurdzinski being principal investigator.

- **The JAviator Project, IBM Faculty Award 2007 (Helicopter Platform)**
  JAviator is a research project of the Computational Systems Group at the Department of Computer Sciences at the University of Salzburg and of the IBM Watson Research Center. The goal of the project is to develop high-level real-time and concurrent programming abstractions and test them on UAVs (unmanned aerial vehicles). We are working on methodologies that enable time-portable programming of high-performance, hard real-time applications in Java. The resulting application code is not only efficient but also robust with respect to real time. Time-portable programs do not change their real-time behavior across different hardware platforms and workloads similar to Java's write-once-run-anywhere paradigm for functional behavior but extended to the temporal domain.
  http://javiator.cs.uni-salzburg.at/
- **MAENAD,** Model-based Analysis & Engineering of Novel Architectures for Dependable Electric Vehicles. MAENAD is an FP7 project funded by the European Commission. The MAENAD project continues the refinement of EAST-ADL for meeting these challenges. The title, Model-based Analysis & Engineering of Novel Architectures for Dependable Electric Vehicles gives a hint of the main objectives: (i) Provision of support for the automotive safety standard ISO 26262, (ii) Provision of capabilities for prediction of dependability & performance, (iii) Provision of capabilities for design optimization, and (iv) Demonstration of project results in a practical electrical vehicle design, in the context of EAST-ADL and Fully Electrical Vehicles. The partners of this project are: Volvo Technology Corporation, Centro Ricerche Fiat S.C.p.A., Continental Automotive, Delphi/Mecel AB, MetaCase, Pulse-AR, Systemite, CEA, KTH, TU Berlin and University of Hull.
  http://www.maenad.eu

- **MARAE**
  MARAE is a French industrial project on robust methods to develop autonomous systems (2008-2010), with ARTIST partner VERIMAG in collaboration with ASTRIUM (EADS) and LAAS. This project is funded by FNRAE ("Fondation Nationale pour la Recherche en Aéronautique et l'Espace")

- **"Modeling and verification of timed systems**" supported by the Swedish research council

- **MoDES** Danish national project sponsored by the Strategic Research Council.

- **MT-LAB - 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/

- **Multiform**
  Project under the 7th Framework Programme of the European Committee. The main goal of the Multiform project is the integration and support for interoperability of tools and methods based on different modeling formalisms. Partners are ESI, University Dortmund, Eindhoven University of Technology, University Joseph Fourier, RWTH Aachen, Aalborg University, VEMAC and KVCA.
  http://www.ict-multiform.eu

- **Octopus project**
  Partially supported by the Dutch Ministry of Economic Affairs under the BSIK program. The Octopus project addresses system adaptability in the context of digital document

printers of company Océ. Other partners are ESI, Delft University of Technology, Eindhoven University of Technology, Radboud University Nijmegen, and University of Twente.
http://www.esi.nl/octopus/

- **Poseidon project**
  The Poseidon project is partially supported by the Dutch Ministry of Economic Affairs under the BSIK program. It concentrates on system evolvability and reliability of systems of systems, Thales Above Water Systems Division provides the industrial challenge, Second participating industrial partner is Noldus Technology. Other partners are ESI, Delft University of Technology, Eindhoven University of Technology, Free University of Amsterdam, University of Amsterdam, and University of Tilburg. http://www.esi.nl/poseidon/
- **Quasimodo.**
  Project under the 7th Framework Programme of the European Committee. The main objective 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. Partners are ESI, CISS, Radboud University Nijmegen, University of Twente, CNRS & ENS, RTWH Aachen, University of Saarland. UL Bruxelles, Terma, Chess and Hydac
  http://www.quasimodo.aau.dk/
- **REVE project.**
  Safe reuse of embedded components in heterogeneous environments.
  http://www.ara-reve.org
- **RT-Simex**
  is a French National Research Agency funded project. This 3 years project started in January 2009 and involves Aonix, CEA LIST, INRIA, Obeo, UBO and Thales Research and Technology. The goal of the project is to provide a platform for real-time models simulation and debugging.
- **SMECY ARTEMIS Project**
  The goal of this ARTEMIS project is to launch an ambitious European initiative to allow Europe to catch up with Asia and USA (e.g. PARLAB in Berkeley, Parallel@illinois and Pervasive Parallelism Laboratory in Stanford) and to enable Europe to become the leader.
- **SNSF** (Swiss National Science Foundation).
- **SPEEDS IP project**
  The SPEEDS project aims at significant enhancement of model-based systems engineering by semantics-based modeling 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/
- **SYSMODEL (Artemis project)**

  SYSMODEL has the goal to allow SMEs to build cost-efficient ambient intelligence systems with optimal performance, high confidence, reduced time to market and faster deployment.
  http://www.sysmodel.eu/Consortium.htm
- **UPMARC**
  Uppsala Programming for Multicore Architectures Research Centre, supported by the Swedish Research Council
  http://www.it.uu.se/research/upmarc

- **VERDE**
  an ITEA funded project. This 3 years project started in June 2009 and involves the following European partners: Thales, CEA LIST, Smartesting, Geensys, Obeo, Atos, EADS Astrium, Robert Bosch, Infineon Technologies, Fraunhofer FOKUS, ScopeSET, FZI Forschungszentrum Informatik, University of Paderborn, ICT-Norway and SINTEF. The goal of the project is to develop and industrialize a solution for iterative, incremental development and validation of real-time embedded systems.

- **Wings Project**
  In the Wings project, ESI collaborates with the Dutch company ASML, the world's leading provider of lithography systems for the semiconductor industry. The project started January 2010 for a duration of 2 years. The objective of this project is to develop predictable embedded control systems for high-performance mechatronics using a multidisciplinary model-based approach.

Internal Reviewers for this Deliverable

- Kim Larsen (Aalborg)
- Alain Girault (INRIA)