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

Activity - Progress Report for Year 4

JPRA Activity (WP3)

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 9th, 2012

Table of Contents

1. Overview of the Activity

1.1 ArtistDesign Participants and their role within the Activity

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)
Q*uantitative 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)
Tool Integration, Formal analysis of heterogeneous composition, abstract algebra, and metamodeling.

-- Changes wrt Y3 deliverable --

No changes

1.2 Affiliated Participants and Roles

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.

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

Jean-Francois Raskin (CVF – Belgium);
*Synthesis for reactive systems. Timed and hybrid automata.*Bernhard Steffen (U. of Dortmund)
Modeling, verification, learning, test, software design methods, tools

Sophie Quinton (Braunschweig)
Contract-based software design methods, distributed implementations

Florian Horn (LiAFA, Paris)
Games and synthesis

-- Changes wrt Y3 deliverable --

The list of affiliate partners has been updated to correspond to the actual contribution of year 4.

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 Y3 deliverable --

No changes with respect to Year 3.

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 Y3 deliverable --

No changes with respect to Year 3.

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 Y3 deliverable --

No changes with respect to Year 3.

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 Y3 deliverable --

No changes with respect to Year 3.

2. Summary of Activity Progress

2.1 Synthesis View of the Main Overall Achievements

During the project, multiple achievements have been obtained by the partners of the modeling cluster and their associated partners. They have been exhaustively reported in the four yearly deliverables. We focus here on the most visible ones of these achievements on which the existence of the ARTIST network had a clear impact. All these projects were a support for a large number of PHD theses.

During the project, we have always maintained the division of the modeling activities into the three sub-activities and we keep this distinction here even if several achievements are strictly speaking related to more than one of the topics:

A. Component Modeling", where we mainly focus on defining and composing models with heterogeneous semantics. We considered rich models including non-functional issues, architectures and assumptions on the environment (contracts) and corresponding modeling and/or synthesis environments.

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). In particular, we considered here problems related to scheduling and resource allocation, to Design Space Exploration and to modeling for performance.

C. Quantitative Modeling", where we specifically focus on design frameworks for quantitative modeling. We have mainly focused on timing and probabilities, but also on multi-valued evaluation. There was an important focus on synthesis.

Sub-activity A (Component Modeling)

Some of the most visible achievements on modeling have been obtained by collaboration in multi-partner projects that mostly have evolved from collaborations within ARTIST. In particular, the European projects ACROSS, ATTEST (1 and 2), CESAR, COMBEST and SPEEDS have been set up due to collaborations in ARTIST and have come up with important results concerning modeling:

- Several meta-models for particular aspects of heterogeneous embedded systems have been defined. The HRC meta-model developed in SPEEDS and further exploited in COMBEST, CESAR … focuses on the notion of contract. The MARTE meta-model that is now an UML standard and widely used provides wide bases for modeling of time and general non-functional properties. The EAST-ADL meta-model developed in ATTEST and further exploited in CESAR focusses on architecture descriptions. The BIP meta-model developed in SPEEDS and further used in COMBEST, ACROSS and a number of other projects focusses on composition. As these meta-models focus on different aspects, combined use is potentially meaningful, and some combinations (e.g. HRC-BIP) have been worked out.
- All these meta-models suppose a component-based approach where composition or MoCs (Models of Computation) and as a consequence compositionality and compositional reasoning are in important aspect. In SPEEDS and follow-ups several interesting contract frameworks have been developed and it has been shown how compose verification results rather than components and contracts also for theories which are not based on the

same semantics. In a larger setting, interesting interface theories based on modal transition systems have been defined and applied to timing properties.

- In these projects, a large number of tools for editing (Papyrus), verification, synthesis (BIP, Uppaal), simulation and code generation (BIP, Giotto, Metropolis) have been developed or extended combined to larger tool chains, and applied to industrial case studies
- The development of (component-based) design and validation methodologies has been another major aspect of all these collaborative projects with penetration in industry (especially automotive, but also energy efficient buildings and bio),

Sub-activity B (Resource Modeling)

- Concerning resource modeling, the cluster partners have mainly explored topics related to performance and scheduling, distributed implementations, and design space exploration. Some of the most visible achievements related to resource usage are the following ones:
- the extension of existing modeling formalisms or frameworks for being able to express resource constraints, resource usage and architecture constraints. In particular, EAST-ADL (CEA, KTH and Volvo) the MARTE UML profile
- based on these models, theories and tools for design space exploration have been developed in several collaborative projects
- significant advances have been achieved in the domain of optimization and scheduler synthesis under multiple constraints
- advances have been made in platform dependent code generation. In several projects, generation of distributed code, also guarantying extra functional properties have been studied.
- the methods and tools developed by the cluster partners have been applied to real-world applications, for example the thermal behavior of an MRI scanner and printers, the Salzburg Helicopter platform, and energy regulation for intelligent buildings.

Sub-activity C (Quantitative Modeling)

Concerning quantitative modeling, the cluster partners have mainly focused on timing and probabilities, but also on multi-valued evaluation with an important focus on synthesis. Some of the most visible achievements are the following ones:

- Quantitative generalization of classical languages, in particular priced time automata and other valued extensions of automata and theoretical studies on expressiveness, closure properties and verification algorithms for these models
- Quantitative theories and extensions of non-quantitative ones for Boolean systems and arbitrary programs, in particular also the definition of quantitative properties fro non quantitative system definitions and quantitative extra-functional properties for software intensive embedded product lines.
- methods and tools for verification and synthesis for the before mentioned models
- Models and theories for on usual “quantities” such as evolvability, extendability, flexibility and robustness.

2.2 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.

This section was already presented in the Y3 deliverable, in section 1.7.

2.3 Work achieved in Year 2 *(Jan-Dec 2009)*

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..)

This section was already presented in the Y3 deliverable, in section 1.8.

2.4 Work achieved in Year 3 *(Jan-Dec 2010)*

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 modelling, 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 analysing 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).

This section was already presented in the Y3 deliverable, in sections 1.8 and 3.1.

2.5 Work achieved in Year 4 *(Jan-Dec 2011)*

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 (in collaboration with INRIA) has worked on compositional specification formalisms for probabilistic systems, ranging from Interval Markov Chains, Constraint Markov Chains and Abstract Probabilistic Automata, and has worked on Logical and compositional reasoning for continuous Markovian systems (Technical Achievement 15).

CISS has worked on introduction of and complexity results for parametric modal transition systems and modal transitions with data, which provides a useful extension of the well-established specification theory of modal transition systems (Technical Achievement 14).

ESI developed the design framework concept, which integrates storage of design reasoning with the design artefacts and models. The prototype tool will be validated in an industrial environment and further developed to meet industrial needs of use, integratability, and maintainability (Technical Achievement 13).

ESI devised a model-based development process for Philips Healthcare to detect faults earlier and to increase the speed of the innovation of medical devices. The approach is based on executable models and simulation during the early phases of development and the use of formal techniques during detailed design (Technical Achievement 13).

INRIA has extended the protocol conversion approach in two directions, first to take into account data mismatches between the components (on top of classical control mismatches), and second to generalize the approach to make it incremental (Technical Achievement 70).

IST Austria + UC Berkeley continued the work on relational interfaces in the synchronous systems setting (Technical Achievement 19).

IST Austria + U Leicester + Rice + Microsoft extended the model of reactive modules with dynamic features, thus allowing dynamic creation and reconfiguration of instances (Technical Achievement 72).

KTH and Volvo investigated and proposed extended behavioral modeling support for the EAST-ADL architecture description language (Technical Achievement 29).

KTH, Volvo and other affiliated partners worked on extending the support for safety modeling as part of the EAST-ADL architecture description language. Closely related an investigation in modeling and robustness analysis through model-level fault-injection in behavior models was concluded with a thesis (Technical Achievement 30).

OFFIS, KTH and Volvo developed a common meta-modeling approach supporting interoperability of models and tools (Technical Achievement 27, 55, 75).

Salzburg, in collaboration with UC Berkeley, continued working on the earlier introduced notion of cyber-physical cloud computing, now funded by a joint, 3-year, medium-scale NSF grant.

Salzburg, in collaboration with the University of Porto, continued exploring the earlier introduced notion of runtime programming using HTL as example.

TRENTO (in collaboration with VERIMAG) has worked on the development of MetroII heterogeneous models that are suitable for the representation of different interaction semantics described as a collection of connectors in the BIP tool. The method has been tested on a distributed sorting algorithm case study (Technical Achievement 77).

Uppsala has worked on modelling for automated learning in collaboration with **TU Dortmund**. The approach includes a novel canonical automaton model, based on register automata that can be used to specify protocol or program behaviour. A canonical automaton representation Technical achievement 80)

Uppsala has worked on “Simpler and more Uniform component modelling” in collaboration with Oxford University, We propose a compositional specification theory for reasoning about components that interact by synchronisation of input and output (I/O) actions, in which the specification of a component constrains the temporal ordering of interactions with the environment (Technical Achievement 81)

VERIMAG worked --- as a continuation of the work on source-to-source architecture transformation (former Technical Achievement 44), 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).

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

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).

CISS has worked on specification formalisms for consumption of resource, e.g. energy. This includes full study and presentation of priced timed automata, introduction of energy automata (allowing for positive and negative weigh rates), weighted extensions of modal transition systems, as well as studying cost-constrained (by interval) behavior of multi-weighted transition systems (Technical Achievement 79).**ESI** extended the Octopus DSE toolset with schedulability analysis and dataflow analysis. Modularity was added to the intermediate representation. Two new modeling frontends have been developed. Several successful DSE case studies in the professional printing domain have been performed (Technical Achievement 12).

ESI developed tool support to extract performance models automatically from existing engineering artifacts. The models are first calibrated by measurements and next used for performance predictions (Technical Achievement 10).

ESI investigated the applicability of dataflow formalisms for modeling and analyzing signal processing applications emerging in the domains of multi-media and high-tech control. A key problem is a need for combining streaming-based dataflow with state-machine based control to capture the increasing dynamism in such applications (Technical Achievement 10).

INRIA has extended previous results on the design and modelling for reliability of safety-critical embedded real-time systems. We have proposed a new off-line tri-criteria scheduling heuristics which, from a given software application graph and a given multiprocessor architecture produces a static multiprocessor schedule that optimizes three criteria (Technical Achievement 71)

INRIA has designed a new data-flow model of computation (MoC) aimed at dynamic systems. The difficult balance to be found is between expressivity and analyzability: at one end of the spectrum is SDF, perfectly analyzable but not dynamic at all; at the other end of the spectrum is DDF, totally dynamic but not analyzable at all. Our new MoC is parametric, it allows dynamic systems to be captured (e.g., we have used it to design a video codec), and it brings a set of static analyzes for boundedness and liveness (Technical Achievement 76).

IST Austria + LIAFA studied the problem of synthesis in context of request-response games (Technical Achievement 73).

Salzburg introduced a new notion of so-called power isolation to model power consumption of individual software processes in isolation from each other (Technical Achievement 67)

TRENTO (in collaboration with ETHZ) has worked on modeling embedded systems using parametric timed automata with the purpose of quantitatively studying the feasibility of the parameter space with respect to timing and safety properties. The method has been tested on simple cases, and on a more advanced system that uses state based components which are difficult to model in MPA (Technical Achievement 78).

Uppsala has worked on Multicore scheduling. The first objective is to evaluate the existing multiprocessor scheduling algorithms and implementation overheads in operating systems. The second is to further improve the precision of schedulability test based on utilization bounds (Technical Achievement 43).

Uppsala has worked on Mixed-criticality systems. The goal is to deploy and integrate different types of applications e.g. hard and soft real-time applications on the same hardware platforms. The applications may have different levels of criticality and thus different requirements of computation resources (Technical Achievement 68).

Verimag and **IST** have developed a general framework to evaluate and construct controllers with respect to how efficient they behave in a given probabilistic environment (Technical Achievement 50).

VERIMAG has continued the work on implementing prioritized global specifications on distributed platforms (Technical Achievement 45). The continuation of the work on real-time (former Technical achievement 63) is reported in details in the deliverable on adaptivity.

Sub-activity C (Quantitative Modeling)

CISS has worked on metrics on quantitative behaviours resulting in several papers and in several directions. In particular, this line of research contains novel contributions to the understanding of robustness for timed automata.

IST Austria, together with IIT Bombay, continued its work on quantitative synthesis, in the setting of concurrent programs (Technical Achievement 21).

IST Austria, together with Hebrew Uni, continued the work on better understanding of quantitative specifications and languages (Technical Achievement 74).

Uppsala has worked on Expressiveness vs. analysis efficiency of models for timed systems. The objective is to find the optimal trade-off to develop models that are expressive enough for modeling of realistic systems, and also tractable in the sense they can be efficiently analyzed automatically. We also establish hardness results on the analysis of scheduling problems (Technical Achievement 69).

-- The above is new material, not present in the Y3 deliverable --

3. Detailed view of the progress in Year 4 *(Jan-Dec 2011)*

3.1 Technical Achievements

1. EC3M, a component-based framework for model-based design of embedded systems (CEA)
eC3M (developed by CEA, available at www.ec3m.net) is a plug-in for Papyrus providing the generation of execution infrastructures for component-oriented specifications. eC3M is generic as 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). In particular, imported model libraries describe elements of a component container (enclosing the business logic) and interactions components which we call connectors. With the help of these libraries, eC3M provides currently support for generating code from MARTE-GCM based models, including the execution of state-charts within the container. By means of a recent addition, the container provides reflective information about the component (including resource consumption) that enable adaptation in resource constraint environment. In the context of safety-critical application, we developed support for (safety) design patterns, in particular related to replication. The pattern support is integrated with the use of specific connectors/containers that enable the runtime support for voting among replicas.
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. In this context, CEA has proposed a new request for proposal (i.e. a specification for a request of new standard) dedicated to extend the fUML standard in order to support component-based approach in a more formal way in the context of the Model Driven Architecture (MDA) approach of OMG.

2. OPTIMUM, a model-based approach for software architectural evaluation against non-functional requirements (CEA)
This year, several extensions for Optimum have been defined. First of all, the main goal of the tool has slightly changed, in order to support not only schedulability evaluation of software architectures, but the overall process of mapping the system-level functional model in the architecture that best fits user-defined metrics (e.g. cost, resource utilization, response time, power consumption, etc.) under a set of constraints (e.g. end-to-end deadlines). A new prototype has been developed that integrates schedulability tests and helps the designer in selecting the software architecture. At this stage it is possible to automatically maps functions to software tasks in optimal way with respect to response time in mono-processor systems. Three Ph.D. thesis has been launched with the following objectives: (1) to extend optimality to different possible metrics, in distributed architectures with time and event-based activation task models; (2) to provide so-called semantics preservation, i.e. the guarantee that functional execution semantics, once mapped in the concrete software architecture, will be preserved; (3) to integrate reliability targets and constraints in the overall process.

.

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

Modern high-tech systems make extensive use of real-time embedded (servo) control systems for active correction of imperfections. Control applications consist of thousands of dependent control tasks and have to satisfy hard real-time end-to-end timing requirements. Applications are highly parallel and are deployed and scheduled on multi-core execution platforms to satisfy these timing requirements. The scale and complexity of these control

systems has outgrown a manual design approach. In the ESI Wings project this problem was addressed by the development of a Y-chart based method to predict and optimize timing performance. Formal domain models were developed to represent the application, mapping and platforms views of the Y-chart. A front-end extraction tool was developed to create these models automatically from engineering artifacts. Critical to the value of the performance prediction results was the accuracy of the timing models. To calibrate the models, a "predict-the-past" exercise was undertaken: measurement data for the existing embedded control system was collected and the obtained performance numbers, both for individual tasks, and end-to-end latencies were fed into the models. With these numbers, the end-to-end performance numbers of the models were within 5% of the actual system's latency: accurate enough to place confidence in further design space explorations with alternative mappings. The method was applied to the motion control of the wafer stage of an industrial ASML wafer scanner and predicted a mapping and scheduling strategy to double its performance. Prototypes of the optimized system confirmed these predictions, again with a timing error of less than 5%. Results are so promising that the method and models will be integrated as first-class citizens in the ASML development flow, not only to predict and optimize performance, but also to synthesize implementations[VHT+11].

ESI also investigated performance modeling and analysis of dynamic signal processing applications [SBA+11, DST+11]. Modern signal processing applications as emerging in the domain of multi-media and high-tech control exhibit more and more dynamism. Examples include processing different frame types in MPEG-4 decoding and control mode changes in mechatronics. Such dynamism can have a substantial impact on the predictability of embedded system performance. Model-based performance prediction requires using formalisms capable of capturing the dynamism in modern signal processing application. To this end, ESI is investigating the application of dataflow models in an industrial context. The novel dataflow model of Scenario-Aware Dataflow (SADF) combines streaming-based dataflow with state-machine based control [YGB+11,SGT+11]. It can be used for evaluating both worst/best-case and average-case performance metrics, for which an exact approach has been developed (and implemented in the SDF^3 toolkit) to compute quantitative numbers for such performance metrics based on model checking techniques [TGV11,TKW12]. In case state-space explosion renders application of these performance model checking techniques infeasible, an automated translation of SADF to the POOSL modeling language is supplied for simulation-based evaluation of the same performance metrics.

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

Work on the Octopus DSE (Design-Space Exploration) toolset continued. The toolset has been extended with schedulability analysis based on the Uppaal model checker and dataflow analysis based on the SDF3 dataflow analysis toolset. One of the challenges in adding these analyses to the toolset was the fact that a parameterized model needs to be converted to a model in which the bounds of the parameter ranges are made explicit (if possible) [HGB11]. To improve easy of modeling, modularity was added to the DSE Intermediate Representation (DSEIR). Two new modeling frontends have been developed, an XML-based one and a graphical editor. Several successful DSE case studies in the professional printing domain have been performed with Océ technologies [THB+11,NVB11]. More information about the Octopus toolset can be found in [THB+2011, BBG+2010] and through http://dse.esi.nl.

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

In the Multiform project, the prototype of the so-called design framework, which was realized in 2010, has been extended. This design framework is intended to support system architects in industry in their development process. In order to validate whether the tool and its concepts do support them, an observational study in an architectural team at the company Vanderlande was conducted. For a period of 2 months, ESI participated in their meetings and mapped the discussions, reasoning, design decisions, modeling activities, etc. on the design framework concepts. This resulted in a better structuring of the development process,

along with a number of high level performance models for candidate system designs that were used by Vanderlande as input to take decisions in the development process.

Together with Vanderlande, ESI has also worked on the modeling and simulation of warehouse management and control systems. This has been used to validate a new system concept. A graphical editor has been developed to model both structure and behavior of a distributed warehouse control system [HV11].

In close collaboration with Philips Healthcare, a number of modeling approaches have been applied to support the development process of interventional X-Ray systems. Main aim is to detect faults earlier, thus reducing the test and integration phase, and obtaining fast support for medical innovations in various clinical segments, such as cardiovascular, neurology, electrophysiology, and surgery. To this end, first a black-box requirements model has been made in POOSL, together with a connection to tools such as Flash and Blender that allow convenient visualization for domain experts. Next POOSL design models have been developed to validate the main architectural concepts by means of simulation. Finally detailed interface and design models have been made using the ASD technology of the company Verum. The tool ASD:Suite supports formal refinement checks and complete code generation from design models [HHS11]. In a case study at FEI Company, the ASD approach has been complemented with the verification of other properties using Uppaal.

14. Data and Parametric Extensions of Modal Transition Systems (CISS) Specification theories as a tool in the development process of component based software systems have recently abstracted a considerable attention. Current specification theories are however qualitative in nature and hence fragile and unsuited for modern software systems. In [BFJLLT11] we propose the first specification theory which allows capturing quantitative aspects during the refinement and implementation process.

[BJLLS11] introduce a novel formalism of label-structured modal transition systems that combines the classical may/must modalities on transitions with structured labels that represent quantitative aspects of the model. On the one hand, the specification formalism is general enough to include models like weighted modal transition systems and allows the system developers to employ even more complex label refinement than in previously studied theories. On the other hand, the formalism maintains the desirable properties required by any specification theory supporting compositional reasoning. In particular, we study modal and thorough refinement, determinization, parallel composition, conjunction, quotient, and logical characterization of label-structured modal transition systems.

Modal transition systems (MTS) are a well-studied specification formalism of reactive systems supporting a step-wise refinement methodology. Despite its many advantages, the formalism as well as its currently known extensions is incapable of expressing some practically needed aspects in the refinement process like exclusive, conditional and persistent choices. [BKLMS11] introduce a new model called parametric modal transition systems (PMTS) together with a general modal refinement notion that overcome many of the limitations and we investigate the computational complexity of modal refinement checking.

Modal Specifications (MSs) is a well-known and widely used abstraction theory for transition systems. MSs are transition systems equipped with two types of transitions: must transitions that are mandatory to any implementation, and may transitions that are optional. The duality of transitions allows developing a unique approach for both logical and structural compositions, and easing the step-wise refinement process for building implementations. [BLLNW11] proposes Modal Specifications with Data (MSDs), the first modal specification theory with explicit representation of data. Our new theory includes all the essential ingredients of a specification theory. As MSDs are by nature potentially infinite-state systems, we also propose symbolic representations based on effective predicates and show

equivalence with the semantic definitions. Our theory serves as a new abstraction-based formalism for transition systems with data.

15. Modular Markovian Logic (CISS) In [MCL11] and [CLM11] we introduce Modular Markovian Logic (MML) for compositional continuous-time and continuous-space Markov processes. MML combines operators specific to stochastic logics with operators reflecting the modular structure of the models, similar to those used by spatial and separation logics. We present a complete Hilbert-style axiomatisation for MML, prove the small model property and analyze the relation between stochastic bisimulation and logical equivalence..

19. Synchronous relational interfaces (IST Austria + UC Berkeley)
In this work, we propose a relational interface theory for specification of synchronous component, that allows in particular expressing relations between input and output assignments. We consider both the stateless and stateful case. In the stateful case, we support composition by connection and feedback operators, where feedback is allowed only for Moore interfaces. Our theory includes explicit notions of environments, pluggability and substitutability. In addition, we define a notion of refinement between interfaces, which are preserved by composition and is equivalent to substitutability for well-formed interfaces, and shared refinement and abstraction operators, corresponding to greatest lower bound and least upper bound with respect to refinement. Finally, we study two restricted classes of synchronous relational interfaces, namely input-enabled and deterministic interfaces. This work was presented in [TLHL11].

21. Quantitative synthesis for concurrent programs (IST Austria + IIT Bombay)
We develop a technique for synthesizing the optimal placement of synchronization constructs in under-specified concurrent programs. Apart from a partial concurrent program, the input also consists of a performance model, expressed as a weighted automaton, which assigns costs of inserting different constructs. Given this input, our method automatically completes the program by adding appropriate synchronization constructs in a way that guarantees both correctness (race and deadlock freedom) and optimal worst-case or average case performance of the resulting program. We show that the synthesis problem for the worst-case performance is equivalent to 2-player graph games with quantitative limit-average objectives. For the average-case performance, we show that the problem is equivalent to 2 ½ player graph games. We have developed a prototype tool that implements this synthesis method. This work was presented in [CCH+11].

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. Further collaborative work in the CESAR project has included industrial evaluation of automotive domain specific tool chain prototypes for this approach, [AZ11].

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.

Further work in this direction has assessed the need for such behavior modeling capabilities in the context of future electrical vehicles. Future fully electrical vehicles (FEV) are safety critical and have particular complexity in operations, design and integration of control functionalities, power efficiency and harness. To develop appropriate language support, there is a need to clarify the specific engineering and quality concerns and thereby to specify necessary language support in regard to both methodology and modeling artifacts. In particular, according to the derived requirements, the expected modeling support for behavior description ranges from the definitions of operation and boundary conditions, to the specifications of functional constraints, mode and error behaviors, and to the physical dynamics of plants, harness and power. While providing an enhanced support for requirements engineering, functional safety, architectural composition, refinement, and contract specification, the proposed native behavior extension of EAST-ADL would also constitute the basis for integrating external methods and tools for early estimations and V&V of performance and dependability [MD11]. The proposed language extension consists of three categories of behavior constraints:

- Attribute Quantification Constraint – relating to the declarations of value attributes and the related acausal quantifications (e.g., U=I*R).
- Temporal Constraint – relating to the declarations of behavior constraints where the history of behaviors on a timeline is taken into consideration.
- Computation Constraint – relating to the declarations of cause-effect dependencies of data in terms of logical transformations (for data assignments) and logical paths.

Each of these behavior constraints can be associated to time conditions given in terms of logical time, of which the exact semantics can be given by the existing EAST-ADL support for execution events (e.g. the triggering, and port data sending & receiving events of a function). The meta-model integration is done in a modular way such that no existing EAST-ADL constructs are modified by the extension.

Model transformations for the purpose of EAST-ADL analysis using Uppaal have also been investigated, first by assessing different mappings and then by transformation experiments, [NC11a]. Mappings from EAST-ADL concepts to Autosar have also been investigated. Three case studies, of a position control, fuel control and a brake-by-wire system, have been used to support and validate the work. The resulting mapping scheme provides a basis for automated architecture refinements and synthesis, [NC11b].

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.

As part of collaborative research in the Maenad project, further work has been carried out to extend the support for modeling and analysis of safety critical automotive embedded systems. The work has included analysis of the ISO26262 safety lifecycle (ISO26262 is the new automotive standard for functional safety), including the key tasks and artifacts, and in providing an overall assessment of what the EAST-ADL architecture description language provides to support the ISO26262 requirements, [TT11]. Recent advances of EAST-ADL support for the design of functional safety and its integration with system architecture design is presented in [CJ11]. The work complements and consolidates our earlier work, [SC11], [CJ08], by introducing in detail the adopted (meta) modeling pattern as well as the language alignment with ISO26262 in regard to the safety life-cycle, safety requirements, architectural and analytical artifacts.

31. Cyber-Physical Cloud Computing (Salzburg + UC Berkeley)
Salzburg, in collaboration with UC Berkeley, continued working on the earlier introduced notion of cyber-physical cloud computing (CPCC). A collaborative team has been formed to develop a number of distributed platforms for studying CPCC. The platforms range from fixed-wing over rotary-wing aircraft to off-the-shelf mobile computers, in particular smart phones. A recent publication provides further details on the CPCC vision identifying the so-called migration (of virtual vehicles) and binding (of virtual-to-real vehicles) problems as the key challenges in CPCC [KSPHHCLRT12]. This effort is funded by a 3-year, medium-scale NSF grant that recently started.

33. Runtime Programming (Salzburg + U. Porto)
Salzburg, in collaboration with the University of Porto, continued exploring the earlier introduced notion of runtime programming through model-preserving and scalable runtime patches. We have used HTL in a case study and recently published the final results [KLMS11].

35. Platform-Based Design and Frameworks: Metropolis and Metro II (Uni. Trento, UC Berkeley, EPFL, Boston U., 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. In addition, in collaboration with VERIMAG, we have worked on the development of MetroII heterogeneous models that are suitable for the representation of different interaction semantics described as a collection of connectors in the BIP tool. The method has been tested on a distributed sorting algorithm case study.

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.

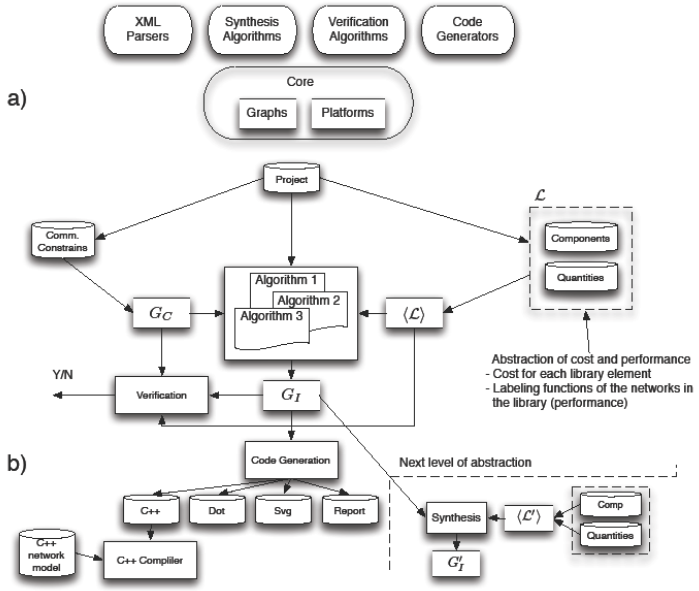

Figure 1. The COSI Platform-Based Design-like structure

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. The framework has been extended to deal with energy efficient buildings and in particular, to the optimal selection of heterogeneous wired and wireless networks [MPS11], [PMPLSV11].

43. Implementation and Empirical Comparison of Multi-core Scheduling Algorithms: (Uppsala)

Recent theoretical studies have shown that partitioning-based scheduling has better real-time performance than other scheduling

Recent theoretical studies have shown that partitioning-based scheduling has better real-time performance than other scheduling paradigms, such as global scheduling on multi-cores. Especially a class of partitioning-based scheduling algorithms (called semi-partitioned scheduling) allows splitting a small number of tasks among different cores, and therefore offering very high resource utilization. The major concern about the semi-partitioned scheduling is that due to the task splitting, some tasks will migrate from one core to another at run time, which incurs higher context switch overhead. Thus, one would suspect that the extra overhead caused by task splitting would counteract the theoretical performance gain of semi-partitioned scheduling. In this work, we implement a semi-partitioned scheduler in the Linux operating system, and run experiments on an Intel Core-i7 4-cores machine to measure the real overhead in both partitioned scheduling and semi-partitioned scheduling. Then we integrate the measured overhead into the state-of-the-art partitioned scheduling and semi-partitioned scheduling algorithms, and conduct empirical comparisons of their real-time performance. Our results show that the extra overhead caused by task splitting in semi-partitioned scheduling is very low, and its effect on the system schedulability is very small. Semi-partitioned scheduling indeed outperforms partitioned scheduling in realistic systems.

45. Distributing priorities and their implementation (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. We have proposed to 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. An optimization can be achieved by computing the knowledge from the controlled rather than the uncontrolled system..

This year we have used these previously developed techniques in order to achieve distributed monitoring, that is, in this case we do not necessarily want to prevent the property to be violated, but if it is, at least we want to know it (e.g. in order to launch a reparation activity). Replacing Control by monitoring allows weakening the enforced property, and thus decreases the complexity of the distributed implementation [GPQ11].

The before mentioned approaches are situated at an abstract level where synchronizations are the interaction primitive. In order to achieve a distributed implementation on real

distributed platform (where interaction is by message passing) we may use an existing algorithm such as α-core. in fact, we have also considered the direct implementation priorities in an algorithm directly based on message-based interactions. In particular, we have considered algorithms where the aim is not, as usually, to minimize the number of messages, but to privilege short sequences of message exchanges leading to a successful interaction [BGQ11], [BGM11], [BJG11].

47. Contract-based modeling and 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 [GPQ11]

50. Synthesis of efficient controllers in Probabilistic Environments (IST Austria + VERIMAG)

We have developed a general framework to evaluate and construct controllers with respect to how efficient they behave in a given probabilistic environment. A controller is a reactive system that regularly observes its environment and then provides control actions to influence the environment in the desired way. Efficiency is defined in terms of a cost model (e.g., energy consumption) and a reward model (e.g., reliability). The cost and the reward model associate to each sequence of actions a number indicating the current costs (and rewards, respectively). The controller aims to find an optimal trade-off between costs and rewards, e.g., to be energy efficient. Given our framework we show how to measure the efficiency of a given controller and how to construct a controller that is optimal, i.e., a controller that minimizes the ratio between the accumulated costs and the accumulated rewards.
We presented preliminary results for ergodic MDPs iWIGP 2011 [EJ11]. The full version including (i) the solution for the general case, (ii) a novel algorithm based on policy iteration, and (iii) an implementation will be presented in VMCAI 2012 [EJ12].

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.
Closely related to safety analysis, and as reported previously, KTH and SP have in collaboration been investigating robustness assessment through fault-injection (FI). A first step in this work has now been completed and a licentiate thesis was presented at KTH by Rickard Svenningsson [SV11]. Fault-injection (FI) is mandated by safety standards for highly critical functions (e.g. in IEC61508) and recommended in the ISO26262 when the claimed diagnosis coverage is at least 90%. One way of performing robustness assessment is to carry out fault injection, also known as fault insertion testing from certain safety standards. The idea behind fault injection is to accelerate the occurrence of faults in the system to evaluate its behavior under the influence of anticipated faults, and to evaluate error handling mechanisms. The thesis investigates how we can benefit from conducting fault injection experiments on behavior models of software by comparing model-implemented FI with traditional hardware and software level FI. The focus has been on the injection of abstractions of hardware fault effects (e.g. bit-level errors in microcontrollers) into Simulink models.
The results reveal that fault injection on software models is efficient and useful for robustness assessment and that results produced with the developed model-level FI tool (MODIFI) appear to be representative for the results obtained with other fault injection methods. However, a software model suppresses implementation details, thus leading to fewer locations where faults can be injected. Therefore it cannot entirely replace traditional fault injection methods, but by performing model-implemented fault injection in early design phases an overview of the robustness of a model can be obtained, given these limitations. It can also be useful for testing of error handling mechanisms that are implemented in the behavior model.

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.
We 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. The flow enables the integration of models from different high-level languages, allowing the interaction between domain experts. Recently we proposed an Intermediate Format based on the Metropolis II meta-model to serve as a common platform between

functional specifications of control algorithms to their implementation. We developed automatic translation from Modelica models to the IF and we demonstrated how to translate from Simulink and LabView models to IF.
Furthermore, we automatically optimized the implementation of the control algorithms on a distributed platform by selecting computation and communication resources, and by performing code generation on selected implementation platforms such as ALC and National Instruments controller boards while meeting the specification.

62. Distributed BIP (Verimag)
We have investigated and implemented methods for generating efficient distributed implementations from BIP.

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 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 [BBQ11], [CBC+11]

67. Power Isolation (Salzburg)
Salzburg introduced a new notion of so-called power isolation to model power consumption of individual software processes in isolation from each other [CKS11]. Power isolation may enable per-process accounting of power consumption in, e.g. cloud computing applications. The challenge is to identify lower and upper bounds on per-process power consumption that are independent of the overall system state despite the fact that power consumption is non-linear in both processor frequencies and voltage levels. In general, the share of a given process in overall power consumption varies with changes in the execution context of the

process. The key contribution of this work is an analysis of the relationship between isolation quality (difference in lower and upper bounds) and isolation cost (total power consumption) [CKS11].

68. Scheduling of Certifiable Mixed-Criticality Task Systems (Uppsala)
An increasing trend in embedded system design is to integrate components with different levels of criticality into a shared hardware platform for better cost and power efficiency. Such mixed-criticality systems are subject to certifications at different levels of rigorousness, for validating the correctness of different subsystems on various confidence levels. The real-time scheduling of certifiable mixed-criticality systems has been recognized to be a challenging problem, where using traditional scheduling techniques may result in unacceptable resource waste. In this work, we present an algorithm called PLRS to schedule certifiable mixed-criticality sporadic tasks systems. PLRS uses fixed-job-priority scheduling, and assigns job priorities by exploring and balancing the asymmetric effects between the workload on different criticality levels. Comparing with the state-of-the-art algorithm by Li and Baruah for such systems, which we refer to as LB, PLRS is both more effective and more efficient: (i) The schedulability test of PLRS not only theoretically dominates, but also on average significantly outperforms LBs. (ii) The run-time complexity of PLRS is polynomial (quadratic in the number of tasks), which is much more efficient than the pseudo-polynomial run-time complexity of LB.

69. Resource Sharing Protocols for Task Graph Systems (Uppsala)
Previous works on real-time task graph models have ignored the crucial resource sharing problem. Due to the nondeterministic branching behavior, resource sharing in graph-based task models is significantly more difficult than in the simple periodic or sporadic task models. In this work we address this problem with several different scheduling strategies, and quantitatively evaluate their performance. We first show that a direct application of the well-known EDF+SRP strategy to graph-based task models leads to an unbounded speedup factor. By slightly modifying EDF+SRP, we obtain a new scheduling strategy, called EDF+saSRP, which has a speedup factor of 2. Then we propose a novel resource sharing protocol, called ACP, to better manage resource sharing in the presence of branching structures. The scheduling strategy EDF+ACP which applies ACP to EDF, can achieve a speedup factor of 1.618, which is the golden ratio.

70. Protocol conversion (INRIA)
INRIA has made further progress on the protocol conversion approach for the correct-by-construction design of MPSoCs. This approach is also known as adapter synthesis. Specifically, we have extended this approach in two directions, first to take into account data mismatches between the components (on top of classical control mismatches), and second to generalize the approach to make it incremental. Incremental means that, starting from three components A, B, and D, a first converter C1 can be generated between components A and B, therefore yielding the assembly (A || C1 || B), and then a second converter C2 can be generated between this assembly and a third component D. This process is associative, meaning that we could have started with (B || C1' || D) and then generated a second converter C2' to solve the mismatches with A. Alternatively, a single converter C3 can be generated for A, B, and D directly, such that the three results are equivalent. This is the first result on protocol conversion that allows incremental design.

71. Offline multi-criteria scheduling for safety critical systems (INRIA)
INRIA has extended previous results on the design and modeling for reliability of safety-critical embedded real-time systems. We have proposed a new off-line tri-criteria scheduling heuristics (length, reliability, power) which, from a given software application graph and a given multiprocessor architecture (homogeneous and fully connected), produces a static

multiprocessor schedule that optimizes three criteria: its length (crucial for real-time systems), its reliability (crucial for dependable systems), and its power consumption (crucial for autonomous systems). Our tri-criteria scheduling heuristics, TSH, uses the active replication of the operations and the data-dependencies to increase the reliability, and uses dynamic voltage and frequency scaling to lower the power consumption [AGK11].

72. Dynamic reactive modules (IST Austria + U Leicester + Rice + Microsoft Research)
State-transition systems communicating by shared variables have been the underlying model of choice for applications of model checking. Such formalisms, however, have difficulty with modeling process creation or death and communication reconfigurability. In [FHN+11], we introduce “dynamic reactive modules”, (DRM) a state-transition modeling formalism that supports dynamic reconfiguration and creation/death of processes. The resulting formalism supports two types of variables, data variables and reference variables. Reference variables enable changing the connectivity between processes and referring to instances of processes. We show how this new formalism supports natural parallel composition and refinement through trace containment. DRM provide a natural language for modeling (and ultimately reasoning about) biological systems and multiple threads communicating through shared variables.

73. Request-response games (IST Austria + LIAFA)
In this work [CHH11], we consider two-player graph games whose objectives are request-response condition, i.-e conjunctions of conditions of the form “if a state with property *Rq* is visited, then later a state with property *Rp* is visited”. The winner of such games can be decided in EXPTIME and the problem is known to be NP-hard. In this paper, we close this gap by showing that this problem is, in fact, EXPTIME-complete. We show that the problem becomes PSPACE-complete if we only consider games played on DAGs, and NP-complete or PTIME-complete if there is only one player (depending on whether he wants to enforce or spoil the request-response condition). We also present near-optimal bounds on the memory needed to design winning strategies for each player, in each case.

74. Quantitative Specifications (IST Austria + Hebrew Uni)
In the first part of this work [BCHK11], we extend temporal logics with quantitative atomic assertions, aiming for a general and flexible framework for quantitative-oriented specifications. We investigate, in particular, the extension of temporal logics with the prefix-accumulation assertions Sum(v)c and Avg(v)c, where v is a numeric variable of the system, c is a constant rational number, and Sum(v) and Avg(v) denote the accumulated sum and average of the values of v from the beginning of the computation up to the current point of time. We also allow the path- accumulation assertions LimInfAvg(v)c and LimSupAvg(v)c, referring to the average value along an entire computation. We study the border of decidability for extensions of various temporal logics. In particular, we show that extending the fragment of CTL that has only the EX, EF, AX, and AG temporal modalities by prefix-accumulation assertions and extending LTL with path-accumulation assertions, result in temporal logics whose model-checking problem is decidable. The extended logics allow to significantly extending the currently known energy and mean-payoff objectives. Moreover, the prefix-accumulation assertions may be refined with “controlled-accumulation”, allowing, for example, specifying constraints on the average waiting time between a request and a grant. On the negative side, we show that the fragment we point to is, in a sense, the maximal logic whose extension with prefix-accumulation assertions permits a decidable model-checking procedure. Extending a temporal logic that has the EG or EU modalities, and in particular CTL and LTL, makes the problem undecidable.
In the second part of this work [BH11], we study specifications expressed in the form of non-deterministic discounted-sum automata (NDA), and study conditions in which these automata can be determinized. Discounted-sum automata are, in general, not determinizable: it is

currently known that for every rational discount factor 1 < c < 2, there is an NDA with c (denoted c-NDA) that cannot be determinized. We provide positive news, showing that every NDA with an integral factor is determinizable. We also complete the picture by proving that the integers characterize exactly the discount factors that guarantee determinizability: we show that for every rational factor c not in N, there is a non-determinizable c-NDA. Finally, we prove that the class of NDAs with integral discount factors enjoys closure under the algebraic operations min, max, addition, and subtraction, which is not the case for general NDAs nor for deterministic NDAs.

75. Development of a service oriented and model-driven approach towards efficient model and tool integration for embedded systems (KTH, ABB)

As mentioned in the previous deliverable, KTH has been addressing this topic as part of the iFEST and CESAR research projects. Tool integration is a multidimensional problem with many connotations. A common reference for assessing the problems, still widely referenced, is the integration dimensions established by Anthony Wasserman already in around 1990. Our investigation reveals that these dimensions are actually dependent and thus not actually dimensions. We have explored these dependencies and found them useful for reasoning about tool integration, for example for designing tool chains and in improving tool chains. Industrial case studies are planned to further evaluate these findings and to explore non-functional aspects of tool integration, [AB11].

As part of the iFEST research project a first version of a tool integration framework has been developed. The framework provides principles and specifications of services (functionalities and data) that provide uniform access to various types of tools including engineering tools for embedded systems development, cross-domain tools such as for configuration management, and basic tools such as model transformations. Initial experiments are very promising. A first set of designs and implementations will be available during the spring 2012. As part of the work we are exploring how to support tool-chain design through a model-based approach. A domain-specific modeling language is being developed that supports tool-chains modeling and generation of adaptors for tool integration [BE11].

76. A Schedulable Parametric DataFlow MoC (INRIA)

Recent data-flow programming environments support applications whose behavior is characterized by dynamic variations in resource requirements. The high expressive power of the underlying models (e.g., Kahn Process Networks, the CAL actor language) makes it challenging to ensure predictable behavior. In particular, checking liveness (i.e., no part of the system will deadlock) and boundedness (i.e., the system can be executed in finite memory) is known to be hard or even undecidable for such models. This situation is troublesome for the design of high-quality embedded systems.

We have introduced the Schedulable Parametric Data-Flow (SPDF) model of computation for dynamic streaming applications [FGP12]. SPDF extends the standard data flow model by allowing rates to be parametric (e.g., of the form 2.x.y). SPDF was designed to be statically analyzable while retaining sufficient expressive power. We formulated sufficient and general static criteria for boundedness and liveness. In SPDF, parameters can be changed dynamically even within iterations. The safety of dynamic parameter changes can be checked and their implementation made explicit in the graph. These different analyses are made possible using well-defined static operations on symbolic expressions. The same holds for quasi-static scheduling which is the first step towards code generation for multi-core systems.

77. Development of heterogeneous component models in the Metroll environment for BIP systems (TRENTO, VERIMAG).

The BIP and Metro II frameworks provide substantial complementary features, the first more oriented towards formal analysis, while the second more towards performance estimation.

For this reason we have found it interesting to integrate the tools as part of the modeling work. Our starting point is the C code generated from the S/R-BIP model, which is based on an explicit send-receive mechanism that more closely follows the communication structure required by MetroII. In MetroII the components communicate through dedicated channels that incorporate the computation performed by the BIP connectors. Components are recreated using the MetroII wrapper mechanism in order to expose the original ports, as well as all the variables required for the correct synchronization. Dedicated components called *engines* implement the connector functionality. However, interactions between components BIP are concretely realized by using a synchronization function call which carries information about the current component state and the ports available for interaction. When the BIP kernel receives all the requests from the components, it correlates the available ports with the list of registered interactions and sends the final decision back to the component, enabling or disabling their transitions to a new state. During code synthesis, this part of the model is not explicitly included into the generated C code of the BIP model. Therefore, in order to make the synthesized MetroII models independent from the BIP core system, we have reimplemented this mechanism in a separate MetroII component called *synchronizer*. This component plays the role of the BIP kernel where the decision about the next state transition of the component automata is taken. These model transformation rules have been implemented as an automatic BIP to MetroII ANTLR-based converter which takes as input the BIP functional model and produces a corresponding, structurally equivalent, MetroII functional model. The results have been submitted to publication.

78. Development of parametric quantitative models based on timed automata (TRENTO, ETHZ).
Modular Performance Analysis is an effective technique for the analysis of timed systems. This technique was recently extended to include state-based models, which are handled by integrating the analysis with timed automata. With this method, however, it is possible to analyze components only for a fixed set of parameters, e. g., fixed CPU speeds, fixed buffer sizes etc. In this work we are interested in studying the feasibility of a system in terms of deadline violation or more general properties as a set of architectural parameters are changed over a continuous region. To do so, we have developed a parametric timed automata model represented in the NuSMV and Uppaal languages
As part of this research project, we have developed a translator that takes as input an MPA description, and its equivalent timed automata representation, and translates it in a format suitable for parametric analysis using a combination of NuSMV and Uppaal. The translator takes care of the semantics adaptation, and in particular updates the model with the required error states necessary to represent the properties of interest. The tool-chain includes converters that translate Uppaal traces into NuSMV traces which are used in combination to speed-up the analysis. The results are reported in conference proceedings [SRPL11].

79. Specification formalisms for consumption (CISS) The problems of time-dependent behavior in general, and dynamic resource allocation in particular, pervade many aspects of modern life. Prominent examples range from reliability of efficient use of communication resources in a telecommunication network to allocation of tracks in a continental railway network, from scheduling the usage of computational resources on a chip for durations of nano-seconds to weekly, monthly or longer-range reactive planning in a factory or supply chains. The invited CACM paper [BFLM11] provides a full account of *priced timed automata*, which is an extension of timed automata with additional continuous cost variables, observer variables growing with positive – but possibly varying – rate. This model is particularly useful for modelling additional consumption of resource, e.g. energy. A number of decision problems related to priced timed automata and the principle underlying how they are settle is provided.

Energy games have recently abstracted a lot of attention. These are games played on finite weighted automata and concern the existence of infinite runs subject to boundary constraints on the accumulated weight, allowing e.g. only for behaviours where a resource is always available (nonnegative accumulated weight), yet does not exceed a given maximum capacity. In [FJLS11] we extend energy games to a multi-weighted and parameterized setting, allowing us to model systems with multiple quantitative aspects. We present reductions between Petri nets and multi-weighted automata and among different types of multi-weighted automata and identify new complexity and (un)decidability results for both one- and two-player games. We also investigate the tractability of an extension of multi-weighted energy games in the setting of timed automata.

80. Simpler and more Uniform component modeling (Uppsala in collaboration with Oxford University) We propose a compositional specification theory for reasoning about components that interact by synchronisation of input and output (I/O) actions, in which the specification of a component constrains the temporal ordering of interactions with the environment. The theory is similar in spirit to Interface automata, proposed by de Alfaro and Henzinger, but provides (in our view) a more general and uniform treatment. On the one hand, the theory supports parallel composition, logical conjunction for independent development, and quotient for incremental development (synthesis of missing components). On the other hand, the conceptual development is streamlined so that a single concept of "inconsistency" is able to cover (1) assumptions on the input provided by the environment; (2) under specification, meaning that it is uncertain what the allowable interactions are; and (3) various (run-time) errors, including communication mismatch, bad behaviour, or divergence. The conceptual development is supported by a natural full-abstraction result [CCJ*12].

81. Automated learning of Models with Data (Uppsala in collaboration with Dortmund University) We have developed a novel approach for generating models of automata extended with data. The approach includes a novel canonical automaton model, based on register automata that can be used to specify protocol or program behavior. A major contribution is the definition of a canonical automaton representation of any language recognizable by a deterministic register automaton, by means of a Nerode congruence. We have used this automaton model for extending the standard active learning algorithm L* to handle also data-aspects of component behavior. Our active learning algorithm is unique in that it directly infers the effect of data values on control flow as part of the learning process. This effect is expressed by means of registers and guarded transitions in the resulting register automata models [CHJ+11, HSC+12].

-- Changes wrt Y3 deliverable --

This is new text, not present in Y3 deliverables. We have kept the numbering scheme from last year: items with number below 66 are continuations of earlier work, items with higher numbers correspond to new work lines, and missing number to lines of work which has not been continued or on which no significant progress has been achieved this year.

3.2 Individual Publications Resulting from these Achievements

CEA

[ATKGT11] S. Anssi, S. Tucci-Piergiovanni, S. Kuntz, S. Gérard, F. Terrier, "Enabling Scheduling Analysis for AUTOSAR Systems". In Proceedings of the 14th IEEE International Symposium on Object/component/service-oriented Real-time distributed computing (ISORC 2011)

[KCGT11] Ali Koudri, Arnaud Cuccuru, Sebastien Gerard and François Terrier, "Designing heterogeneous component based systems: evaluation of MARTE standard and enhancement proposal," in Proceedings of the 14th international conference on Model driven engineering languages and systems, Wellington, New Zealand, 2011, pp. 243-257.

[MTG11] C. Mraidha, S. Tucci-Piergiovanni, S. Gerard, "Optimum: a MARTE-based methodology for schedulability analysis at early design stages". ACM SIGSOFT Software Engineering Notes 36(1): 1-8 (2011)

[TMWLG11] S. Tucci-Piergiovanni, C. Mraidha, E. Wozniak, A. Lanusse, S. Gerard, "A UML Model-Based Approach for Replication Assessment of AUTOSAR Safety-Critical Applications" in Proceedings of the 8th IEEE International Conference on Embedded Software and Systems (ICESS 2011)

[WMGT11] Ernest Wozniak, Chokri Mraidha, Sébastien Gérard and François Terrier, "A Guidance Framework for the Generation of Implementation Models in the Automotive Domain," in *presented at the 2nd international workshop DANCE, (Distributed Architecture modeling for Novel Component based Embedded systems), and published in the proceedings of the 37th EUROMICRO Conference on Software Engineering and Advanced Applications (SEAA 2011)*, Oulu, Finland, 2011, pp. 468-476.

[WBKRG11] Gereon Weiss, Klaus Becker, Benjamin Kamphausen, Ansgar Radermacher and Sébastien Gérard, "Model-Driven Development of Self-Describing Components for Self-Adaptive Distributed Embedded Systems," in 2nd international workshop DANCE, (Distributed Architecture modeling for Novel Component based Embedded systems), and published in the proceedings of the 37th EUROMICRO Conference on Software Engineering and Advanced Applications (SEAA 2011), Oulu, Finland, 2011, pp. 477-484.

CISS

[BFLM11] Patricia Bouyer, Ulrich Fahrenberg, Kim G. Larsen, and Nicolas Markey. Quantitative modelling and analysis of embedded systems. Communications of the ACM, 2011. Invited paper.

[MCL11] Radu Mardare, Luca Cardelli, and Kim G. Larsen. Continuous markovian logic - from complete axiomatization to the metric space of formulas. In Computer Science Logic (CSL), 25th International Workshop / 20th Annual Conference of the EACSL, CSL 2011, September 12-15, 2011, Bergen, Norway, Proceedings, LIPIcs, pages 144–158. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik,2011.

[CLM11] Luca Cardelli, Kim G. Larsen, and Radu Mardare. Modular markovian logic. In Automata, Languages and Programming - 38th International Colloquium, ICALP 2011, Zurich, Switzerland, July 4-8, 2011, Proceedings, Part II, pages 380–391, 2011.

[BKLMS11] Beneš, J. Křesinský, K.G. Larsen, M.H. Møller, and J. Srba. Parametric modal transition systems. In Proceedings of the 9th International Symposium on Automated Technology for Verification and Analysis (ATVA'11), LNCS. Springer-Verlag, 2011.

ESI

[HGB11] M. Hendriks, M. Geilen, T. Basten. Pareto Analysis with Uncertainty. In 9th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, EUC 2011, Proceedings. Melbourne, Australia, October 24-26, 2011. IEEE Computer Society Press, Los Alamitos, CA, USA, 2011.

[SBA+11] S. Stuijk, T. Basten, B. Akesson, M. Geilen, O. Moreira, J. Reineke. Designing Next-Generation Real-Time Streaming Systems. In 9th IEEE/ACM International Conference on Hardware/Software-Codesign and System Synthesis, CODES+ISSS 2011, Proceedings, pages 375-376. Tutorial. Part of the Embedded Systems Week. Taipei, Taiwan, October 9-14, 2011. ACM, NY, NY, USA, 2011.

[DST+11] M. Damavandpeyma, S. Stuijk, T. Basten, M. Geilen, H. Corporaal. Hybrid Code-Data Prefetch-Aware Multiprocessor Task Graph Scheduling. In 14th Euromicro Conference On Digital System Design: Architectures, Methods and Tools, DSD 2011, Proceedings, pages 583-590. Oulu, Finland, 31 August - 2 September 2011. IEEE Computer Society Press, Los Alamitos, CA, USA, 2011.

[YGB+11] Y. Yang, M. Geilen, T. Basten, S. Stuijk, H. Corporaal. Iteration-based Trade-off Analysis of Resource-aware SDF. In 14th Euromicro Conference On Digital System Design: Architectures, Methods and Tools, DSD 2011, Proceedings, pages 567-574. Oulu, Finland, 31 August - 2 September 2011. IEEE Computer Society Press, Los Alamitos, CA, USA, 2011.

[SGT+11] S. Stuijk, M. Geilen, B. Theelen, T. Basten. Scenario-Aware Dataflow: Modeling, Analysis and Implementation of Dynamic Applications. In L. Carro and A.D. Pimentel, editors, International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation, IC-SAMOS 11, Proceedings, pages 404-411. Samos, Greece, 18-21 July 2011. IEEE Computer Society Press, Los Alamitos, CA, USA, 2011.

[THB+11] N. Trcka, M. Hendriks, T. Basten, M. Geilen, L. Somers. Integrated Model-Driven Design-Space Exploration for Embedded Systems. In L. Carro and A.D. Pimentel, editors, International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation, IC-SAMOS 11, Proceedings, pages 339-346. Samos, Greece, 18-21 July 2011. IEEE Computer Society Press, Los Alamitos, CA, USA, 2011.

[NVB11] N. Trcka, M. Voorhoeve, T. Basten. Parameterized Partial Orders for Modeling Embedded System Use Cases: Formal Definition and Translation to Coloured Petri Nets. In Application of Concurrency to System Design, 11th International Conference, ACSD 2011, Proceedings, pages 13-18. Newcastle upon Tyne, UK, 20-24 June 2011. IEEE Computer Society Press, Los Alamitos, CA, USA, 2011.

[VHT+11] J.P.M. Voeten, T. Hendriks, B.D. Theelen, J. Schuddemat, W. Tabingh Suermondt, J. Gemei, K. Kotterink and C. van Huet. Predicting Timing Performance of Advanced Mechatronics Control Systems In: Proceedings of the IEEE Computer Software and Applications Conference Workshops (COMPSAC), pp. 206-210, 2011

[TGV11] B.D. Theelen, M.C.W. Geilen, and J.P.M. Voeten. Performance Model Checking Scenario-Aware Dataflow In: Proceedings of the International Conference on Formal

Modeling and Analysis of Timed Systems (FORMATS), LNCS 6919, pp. 43-59, Springer 2011

[TKW12] B.D. Theelen, J.-P. Katoen and H. Wu. Model Checking of Scenario-Aware Dataflow with CADP To be published in: Proceedings of Design, Automation and Test in Europe (DATE), 2012

[HHS11] J. Hooman, Huis in 't Veld, and M. Schuts. Experiences with a Compositional Model Checker in the Healthcare Domain, Foundations of Health Information Engineering and Systems (FHIES 2011), Pre-symposium Proceedings, UNU-IIST Report 454, McSCert Report 5, pp. 92-109, 2011

[HV11] R. Hamberg and J. Verriet (Eds). Automation in Warehouse Development, Springer, London, 2011

INRIA

[AGK11] I. Assayad, A. Girault, and H. Kalla, "Tradeoff exploration between reliability, power consumption, and execution time", in SAFECOMP'11, Napoli, Italy, September 2011

[FGP12] Pascal Fradet, Alain Girault, and Peter Poplavko, "SPDF: A Schedulable Parametric DataFlow MoC", To appear in Proc. Design, Automation and Test in Europe Conference (DATE'12), Dresden, Germany, March 2012.

IST

[BH11] Udi Boker, Thomas A. Henzinger: Determinizing Discounted-Sum Automata. CSL 2011: 82-96

KTH

[AB11] Fredrik Asplund, Matthias Biehl, Jad Elkhoury and Martin Törngren. Tool Integration Beyond Wasserman. INISET 2011: First Workshop on Integration of Information Systems Engineering Tools, part of the 23rd International Conference on Advanced Information System Engineering (CAISE 2011).

[BE11] Matthias Biehl, Jad El-Khoury, Frédéric Loiret, Martin Törngren. A Domain Specific Language for Generating Tool Integration Solutions. 4th Workshop on Model-Driven Tool & Process Integration (MDTPI2011) at the European Conference on Modelling Foundations and Applications (ECMFA 2011), June 6th 2011, Birmingham, UK

[NC11a] Tahir Naseer Qureshi, DeJiu Chen, Magnus Persson, Martin Törngren. Towards the Integration of UPPAAL for Formal Verification of EAST-ADL Timing Constraint Specification. The 1st International Workshop on Model-Based Design with a Focus on Extra-Functional Properties (MBDEFP) October 13th 2011, Taipei, Taiwan.

[SV11]. Rickard Svenningsson. Licentiate thesis: Model-Implemented Fault Injection for Robustness Assessment. Presented at KTH, Dec. 9th 2011. TRITA MMK 2011:16, ISSN 1400-1179, ISRN KTH/MMK/R-11/16-SE, ISBN 978-91-7501-173-8.

Salzburg

[CKS11] S.S. Craciunas, C.M. Kirsch, and A. Sokolova. The power of isolation. Technical Report 2011-02, Department of Computer Sciences, University of Salzburg, July 2011.

[KSPHHCLRT12] C.M. Kirsch, R. Sengupta, E. Pereira, J. Huan, R. Hansen, H. Chen, F. Landolt, A. Rottmann, and R. Trummer. Cyber-physical cloud computing: The binding and migration problem. In Proc. International Conference on Design, Automation and Test in Europe (DATE), 2012.

[KLMS11] C.M. Kirsch, L. Lopes, E.R.B. Marques, and A. Sokolova. Runtime programming through model-preserving, scalable runtime patches. In Proc. International Conference on Application of Concurrency to System Design (ACSD), pages 77–86. IEEE, 2011.

Trento

[RPMP11] Tizar Rizano, Roberto Passerone, David Macii and Luigi Palopoli, Model-Based Design of Embedded Control Software for Hybrid Vehicles. In Proceedings of the 6th IEEE International Symposium on Industrial Embedded Systems (SIES11), Västerås, Sweden, June 15-17, 2011.

Uppsala

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

[GLGY12] Nan Guan, Mingsong Lv, Yu Ge and Wang Yi. WCET Analysis with MRU Caches: Challenging LRU for Predictability. To appear in the proc. of RTAS 2012.

[GSGY12] Nan Guan, Martin Stigge, Yu Ge, and Wang Yi. Parametric Utilization Bounds for Fixed-Priority Multiprocessor Scheduling. In the proc. of the 26th IEEE International Parallel and Distributed Processing Symposium. May 21-25, 2012, Shanghai, China.

[GESY11a] Nan Guan, Pontus Ekberg, Martin Stigge and Wang Yi. Effective and Efficient Scheduling of Certifiable Mixed-Criticality Sporadic Task Systems. In the proc. of IEEE RTSS 2011, Vienna, Austria. Nov 30 - Dec 2, 2011

[LGDYY11] Mingsong Lv, Nan Guan, Qingxu Deng, Ge Yu, Wang Yi: McAiT - A Timing Analyzer for Multicore Real-Time Software. In the proc. of ATVA 2011: 414-417.

[ZGXY11] Yi Zhang, Nan Guan, Yanbin Xiao, Wang Yi. Implementation and Empirical Comparison of Partitioning-based Multi-core Scheduling. In the proc. of the 6th IEEE International Symposium on Industrial Embedded Systems (SIES11), Vaesteraas, Sweden, June 15th - 17th, 2011.

[SEGY11a] Martin Stigge, Pontus Ekberg, Nan Guan, and Wang Yi. On the Tractability of Digraph-Based Task Models. In the proc of the 23rd Euromicro Conference on Real-Time Systems, Porto, Portugal July 6th - 8th, 2011.

[JGDY11] Xi Jin, Nan Guan, Qingxu Deng, Wang Yi. Memory Aware Mapping for Network-on-Chips, In the proc. of the 17th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA 2011), August 28-31, Toyama, Japan.

[GESY11b] Nan Guan, Pontus Ekberg, Martin Stigge and Wang Yi. Resource Sharing Protocols for Real-Time Task Graph Systems. In the proc. of the 23rd Euromicro Conference on Real-Time Systems. Porto, Portugal July 6th - 8th, 2011.

[SEGY11b] Martin Stigge, Pontus Ekberg, Nan Guan and Wang Yi. The Digraph Real-Time Task Model. In the proc. of the 17th IEEE Real-Time and Embedded Technology and

Applications Symposium, Chicago, IL, USA April 11-14, 2011. **Best Paper Nomination**.

[GYDGY11] Nan Guan, Wang Yi, Qingxu Deng, Zonghua Gu, Ge Yu. Schedulability analysis for non-preemptive fixed-priority multiprocessor scheduling. Journal of Systems Architecture – Embedded Systems Design 57(5): 536-546 (2011).

[KYD11] Fanxin Kong, Wang Yi, Qingxu Deng. Energy-efficient scheduling of real-time tasks on cluster-based multicores. In the proc. of DATE 2011: 1135-1140.

[KGDY11] Fanxin Kong, Nan Guan, Qingxu Deng, Wang Yi. Energy-efficient scheduling for parallel real-time tasks based on level-packing. In the proc of ACM SAC 2011: 635-640.

VERIMAG

[ASR+11] Takoua Abdellatif, Lilia Sfaxi, Riadh Robbana, Yassine Lakhnech , Information Flow Control of Component-based Distributed Systems. - Concurrency and Computation, Practice and Experience

[**BBQ11**] B. Bonakdarpour, M. Bozga, J. Quilbeuf Automated Distributed Implementation of Component-Based Models with Priorities In EMSOFT'11 Conference

[BBB+11] Rigorous Component-Based System Design Using the BIP Framework. Ananda Basu, Saddek Bensalem, Marius Bozga, Jacques Combaz, Mohamad Jaber, Thanh-Hung Nguyen, Joseph Sifakis - IEEE Software

[BGQ11] Imene Ben-Hafaiedh, Susanne Graf, Sophie Quinton, Building Distributed Controllers for Systems with Priorities. - Journal of Logic and Algebraic Programming

[BGJ11] Imene Ben-Hafaiedh, Susanne Graf, Mohamad Jaber, Model-based design and Distributed Implementation of Bus Arbiter for Multiprocessors. IEEE International Conference on Electronics, Circuits, and Systems

[BGM11] Distributed Implementation of Systems with Multiparty Interactions and Priorities. Imene Ben-Hafaiedh, Susanne Graf, Nejla Mazouz - Proc. of SEFM'11

[BMM11] Nicolas Berthier, Florence Maraninchi, and Laurent Mounier. Synchronous Programming of Device Drivers for Global Resource Control in Embedded Operating Systems. - ACM SIGPLAN/SIGBED Conference on Languages, Compilers, Tools and Theory for Embedded Systems (LCTES)

[BS11] Synthesizing Glue Operators from Glue Constraints for the Construction of Component-Based Systems. Simon Bliudze, Joseph Sifakis - Software Composition - 10th International Conference, SC 2011, Zurich, Switzerland, June 30 - July 1, 2011. Proceedings

[**CBC+11**] Chih-Hong Cheng, Saddek Bensalem, Yu-Fang Chen, Rongjie Yan, Barbara Jobstmann, Harald Ruess, Christian Buckl, Alois Knoll: Algorithms for Synthesizing Priorities in Component-Based Systems. ATVA 2011: 150-167

[CHJ11] QUASY: Quantitative Synthesis Tool. Krishnendu Chatterjee, Thomas A. Henzinger, Barbara Jobstmann, Rohit Singh - Tools and Algorithms for the Construction and Analysis of Systems (TACAS) 2011

[EJ11] Synthesizing Systems with Optimal Average-Case Behavior for Ratio Objectives. Christian von Essen, Barbara Jobstmann - International Workshop on Interactions, Games and Protocols, 2011

[**GPQ11**] Susanne Graf, Doron Peled, Sophie Quinton, Monitoring Distributed Systems Using Knowledge. - Formal Techniques for Distributed Systems - Joint 13th IFIP WG 6.1 International Conference, FMOODS 2011, and 31st IFIP WG 6.1 International Conference, FORTE 2011, Reykjavik, Iceland, June 6-9, 2011

[FM11] Modeling of Time in Discrete-Event Simulation of Systems-on-Chip. Giovanni Funchal, Matthieu Moy - ACM/IEEE Ninth International Conference on Formal Methods and Models for Codesign MEMOCODE 2011

[FFM11] Ylies Falcone, Jean-Claude Fernandez, Laurent Mounier. What can you Verify and Enforce at Runtime ? - Software Tool in Technology Transfer (STTT) 2011

[FFMR11] Ylies Falcone, Jean-Claude Fernandez, Laurent Mounier and Jean-Luc Richier. Runtime Enforcement Monitors: composition, synthesis, and enforcement abilities. - Formal Methods in System Design, 2011

[Sif11] Joseph Sifakis A vision for computer science - the system perspective. - Central Europ. J. Computer Science

[Sif11b] Methods and tools for component-based system design. Joseph Sifakis - Design, Automation and Test in Europe, DATE 2011, Grenoble, France, March 14-18, 2011

-- Changes wrt Y3 deliverable --

This is new text, not present in Y3 deliverables.

3.3 Interaction and Building Excellence between Partners

Trento, KTH and UC Berkeley. Martin Törngren, KTH, was invited to UC Berkeley as a visiting scholar to promote collaboration with Berkeley as well as with Trento through Alberto Sangiovanni-Vincentelli for the period Sept through December 2011. The autumn was fruitful and several collaborations have been initiated including a study on real-time control systems based design approaches and Martin has also participated in ongoing work in combining the strengths of the Ptolemy II and MetroII approaches and environments.

Trento and **UC Berkeley**. focused on the challenges of modeling cyber–physical systems (CPSs) that arise from the intrinsic heterogeneity, concurrency, and sensitivity to timing of such systems. It used a portion of an aircraft vehicle management system (VMS), specifically the fuel management subsystem, to illustrate the challenges, and then discusses technologies that at least partially address the challenges. Specific technologies described include hybrid system modeling and simulation, concurrent and heterogeneous models of computation, the use of domain-specific ontologies to enhance modularity, and the joint modeling of functionality and implementation architectures [DLSV11]

Trento and **UC Berkeley** explored the use of the theory of contracts to model the interaction between analog and digital circuits. We developed a design flow for such systems that used contracts also to validate model abstractions and design refinement (vertical contracts) [NSV12].In the course of ARTIST, startet a close collaboration between CEA, KTH, Volvo, OFFIS and some ARTIST affiliated partners around models for real-time systems and there use for validation and code generation, 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.. This collaboration started in ATTEST, then ATTEST2, ADAMS, MAENAD and several more projects. and new projects are being started. This collaboration will well continue after the end of ARTIST.

IST Austria + VERIMAG continue collaborating on robust synthesis [EJ11,EJ12].

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, **OFFIS**, **IST-Austria**, **TRENTO** and **Verimag** have been collaborating intensely on the definition of contract-based theories. This collaboration will clearly continue beyond the duration of ARTIST. A collaboration about synthesis, and in particular contract-based synthesis is being envisaged.

Salzburg + IST We have obtained preliminary research results on relaxing semantics of concurrent data structures for improved performance and scalability. This work is part of the rigorous systems engineering (RiSE) initiative in Austria.

Uppsala is collaborating with **ETHZ** Absint, ETH Zurich, TU Braunschweig and Verimag on Mixed Criticality Systems (MCS).

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 particular, this year **TRENTO** and **VERIMAG** have collaborated on the combination of different contract and component frameworks to achieve a combined reasoning framework **[GPQ11]**.
- 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 particular, **TRENTO** and **VERIMAG** are collaborating for the development of an integrated modeling and analysis tool-chain between the BIP and the MetroII environments. And **TRENTO** and **ETHZ** are collaborating for the integration of parametric timed models and analysis into the MPA environment.
- **CEA** and **KTH** collaborate in the 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 Y3 deliverable --

This is new text, not present in Y3 deliverables.

3.4 Joint Publications Resulting from these Achievements

[AZ11] Eric Armengaud, Markus Zoier, Andreas Baumgart, Matthias Biehl, DeJiu Chen, Gerhard Griessnig, Christian Hein, Tom Ritter, Ramin T. Kolagari. Model-based Toolchain for the Efficient Development of Safety-Relevant Automotive Embedded Systems. SAE 2011 World Congress & Exhibition, April 2011, Detroit, USA

[BFJLLT11] Sebastian S. Bauer, Uli Fahrenberg, Line Juhl, Kim G. Larsen, Axel Legay, and Claus Thrane. Quantitative refinement for weighted modal transition systems. In Mathematical Foundations of Computer Science 2011 - 36th International Symposium, MFCS 2011, Warsaw, Poland, August 22-26, 2011. Proceedings, volume 6907 of LNCS, pages 60–71. Springer-Verlag, 2011.

[BJLLS11] Sebastian S. Bauer, Line Juhl, Kim G. Larsen, Axel Legay, and Jiri Srba. Extending modal transition systems with structured labels. Mathematical Structures in Computer Science, 2011

[BLLNW11] Sebastian Bauer, Kim G. Larsen, Axel Legay, Ulrik Nyman, and Andrzej Wąsowski. A modal specification theory for components with data. In 8th International Symposium on Formal Aspects of Component Software, Oslo, Norway, September 14-16, 2011, 2011. (Best Paper Award)

[BDLPY11] Gerd Behrmann, Alexandre David, Kim Guldstrand Larsen, Paul Pettersson and Wang Yi. Developing UPPAAL over 15 years. In Journal: Software - Practice and Experience, 41(2): 133-142 (2011).

[BCHK11] Udi Boker, Krishnendu Chatterjee, Thomas A. Henzinger, Orna Kupferman: Temporal Specifications with Accumulative Values. LICS 2011: 43-52

[BFLM11] Patricia Bouyer, Ulrich Fahrenberg, Kim G. Larsen, and Nicolas Markey. Quantitative modelling and analysis of embedded systems. Communications of the ACM, 2011. Invited paper.

[BS11] Synthesizing Glue Operators from Glue Constraints for the Construction of Component-Based Systems. Simon Bliudze, Joseph Sifakis - Software Composition - 10th International Conference, SC 2011, Zurich, Switzerland, June 30 - July 1, 2011. Proceedings

[CCH+11] Pavol Cerný, Krishnendu Chatterjee, Thomas A. Henzinger, Arjun Radhakrishna, Rohit Singh: Quantitative Synthesis for Concurrent Programs. CAV 2011: 243-259

[CCJ*12] Taolue Chen, Chris Chilton, Bengt Jonsson, Marta Kwiatkowska: A Compositional Specification Theory for Component Behaviours.
In Proc. ESOP (European Symp. on Programming) 2012, to appear

[CHJ11] Krishnendu Chatterjee, Thomas A. Henzinger, Barbara Jobstmann, Rohit Singh QUASY: Quantitative Synthesis Tool. Tools and Algorithms for the Construction and Analysis of Systems (TACAS) 2011

[CHJM+11] Sofia Cassel, Falk Howar, Bengt Jonsson, Maik Merten, Bernhard Steffen: A Succinct Canonical Register Automaton Model, ATVA 2011

[CHH+11] Krishnendu Chatterjee, Thomas A. Henzinger, Florian Horn: The Complexity of Request-Response Games. LATA 2011: 227-237

[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

[CJ11] DeJiu Chen, Rolf Johansson, Henrik Lönn, Hans Blom, Martin Walker, Yiannis Papadopoulos, Sandra Torchiaro, Fulvio Tagliabo, Anders Sandberg: Integrated Safety and Architecture Modeling for Automotive Embedded Systems. e&i - elektrotechnik und informationstechnik, Volume 128, Number 6, Automotive Embedded Systems. Springer Wien, 2011. ISSN 0932-383X / 1613-7620.

[DLSV11] Patricia Derler, Edward Lee and Alberto Sangiovanni Vincentelli, Modeling Cyber–Physical Systems, Proceedings of the IEEE, Vol. 100, n.1, January 2012, invited paper.

[EJ11] Christian von Essen and Barbara Jobstmann. Synthesizing systems with optimal average-case behavior for ratio objectives. In International Workshop on Interactions, Games and Protocols (iWIGP), pages 17-32, 2011.

[EJ12] Christian von Essen and Barbara Jobstmann. Synthesizing efficient controllers. In International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI), 2012. To appear.

[FFMR11] Ylies Falcone, Jean-Claude Fernandez, Laurent Mounier and Jean-Luc Richier. Runtime Enforcement Monitors: composition, synthesis, and enforcement abilities. - Formal Methods in System Design, 2011

[FHN+11] Jasmin Fisher, Thomas A. Henzinger, Dejan Nickovic, Nir Piterman, Anmol V. Singh, Moshe Y. Vardi: Dynamic Reactive Modules. CONCUR 2011: 404-418

[GPQ11] Graf, Susanne and Passerone, Roberto and Quinton, Sophie "Contract-Based Reasoning for Component Systems with Complex Interactions", TIMOBD 2011

[HSC+12] Falk Howar, Bernhard Steffen, Sofia Cassel, Bengt Jonsson: Inferring Canonical Register Automata. To appear in VMCAI 2012

[LDZS11] C.-W. Lin, M. Di Natale, H. Zeng, A. Sangiovanni-Vincentelli, "Performance analysis of synchronous models implementations on loosely time-triggered architectures," in Work-in-Progress Session of IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS-2011), Chicago, IL, Apr. 2011.

[MD11] Maenad Deliverable 2011: D3.1.1 Language Concepts Supporting Engineering Scenarios. Public deliverable of the Maenad FP7 project, 2011. http://www.maenad.eu/public_pw/Maenad_Deliverable_D3.1.1_V1.0.1.pdf (Current release. A new release is scheduled in December 2011)

[MPS11] M. Maasoumy, A. Pinto, and A. Sangiovanni-Vincentelli. "Model-based hierarchical optimal control design for HVAC systems." In Dynamic System Control Conference (DSCC), 2011. ASME, 2011

[MPPLS11] Mohammad Mozumdar, Alberto Puggelli, Alessandro Pinto, Luciano Lavagno, Alberto L. Sangiovanni-Vincentelli "A hierarchical wireless network architecture for building automation and control systems", The Seventh International Conference on Networking and Services , pages 178 -183, 2011, ISBN: 978-1-61208-133-5, Venice, Italy

[NC11b] Qureshi, Tahir Naseer; Chen, DeJiu; Lönn,Henrik ; Törngren, Martin: From EAST-ADL to AUTOSAR Software Architecture: A Mapping Scheme, the 5th European Conference on Software Architecture (ECSA 2011), Essen, Germany, 13-16 September 2011

[NSV12] P. Nuzzo, A. Sangiovanni Vincentelli, X. Sun, A. Puggelli, A Methodology for the Design of Analog Integrated Interfaces Using Contracts, IEEE Sensors Journal, 2012, invited paper.

[PMPLSV11] Alberto Puggelli, Mohammad Mozumdar, Alessandro Pinto, Luciano Lavagno, Alberto Sangiovanni-Vincentelli. "A Routing-Algorithm-Aware Design Tool for Indoor Wireless Sensor Networks". Proceedings of the IEEE International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 2012.

[RBBC11] Jean-Baptiste Raclet, Eric Badouel, Albert Benveniste, Benoît Caillaud, Axel Legay and Roberto Passerone. A Modal Interface Theory for Component-based Design. Fundamenta Informaticae, 108(1-2):119-149, 2011.

[SC11] 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. Lecture Notes in Computer Science, Volume 6351, Series: Computer Safety, Reliability, and Security (SAFECOMP), Pages 332-346. Springer Berlin / Heidelberg, 2011. ISSN 0302-9743

[SRPL11] Alena Simalatsar, Yusi Ramadian, Roberto Passerone, Kai Lampka, Simon Perathoner and Lothar Thiele. Enabling Parametric Feasibility Analysis in Real-time Calculus Driven Performance Evaluation. In Proceedings of the International Conference on Compilers, Architectures and Synthesis of Embedded Systems (CASES11), Taipei, Taiwan, October 9-14, 2011.

[TLHL11] Stavros Tripakis, Ben Lickly, Thomas A. Henzinger, Edward A. Lee: A Theory of Synchronous Relational Interfaces. ACM Trans. Program. Lang. Syst. 33(4): 14 (2011)

[ZDGS11] Haibo Zeng, Marco Di Natale, Arkadeb Ghosal, and Alberto Sangiovanni-Vincentelli. Schedule Optimization of Time-Triggered Systems Communicating over the FlexRay Static Segment. IEEE Transactions on Industrial Informatics, Vol. 7, No. 1, February 2011, 1-17.

-- Changes wrt Y3 deliverable --

This is new text, not present in Y3 deliverables.

3.5 Keynotes, Workshops, Tutorials

Keynote: Twan Basten
The disappearing computer
Devlab Café, Development Laboratories, Eindhoven, the Netherlands, 29 April 2011

Keynote: Jeroen Voeten
Performance prediction and optimization for Wafer Scanners
Dutch Model Checking Day 2011, Delft, the Netherlands, 17 June 2011

Keynote: Jozef Hooman
Using a Commercial Model Checker at Philips Healthcare
System Validation seminar, University of Twente, the Netherlands, 23 May 2011

Keynote: Jozef Hooman
Compositional Model Checking using Verum's ASD:Suite at Philips Healthcare
MBSD seminar, Radboud University, Nijmegen, the Netherlands, 1 July 2011

Keynote: Jozef Hooman
Experiences with a Compositional Model Checker in the Healthcare Domain

International Symposium on Foundations of Health Information Engineering and Systems (FHIES 2011), Johannesburg, South Africa, 30 August 2011

Keynote: *Sara Tucci*
AUTOSAR Timing Extension and a Case Study for Schedulability Analysis
ArtistDesign Workshop on Real-Time System Models for Schedulability analysis University of Cantabria 7-8 February 2011

Keynote: *Sara Tucci*
Applying Model Driven Engineering to RTES: Technologies, Standards and Experiences
ES-week Workshop on Time Analysis and Model-Based Design, from Functional Models to Distributed Deployments, Taipei, 2011

Keynote: Wang Yi
The Digraph Real-Time Task Model, invited talk, Workshop on Rigorous Embedded Design 2011, April 10th, 2011, Salzburg, Austria (within EuroSys 2011).

Keynote Lecture: Thomas A. Henzinger
Computational Science versus Computer Science, Ninth Basel Computational Biology Conference (BC2), Basel, Switzerland, June 2011.

Keynote Lecture: Joseph Sifakis
Trustworthy Software Systems, int conf on Sensornetworks Sensornets February 2012, Rome

Keynote Lecture: Joseph Sifakis
Rigorous System Design, VLSI-SoC, October 3–5, 2011, Hong Kong, China

Keynote Lecture: Joseph Sifakis
Methods and tools for component-based system design, DATE 2011, Grenoble

Key Note: The Major Challenges of the EDA Industry in the Next 5 Years
Tel Aviv, May 3, 2011
Alberto Sangiovanni Vincentelli gave the key note address at the Israel Executive Forum addressing the future directions of the EDA industry.
http://www.israelexecutiveforum.com/agenda.aspx

Key Note: 1,000 Electronic Devices Per Living Person: Dream Or Nightmare?, 4th IEEE International Workshop on Advances in Sensors and Interfaces
Borgo Egnazia, June 9th, 2011
Alberto Sangiovanni Vincentelli gave the opening key note talking about the potential offered by the myriad of sensors, controller and actuators that will be soon available.
http://iwasi2011.poliba.it/programme.html

Key Note: 1000 electronic devices per person, dream or nightmare, International Electronic Forum, Future Horizon
Seville, October 7th, 2011
Alberto Sangiovanni Vincentelli delivered this talk to an audience consisting of CEO, COO and CTO of the semiconductor industry.

Key Note: Application Driven Design – New Directions Require New Tools!
Tel Aviv, May 4, 2011

Alberto Sangiovanni Vincentelli gave the key note at this conference stressing the need for new tools for system level design. He was awarded at the Conference with the ChipEx Award for exceptional contribution to the semiconductor industry delivered by the Science and Technology Minister of Israel Professor Daniel Hershkovitz (see picture below).

Key Note: DAC Workshop
San Diego, June 5th, 2011
Alberto Sangiovanni Vincentelli chaired and gave the opening key note talk at the DAC Workshop on Intra and Inter-Vehicle Networking.
Key Note and Workshop: DAC Workshop on Design Analysis and Implementation of Real-Time Systems with Time-Triggered and Event-Triggered Applications
San Diego, June 5th , 2011
Alberto Sangiovanni Vincentelli chaired and presented the Key Note opening address

***Invited Lecture*:**
Haifa, March 8, 2011
Alberto Sangiovanni Vincentelli gave a distinguished seminar talk at Haifa IBM Research attended by all researchers on System and Contract-Based Design.

Invited Lecture:
Lausanne, March 11, 2011
Alberto Sangiovanni Vincentelli gave a distinguished seminar series talk on Interconnect Everywhere at EPFL.

Invited Lecture:
Rome April 28, 2011
Alberto Sangiovanni Vincentelli gave a *lectio magistralis* (500 people attending) at the University of Rome on Innovation, Funding New Enterprise and the Importance of a Rich Ecosystem.

Lectio Magistralis: What is Important in the Design of Systems
Politecnico di Bari, December 2nd , 2011
Alberto Sangiovanni Vincentelli delivered the Lectio Magistralis at the Commencement of Politecnico di Bari about the importance of research in and teaching of system design.

Invited Lecture: Christoph Kirsch,
Virtualizing Time, Space, and Power for Cyber-Physical Cloud Computing, ARTIST Workshop on Rigorous Embedded Design, Salzburg, Austria, April 2011.

Invited Lecture: Thomas A. Henzinger,
From Boolean to Quantitative Synthesis, Eleventh Annual Conference on Embedded Software (EMSOFT), Taipei, Taiwan, October 2011.

Invited Lecture: Thomas A. Henzinger
Ten Years of Interface Automata, ACM SIGSOFT Impact Paper Award Lecture, 19th Annual Symposium on Foundations of Software Engineering (FSE), Szeged, Hungary, September 2001.

Invited Lecture: Thomas A. Henzinger
Quantitative Reactive Models, Workshop on Synthesis, Verification, and Analysis of Rich Models (SVARM), Saarbrucken, Germany, April 2011.

Invited Lecture: Thomas A. Henzinger

Formal Methods for Composing Systems, Design Automation and Test in Europe (DATE),Grenoble, France, March 2011.

Invited Lecture: Kim G. Larsen
ARTIST Summer School in China, IOS/ISCAS, Beijing, August 8-12, 2011.
www.artist-embedded.org/artist/Overview,2239.html

Invited Lecture: Kim G. Larsen
ARTIST Summer School, Aix-les-Bains, France, September 4-9, 2011

Panelist: Christoph Kirsch, Vehicular Wireless Networks: What should the future hold? International Symposium on Wireless Vehicular Communications (WiVeC), San Francisco, California, September 2011.

Invited Panelist: Kim G. Larsen
Microsoft Software Summit , Paris, France, April 14, 2011, research.microsoft.com/en-us/events/ss2011

Invited Lecture: Christoph Kirsch,
Virtualizing Time, Space, and Power for Cyber-Physical Cloud Computing, ARTIST Workshop on Rigorous Embedded Design, Salzburg, Austria, April 2011.

Invited talk: Kim G Larsen
RED, Rigorous Embedded Systems, Salzburg, Austria, April 10, 2011. www.artist-embedded.org/artist/Programm,2288.html/

Tutorial: Twan Basten
Designing Next-Generation Real-Time Streaming Systems.
9th IEEE/ACM International Conference on Hardware/Software-Codesign and System Synthesis, CODES+ISSS 2011. Embedded Systems Week. Taipei, Taiwan, October 9, 2011.
http://esweek.acm.org/ and http://www.es.ele.tue.nl/~sander/tutorials/esweek-2011/.

Summer School Speaker: Christoph Kirsch
Virtualizing Time, Space, and Power for Cyber-Physical Cloud Computing, Georgia Tech Summer School on Cyber-Physical Systems, Atlanta, Georgia, USA, June, 2011.

Tutorial Speaker: Christoph Kirsch
The Logical Execution Time Paradigm, Tutorials on Time-Predictable and Composable Architectures for Dependable Embedded Systems, ESWEEK, Taipei, Taiwan, October 2011.

Invited Tutorial: Thomas A. Henzinger
Applications of Games in Quantitative Verification and Synthesis, invited tutorial, Annual GAMES Workshop, Paris, France, September 2011.

Conference: The European Conference on Computer Systems (EuroSys 2011), University of Salzburg, Salzburg, Austria
10-13 April 2011
The EuroSys conference series brings together professionals from academia and industry. It has a strong focus on systems research and development: operating systems, data base systems, real-time systems and middleware for networked, distributed, parallel, or embedded computing systems. EuroSys has become a premier forum for discussing various issues of

systems software research and development, including implications related to hardware and applications.
EuroSys 2011 followed the pattern established by the previous EuroSys conferences, by seeking papers on all aspects of computer systems. EuroSys 2011 also included a number of workshops to allow junior and senior members of the systems community to explore leading-edge topics and ideas before they are presented at a conference.
The general chair was Christoph Kirsch from the University of Salzburg.
http://eurosys2011.cs.uni-salzburg.at

Conference: ACM/IEEE Ninth International Conference on Formal Methods and Models for Codesign (Memodode 2011)
Verimag has co-chaired this conference which had taken place in Cambridge. Memocode attracts researchers and practitioners who create methods, tools, and architectures for the design of hardware/software systems. These systems face increasing design complexity including tighter constraints on timing, power, costs, and reliability.
http://www.memocode-conference.com

Conference: The 6th IEEE International Symposium on Industrial Embedded Systems (SIES 2011), Mälardalen University, Västerås, Sweden.
June 15-17, 2011.
TRENTO has co-chaired this conference, which is concerned with all aspects related to modelling and developing embedded systems, with particular emphasis on their application in a variety of industrial environments. The considered applications range from SoCs, which are making inroads in to the area of industrial automation, to automotive and safety-critical systems.
In particular, at this year conference, TRENTO and IST-Austria have organized a special session dedicated to various aspect of robust design with a keynote speech by Jean-François Raskin on the Synthesis of Robust Controller and Games With Imperfect Information, and a set of three invited papers on specification, control and design methodologies.

Conference: 9th International Conference on Formal Modeling and Analysis of Timed Systems, FORMATS 2011, Phønix Hotel, Aalborg, Denmark, 21-23 September 2011
http://formats2011.cs.aau.dk/

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 focusses 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.

Organizers: Alexandre David, Kim G Larsen, Claus Thrane, Rikke W. Uhrenholt

3rd Workshop on Games for Design, Verification and Synthesis.
Co-located with CONCUR'11, Aachen (Germany), 10 September 2011

http://www.lsv.ens-cachan.fr/Events/gasics10/

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

- Adapted notions of games for synthesis of complex interactive computational systems
- Games played on complex and infinite graphs

- Games with quantitative objectives
- Game ith incomplete information and over dynamic structures
- Heuristics for efficient game solving.

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

Workshop: Design framework -- concept and tool
Hristina Moneva, Teade Punter, Roelof Hamberg – ESI workshop for industry with participation from companies Océ, ASML, Philips Healthcare, and Vanderlande, Eindhoven, the Netherlands, November 11, 2011

Workshop: A Design Framework for Model-based Development of Complex Systems
Hristina Moneva, Roelof Hamberg, Teade Punter – AVICPS (Analytic Virtual Integration of Cyber-Physical Systems Workshop), Vienna, Austria, November 29, 2011

Workshop: Synchron Workshop 2010 and 2011
INRIA organized through its Aoste team the 17th edition of Synchron in Frejus. The seminar is a rather informal event, of one-week duration, meant to gather international experts together with junior researchers and PhD/postdoc students in a studious while festive atmosphere. Days are given to formal presentations, and evenings may be spent in further talks and informal demos. In 2010 the Synchron seminar attracted over 50 participants, and acknowledged the active support of Artist-Design. The 2011 edition of Synchron has been hold in Fontainebleau in December 2011
http://www.artist-embedded.org/artist/Synchron-2010,2206.html

Tutorial Day: Formal Methods in Computer-Aided Design (FMCAD 2011)
Verimag has organised the Tutorial day of this conferences on the theory and applications of formal methods in hardware and system verification. FMCAD provides a leading forum to researchers in academia and industry for presenting and discussing ground breaking methods, technologies, theoretical results, and tools for reasoning formally about computing systems. It covers formal aspects of computer-aided system design including verification, specification, synthesis, and testing.
http://www.cs.utexas.edu/users/ragerdl/fmcad11

Workshop: ACESMB 2011, 4th International Workshop on Model Based Architecting and Construction of Embedded Systems
October 18th, 2011, Wellington (New-Zealand, held in conjunction with MoDELS 2011).
The objective of this workshop was to bring together researchers and practitioners interested in model-based software engineering for real-time embedded systems. Contributions related to this subject at different levels, and ranged from modelling languages and semantics to concrete application experiments, from model analysis techniques to model-based implementation and deployment. Due to the criticality of the application domain, a particular focus was on model-based approaches yielding efficient and provably correct designs.
http://www.artist-embedded.org/artist/Overview,2337.html

Workshop: UML&FM'2011, Fourth IEEE International workshop UML and Formal Methods
June 20th, 2011, Lero, Limerick, Ireland (held in conjunction with FM 2011)
or more than a decade now, the two communities of UML and formal methods have been working together to produce a simultaneously practical (via UML) and rigorous (via formal methods) approach to software engineering. UML is the de facto standard for modelling various aspects of software systems in both industry and academia, despite the inconvenience that its current specification is complex and its syntax imprecise. The fact that the UML semantics is too informal have led many researchers to formalize it with all kinds of existing formal languages, like OCL, Z, B, CSP, VDM, Petri Nets, UPPAAL, HOL, Coq, PVS

etc. This fourth workshop was meant to be open to various subjects as the main objective was to encourage new initiatives of building bridges between informal, semi-formal and formal notations.
http://www.artist-embedded.org/artist/Overview,2271.html

Workshop: UML&AADL'2011, Sixth IEEE International workshop UML and AADL
April 27th, 2011, Las Vegas, USA (in conjunction with ICECCS 2011)
New real-time systems have increasingly complex architectures because of the intricacy of the multiple interdependent features they have to manage. They must meet new requirements of reusability, interoperability, flexibility and portability. These new dimensions favour the use of an architecture description language that offers a global vision of the system, and which is particularly suitable for handling real-time characteristics. Due to the even more increased complexity of distributed, real-time and embedded systems (DRE), the need for a model-driven approach is more obvious in this domain than in monolithic RT systems. The purpose of this workshop was to provide an opportunity to gather researchers and industrial practitioners to survey existing efforts related to behaviour modelling and model-based analysis of DRE systems.
http://www.artist-embedded.org/artist/Overview,2195.html

Workshop: Rigorous Embedded Design 2011
organised and funded by ARTIST
April 10th, 2011 Salzburg, Austria (within EuroSys 2011)
The objective of this workshop organised by VERIMAG was to discuss new methodologies for the rigorous design of embedded systems. Through a series of invited talks, the workshop surveyed some of the challenges and emerging approaches in the area. A series of design flows have been presented. The workshop mainly discussed performance analysis, correctness (high confidence and security), code generation, and modelling aspects (including timed scheduling and software/hardware interactions). Those concepts are illustrated with examples coming from the aeronautic, automotive, and robotic areas. Interactions between industrials and academic researchers have been facilitated through a series of open discussion sessions.
http://www.artist-embedded.org/artist/Programm,2288.html

Workshop: VVPS. Verification and Validation of Planning and Scheduling Systems
organised and funded by ARTIST
June 13, 2011, Freiburg, Germany (within ICAPS)
The VVPS workshop organised by VERIMAG aimed at enhancing a stable forum on relevant topics connected to contaminations between V&V and P&S. The workshop intended to deepen the debate on relevant aspects of interactions between V&V methods and P&S-based systems. It investigated new solutions and identified open issues.

Workshop: ICES Seminar: Formalisms for Description and Visualization of Embedded Systems Architectures – Current State of Practice, Needs and Research Topics

Stockholm, Sweden, April 12th, 2010

This ArtistDesign workshop was carried out as part of CPS Week at KTH, 12 April 2010, with approx. 50 participants from industry and academia.

http://www.artist-embedded.org/artist/Overview,1937.html

Workshop: TiMoBD, Time Analysis and Model-Based Design, from Functional Models to Distributed Deployments

ESWeek, Taiwan, October 9-14, 2011

Model-based and Model-driven design flows are very popular in the industry because of the possibility of analysis and verification by simulation or model checking and because of the availability of automatic code generation tools that provide a path to implementation. However, in most flows, the timing behavior of the system depends on features of the computation and communication architecture that are modelled late or not modelled at all, bringing the possibility for an inappropriate selection of the computing platform (over- or underperforming) and possibly an incorrect software implementation of the functional model. To this end, timing analysis techniques can provide support for the analysis of architecture solutions and system configurations and also define analytical methods for the synthesis of feasible/correct solutions. Hence, there is a need for a better integration of timing analysis technologies, methods and tools in model-based and model-driven flows. The workshop attempted at bridging the gap between the three communities of model-based design, real-time analysis and model-driven development, for a better understanding of the ways in which new development flows that go from system-level modelling to the correct and predictable generation of a distributed implementation can be constructed leveraging current and future research results.

Workshop Green and Smart Embedded System Technology: Infrastructures, Methods and Tools at the Cyber-Physical System Week
Stockholm, Sweden, April 12th, 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

-- Changes wrt Y3 deliverable --

This is new text, not present in Y3 deliverables.

Internal Reviewers for this Deliverable

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