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

Activity - Progress Report for Year 1

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.**No index entries found.**

Versions

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

Table of Contents

1. Overview of the Activity

1.1 ArtistDesign Participants and Roles

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

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

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

Prof. Kim Guldstrand Larsen (CISS, Center for Embedded Software Systems, Denmark)

Timed automata based models with particular emphasis on extensions with cost, probabilities and multiplayer extensions. Verification, synthesis, performance evaluation and model-based testing.

Prof. Dr. Ir. Boudewijn R. Haverkort (Scientific Director of the ESI, The Netherlands)
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)
Compositional timing and reliability modeling in 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)
Resource Scheduling and Verification (UPPAAL and TIMES), Combination of State-Based and Analytical Analysis Techniques (CATS tool).

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

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

-- Changes wrt Y1 deliverable --

Tom Henzinger left EPFL (Switzerland) for IST (Austria) and Susanne Graf took over his role of Modeling activity leader.

Ed Brinksma left ESI.

Parades left the consortium and Trento moved from associate to full partner instead. Alberto Sangiovanni Vincentelli moved from PARADES to Trento.

1.2 Affiliated Participants and Roles

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

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

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

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

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

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

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

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

-- Changes wrt Y1 deliverable --

The list of affiliate partners has been updated to correspond to the actual contribution of year 2.

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 Y1 deliverable --

No changes with respect to Year 1.

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 Y1 deliverable --

No changes with respect to Year 1.

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 Y1 deliverable --

No changes with respect to Year 1.

1.6 Technical Description: Joint Research

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

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

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

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

-- Changes wrt Y1 deliverable --

No changes with respect to Year 1.

1.7 Problem Tackled in Year 1

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 wit 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 metamodels for heterogeneous systems. Metropolis has been analyzed and compared to other metamodeling approaches. In addition, heterogeneous composition based

on conservative approximations has been studied. The models of complex interconnects have been developed in the COSI modeling, analysis and synthesis framework.

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

Sub-activity B (Resource Modeling)

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

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

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

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

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

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

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

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

Sub-activity C (Quantitative Modeling)

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

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

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

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

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

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

-- Changes wrt Y1 deliverable --

No changes with respect to Year 1.

1.8 Problems Tackled in Year 2

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

- **A.** Component Modeling", where we focus on defining and composing models with heterogeneous semantics.
- **B.** Resource Modeling", where we study the design of resource-constrained systems, where the resource can be quantitative (e.g. energy consumption) or not (e.g. shared memory access).
- **C.** Quantitative Modeling", where we specifically focus on design frameworks for quantitative modeling (mainly timing and resource consumption).

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

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 metamodels such as the Heterogeneous Rich Component and the Metropolis metamodel 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 multicore 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 Achievement8).

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 Achievement 4, 5).

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

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

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

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

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

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

-- Changes wrt Y1 deliverable --

This is new text, not present in Y1 deliverables.

2. Summary of Activity Progress

2.1 Technical Achievements

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

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

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

4. **Priced Timed Automata** (**CISS + LSV Cachan**)
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 nanoseconds to weekly, monthly or longer-range reactive planning in a factory or supply chain.

5. Exponentially Priced Timed Automata* (**CISS + LSV Cachan**)
We study one-clock priced timed automata in which prices can grow linearly (p' = k) or exponentially (p' = kp), with discontinuous updates on edges. We propose EXPTIME algorithms to decide the existence of controllers that ensure existence of infinite runs or reachability of some goal location with nonnegative observer value all along the run. These algorithms consist in computing the optimal delays that should be elapsed in each location along a run, so that the final observer value is maximized (and never goes below zero).

6. Modal Transition Systems* (**CISS + Brno**)
Modal transition system (MTS) is a formalism which extends the classical notion of labeled transition systems by introducing transitions of two types: must transitions that have to be present in any implementation of the MTS and may transitions that are allowed but not required. The MTS framework has proved to be useful as a specification formalism of component-based systems as it supports compositional verification and stepwise refinement. Nevertheless, there are some limitations of the theory, namely that the naturally defined notions of modal refinement and modal composition are incomplete with respect to the semantic view based on the sets of the implementations of a given MTS specification. Recent work indicates that some of these limitations might be overcome by considering deterministic systems, which seem to be more manageable but still interesting for several application areas. In the present work, we provide a comprehensive account of the MTS framework in the deterministic setting. We study a number of problems previously considered on MTS and point out to what extend we can expect better results under the restriction of determinism. Also the problem of the exact computational complexity of thorough refinement checking between two finite MTSs remained unsolved. We settle down this question by showing EXPTIME-completeness of thorough refinement checking on finite MTSs. The upper-bound result relies on a novel algorithm running in single exponential time providing a direct goal-oriented way to decide thorough refinement. If the right-hand side MTS is moreover deterministic, or has a fixed size, the running time of the algorithm becomes polynomial. The lower-bound proof is achieved by reduction from the acceptance problem of alternating linear bounded automata and the problem remains EXPTIME-hard even if the left-hand side MTS is fixed.

7. Actor Semantics (**CISS**)
Models of embedded systems with communicating actors and deadlines offer abstraction and encapsulation of related functionality, but their behavior is complex. Verification is therefore difficult and requires a combination of simulation, model checking and testing tools. In order to rely on the results, these tools must use consistent semantics for the model. Yet, a monolithic semantic model is just as complex as the entity it describes. In order to circumvent this issue, we define a three level semantics giving independent definitions of the functionality of actors, the temporal properties of communications, and finally imposing deadlines on the timing of dependent actors. With this approach the semantics is used directly in developing a simulator supporting the non-determinism of the abstract semantics such that e.g. potential race conditions can be detected. The layers are also planned to underpin independent specialized verification tools. The verification task for timed, hybrid systems can thus be divided into the continuous, discrete, and timing domains with automated translation to specialized tools, and this promises better scalability than simulation or model checking of one complex model.

8. Quantitative Analysis of Weighted Transition Systems (**CISS**)
We present a general framework for the analysis of quantitative and qualitative properties of reactive systems, based on a notion of weighted transition systems. We introduce and analyze three different types of distances on weighted transition systems, both in a linear and a branching version. Our quantitative notions appear to be reasonable extensions of the standard qualitative concepts, and the three different types introduced are shown to measure inequivalent properties. When applied to the formalism of weighted timed automata, we show

that some standard decidability and undecidability results for timed automata extend to our quantitative setting. We also generalize the usual Boolean satisfaction relation of CTL, to a map assigning states and temporal formulae with a real-valued distance, describing the degree of satisfaction. We describe a general approach to obtaining quantitative interpretations for a generic extension of the CTL syntax, and show that, for one such interpretation, the logic is both adequate and expressive with respect quantitative bisimulation.

9. Discounting for Priced Timed Automata (**CISS**)
This work deals with the issue of discounting in weighted timed transition systems. Discounting provides a way to model optimal-cost problems for infinite runs and has applications in optimal scheduling and other areas. We show that when postulating a certain natural additivity property for the discounted weights of runs, there is essentially only one possible way to introduce a discounting semantics. Our proof relies on the fact that a certain functional equation essentially only has one solution, for which we provide an elementary proof.

We also consider the discounting semantics for priced timed automata. In the discounting semantics, prices decrease exponentially, so that the contribution of a certain part of the behavior to the overall cost depends on how far into the future this part takes place. We consider the optimal infinite run problem under this semantics: Given a priced timed automaton, find an infinite path with minimal discounted price. We show that this problem is computable, by a reduction to a similar problem on finite weighted graphs. The proof relies on a new theorem on minimization of monotonous functions defined on infinite-dimensional zones, which is of interest in itself.

10. Performance Prediction and Optimization for High-Tech Embedded Control (ESI)
Embedded control is a key product technology differentiator for many of the high-tech industries. The strong increase in complexity of embedded control systems combined with the occurrence of late changes in control requirements, results in many timing performance problems showing up only during the integration phase. This results in extremely costly design iterations, severely threatening the time-to-market and time-to-quality constraints. In the ESI Wings project this integration problem is attacked systematically through the construction of executable POOSL models. The key approach is to separate the logic of the embedded control application from the execution platform on which it is deployed, following the Y-chart approach. Modeling patterns with standardized interfaces were developed for reasons of scalability and distributed and multi-domain model development. The resulting models yield an overview and a system-wide insight in the performance bottlenecks. They further allow one to rapidly explore alternatives to optimize the performance, by adapting the application, the execution platform or the mapping. The ESI Wings project has demonstrated the effectiveness of the performance prediction and optimization method by applying it to a complex performance-critical subsystem of a Wafer Scanner. The application of the method within ASML has resulted in more than a dozen improvement proposals with an expected overall timing performance gain of more than 50%.

11. Genesys Cross-Domain Reference Architecture Template for Embedded Systems (ESI) ESI contributed to the development of the Genesys Cross-Domain Reference Architecture Template for Embedded Systems, determined its requirements and architectural concepts within the consumer electronics domain (together with Nokia and others), and analyzed its suitability for these purposes [Gen09].

12. Computational Modeling for Design-space Exploration (ESI)
Several activities are aiming to develop new concepts and approaches for modeling embedded systems for the purpose of design-space exploration, following up on the activities done last year. We are working with dataflow, Petri nets, and timed automata, targeting multi-objective trade-off analysis, simulation, and schedule optimization, respectively. Techniques

to avoid state-space explosion are under investigation, which is needed to scale to industrial cases. We have started to integrate the various techniques into a design-space exploration framework that leverages the various (formal) modeling and analysis techniques and tools (CPNTools, Uppaal, SDF3). Initially the toolset targets professional printers but it is intended to be retargetable to other embedded systems.

13. Behavior modeling for complex software-intensive systems (ESI)
Modeling techniques to capture the required behavior of complex embedded systems have been applied to case studies such as car entertainment systems, electron microscopes, and medical imaging systems. Techniques have been developed to capture runtime behavior of embedded systems and to relate it to a model of the system have been extended to resource usage. New ways of expressing this observed runtime behavior also have been developed and published. Many activities were aimed at developing a reference architecture for software-intensive systems, i.e., a collection of models and other views that capture the essential aspects of the system. Such a reference architecture is an important asset in improving the evolvability of the underlying system.

14. A Modal Interface Theory for Component-based Design (INRIA + Trento)
INRIA and the University of Trento have developed a rich composition algebra for modal specifications that meets certain methodological requirements [RBB+09]. In [RBB+09], INRIA and the University of Trento have then unified modal specifications with the framework of interface automata originally defined by de Alfaro and Henzinger.

15. A Compositional Approach on Modal Specifications for Timed System (INRIA)
INRIA has proposed a timed extension of modal specifications, defined their notions of refinement and consistency, and established their decidability in [BPR09]. INRIA has also considered the subclass of modal event-clock automata and developed an entire theory with conjunction, product, and quotient, that promotes efficient incremental design techniques and that enables to reason in a compositional way about timed system [BLPR09].

16. Modal Contracts for Component-based Design (INRIA)
INRIA has studied assume/guarantee contracts as pairs of modal specifications [GR09]. The theory relies on a weak implication operation between the assumptions and the guarantees. This implicit form for a contract is used to define parallel composition of two modal contracts as the strongest contract refined by the parallel composition of any pair of implementations of the contracts, and conjunction of contracts as the weakest contract refining both contracts.

17. Modal Contracts for Component-based Design (INRIA + Virginia Tech)
INRIA hosted Sandeep Shukla, associate professor at Virginia Tech, for his sabbatical. The visit of Sandeep Shukla was jointly funded by the University of Rennes, INRIA Rennes-Bretagne-Atlantique, the Scientific Board of INRIA and the Artist-Design Network of Excellence. The main objective of the sabbatical was to jointly investigate the state of the art to modeling multi-clocked synchronous embedded systems, as in Polychrony, for instance, and to explore alternatives modeling, analysis and compilation techniques. These discussions resulted in a number of joint publications with INRIA participants to Artist-Design and are subject to several related and ongoing work (see list of publication). The most salient dissemination and publication results resulting of this visit are the organization of 2 workshops on this topic (see further down)

18. Tradeoff exploration between reliability, power consumption, execution time (INRIA)
We have developed a scheduling heuristics that, from a given software application graph and a given multiprocessor architecture, 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 scaling to lower the power consumption.

19. Theory of relational interfaces (IST Austria)
Despite the significant progress that has been made in the recent past towards the development of a comprehensive theory of interfaces for component-based design, existing interface theories fail to capture functional relations between inputs and outputs. Consider as a motivating example a component that is supposed to take as input a number n ≥ 0 and return as output n + 1. This simple component cannot be specified using existing interface theories. In fact, the interface of such a component could be expressed as a binary relation between the inputs and the outputs that contains all the pairs (n,n+1), such that n ≥ 0. This relation can be seen as a contract between the component and its environment. In this particular example, the assumption is that the environment provides as inputs only non-negative values to the component, and for every legal input, the component guarantees to generate as output the input value increased by one. We propose, in a joint work with U. C. Berkeley, a theory of *relational interfaces* that precisely allows specifying input/output relations as first-order logic (FOL) formulae over the input and output variables. We show, under some reasonable restrictions on the feedback loops in the interfaces, that our theory of relational interfaces supports both *stepwise refinement* (if I_1 refines I_2, then I_1 can replace I_2 in any context) and *independent implementability* (if components I'_i refine components I_i, then the composition of I'_i refines the composition of I_i). Our theory also supports *component reuse* through the *shared refinement* operator. Finally, our framework seamlessly supports both *stateless* and *stateful* interfaces [TLHL09].

20. Quantitative generalizations of languages (IST Austria)
Quantitative generalizations of classical languages have been developed in [CDH08], where each word is assigned with a real number instead of a Boolean value. *Quantitative languages* have applications in modeling resource-constrained computation. We extended the work in [CDH08], by studying *expressiveness* and *closure* properties for quantitative languages. In order to define natural classes of quantitative languages, we use *weighted automata*, non-deterministic automata with numerical weights. In the case of infinite words, the value of a run is naturally computed as the *maximum*, *limsup*, *liminf*, *limit average*, or *discounted sum* of the transition weights. For example, peak power consumption can be modeled as the maximum of a sequence of weights representing power usage and average response time as the limit average. In the first part of this work, we investigated alternative ways of comparing the expressive power of weighted automata. We also considered automata with transition weights 0 or 1 and showed that they are as expressive as general weighted automata in the limit-average case, but not in the discounted-sum case. For quantitative languages L_1 and L_2, we considered operations *max* (L_1,L_2), *min* (L_1,L_2) and *1-*L_1, which generalize the Boolean operations on languages, as well as the sum. We established the closure properties of all classes of quantitative languages with respect to these four operations.

Finally, we studied *alternating* and *probabilistic* extensions of weighted automata and their expressiveness and closure properties. We introduced alternating weighted automata in which the transitions of the runs are chosen by *two players* in a *turn-based fashion*. In particular, we showed that for limit average and discounted sum, alternation brings more expressive power than non-determinism. We also presented decidability results and open questions for the quantitative extension of the classical decision problems in automata theory (emptiness, language inclusion and language equivalence). We introduced probabilistic weighted automata, in which transitions are chosen in a *randomized* fashion. In particular, we showed that probabilities allow us to define a wide variety of new classes of quantitative languages, except for discounted-sum automata, where probabilistic choice is no more expressive than non-determinism [CDHa09, CDHb09, CDHc09].

21. Quantitative Synthesis (IST Austria)
Most specification languages express only qualitative constraints. However, between two implementations that satisfy a given specification, one may be preferred to another. For example, if a specification asks that every request is followed by a response, one may prefer an implementation that generates responses quickly but does not generate unnecessary responses. We use quantitative properties to measure the "goodness" of an implementation. Using games with corresponding quantitative objectives, we can synthesize "optimal" implementations, which are preferred among the set of possible implementations that satisfy a given specification. In particular, we show how automata with lexicographic mean-payoff conditions can be used to express many interesting quantitative properties for reactive systems. In this framework, the synthesis of optimal implementations requires the solution of lexicographic mean-payoff games (for safety requirements), and the solution of games with both lexicographic mean-payoff and parity objectives (for liveness requirements). We present algorithms for solving both kinds of novel graph games [BCHJ09].

22. Robustness of Sequential Circuits (IST Austria + INRIA + CVF)
Digital components play a central role in the design of complex embedded systems. These components are interconnected with other, possibly analogue, devices and the physical environment. This environment cannot be entirely captured and can provide inaccurate input data to the component. It is thus important for digital components to have a robust behavior, i.e. the presence of a small change in the input sequences should not result in a major change in the output sequences. In this work, we study the robustness property for sequential circuits. Our contributions are (1) a model of robustness as a form of continuity for such circuits, (2) the characterization of the exact class of sequential circuits that are robust according to our definition, (3) an algorithm to decide whether a sequential circuit is robust or not. We also consider the preservation of robustness by composition of sequential circuits as well as an asynchronous extension of our definition of robustness [DHLN09].

23. Robust Synthesis (IST Austria)
Many specifications include assumptions on the environment. If the environment satisfies the assumptions then a correct system reacts as intended. However, when the environment deviates from its expected behavior, a correct system can behave arbitrarily. We want to synthesize robust systems that degrade gracefully, i.e., a small number of environment failures should induce a small number of system failures. We define ratio games and show that an optimal robust system corresponds to the winning strategy of a ratio game, where the system minimizes the ratio of system errors to environment errors. We show that ratio games can be solved in pseudo-polynomial time [BGHJ09].

24. Transactional Memories (IST Austria)
Transactional memory (TM) has shown potential to simplify the task of writing concurrent programs. However, the semantics of interactions between transactions managed by a TM and non-transactional operations, while widely studied, lacks a clear formal specification. Those interactions can vary, sometimes in subtle ways, between TM implementations and underlying memory models. We propose a new correctness condition for TMs, *parameterized opacity*, which captures the two following intuitive requirements: first, every transaction appears as if it is executed instantaneously with respect to other transactions and non-transactional operations, and second, non-transactional operations conform to a given memory model. Parameterized opacity corresponds to the well-studied strong atomicity property, which lacks a formal definition and is, in fact, ambiguous. We use our formalization to theoretically investigate the inherent cost of implementing parameterized opacity. We first prove that parameterized opacity requires either instrumenting non-transactional operations (for most memory models) or writing to memory by transactions using potentially expensive read-modify-write instructions (such as compare-and-swap). Then, we show that for a class of relaxed memory models, parameterized opacity can indeed be implemented with constant-time instrumentation of non-transactional writes and no instrumentation of non-transactional

reads. We show that, in practice, parameterizing the notion of correctness allows to develop more efficient TM implementations [GHKS09]. The work done on transactional theories resulted in the PhD thesis of Vasu Singh from IST Austria [Sin09].

25. Component Modeling with ForSyDe (**KTH**)
KTH has further developed ForSyDe as a framework for modeling, verifying and analyzing designs of heterogeneous systems [SAJ09, Jan09]. As part of the ANDRES project we have completed our work to include dynamically reconfigurable systems in ForSyDe [SZJ+09]. A performance analysis method and accompanying tools for general, heterogeneous multi-core systems has been developed [ZSJ09]. In the context of a new Artemis project SYSMODEL (http://www.sysmodel.eu/), KTH in cooperation with DTU and TUT in Tampere, develops a SystemC based modeling framework based on ForSyDe semantics.

26. Modeling for Performance analysis (**KTH**)
KTH has systematically studied resource allocation for delivering high performance and QoS in a variety of applications and systems. This work has resulted in a survey paper and several case studies and architecture specific techniques [ZSJ+09, SZJ+09,LMJ09]. Together with NXP and ARM, KTH has developed a contract based performance analysis in MPSoCs [LMJ09, LBJ09], is now working on a system dimensioning and optimization method and tool.

Based on the Network Calculus theory and in collaboration with NUDT (Changsha, China) KTH has developed an elaborate performance analysis method [QLD+09a-f].

In the medical application domain ECG analysis has been studied thoroughly and has resulted in a design methodology and performance analysis and design space exploration method. For on-chip communication networks a TDM based technique has been developed for guaranteeing minimum bandwidth and maximum latency service. Also, KTH has studied Network Calculus and found a significant potential to apply it for on-chip and inter-device communication. On-chip it has been used for modeling complex memory controllers and analyzing performance of memory transactions. Work in progress develops a contract based system dimensioning and analysis method where contracts are formulated as Network Calculus arrival curves. Finally, KTH has applied Network calculus based performance analysis for communication in sensor networks.

27. Model-based engineering of self-configurable embedded systems (**KTH**)
As part of the Dyscas project (FP6, www.dyscas.org - the project finished in March 2009), a middleware architecture for self-configuring automotive embedded systems was developed (this middleware is mainly described in the Adaptivity cluster of the ArtistDesign network). The work included both the development of a reference architecture as well as concrete implementations of it. One aspect of the work has been the adoption of model-based development for the middleware architecture. Moreover, since the middleware is adaptive, run-time models of applications and of the system resources are essential to support on-line reasoning and adaptation (e.g. triggering an application to switch to a different QoS mode or redeploying an application to another node). In a DySCAS system, the management and control decisions are carried out hierarchically based on embedded system meta-data and adaptation policies/rules. Such system meta-data provide built-in knowledge about system configurability and adaptability, and is the basis for any embedded configuration management decisions. DySCAS provides an information-model to support the design of adaptation meta-data and policies/rules. The issues of particular concern include impacts of changes on the overall system functionality, end-to-end performance, and dependability. The specified information may include, e.g., the application's maximum need of processor, memory and communication resources, as well as task timing parameters and overall system merit/benefit in each QoS mode, [CTMFQ09], [QPCTF09].

28. An extensible formal framework for modeling of resource usage and adaptability of software components (**KTH**)
In embedded real-time systems, timing and resource utilization both are vital aspects, putting important constraints on the deployed software. Related to the DySCAS project, an extensible formal framework for modeling of resource usage and adaptability of software components has been developed, based on the idea of resource interfaces. The formalism explicitly allows modeling of resources of various types and in different ways; and the timing requirements that applications have. The formalism is based on timed automata annotated with resource usage. The models can be used as a basis for quantitative analysis during both design and run-time, as a basis for online reconfiguration reasoning, and in the extension as a basis for system synthesis, [PT09a], [PT09b]

29. Integrating safety analysis and system design through model-based engineering (**KTH + Volvo**)
EAST-ADL2 is an architectural description language (ADL) intended to support a safety-driven, model-based design process for automotive embedded systems. One of the objectives of EAST-ADL2 is to provide native, language-level support for ISO26262 concepts, allowing EAST-ADL2 models to directly represent safety-related information. In particular, the error-modeling package of EAST-ADL2 allows explicit description of likely behaviors that a component/system may exhibit when it deviates from the supposed functions or behaviors. It provides explicit language constructs for capturing the anomalies of various system entities and for managing such information and its integration with system requirements, nonfunctional constraints, nominal behaviors, and V&V needs, [CFJ+09]. The work is carried out in the ATESST2 FP7 project (www.atesst.org)

The EAST-ADL2 approach aims to enable multi-leveled error modeling with multiple formalisms for the development of automotive embedded systems, required to cope with the complexity and the different needs in different lifecycle stages. Structured fault-models for example provide information about the component/system failure-modes, internal and external faults, and the cause-effect relationship of faults and failure-modes. In system development, such models often constitute the primary means for hazard assessment and for the derivation of safety requirements and V&V needs. On the other hand, more detailed behavior models are normally needed in order to simulate and analyze error behaviors and safety solutions (e.g., through simulation and fault-injection), or to validate the structured fault-models. Such models extend nominal behavior models with information about the occurrences of faults and failures, errors and error transitions, and possible error handling behaviors. For the definitions of various error behaviors, EAST-ADL2 allows the integration of existing external formalisms (e.g., HiP-HOPS), while providing support for model transformation and tool interoperability with the related external safety analysis techniques, [WPP+09] [PWP+09]. The tooling and analysis concepts in this approach are described in the Validation deliverable.

30. Evaluation of modeling languages for physical systems and their relation to embedded systems modeling (**KTH**)
As a part of the research at KTH within the ATESST2 project on the EAST-ADL2 language, KTH performed an extensive evaluation of languages and tools for the purpose of investigating physical systems modeling, and the connection to embedded systems behaviors and modeling languages. The study included Bond graphs, MATLAB/Simulink, Ptolemy II, Modelica, MATLAB/Simscape and SysML. For SysML, the modeling of continuous-time systems and how it relates to MATLAB/Simulink and Modelica is evaluated. A case study of an electric power assisted steering is modeled to show the differences, the similarities and the usage of the above-mentioned languages and tools. To be able to classify the tools and languages, five realization levels were developed {Physical modeling models, Constraint models, Continuous causal models, Discretized models, Discretized models with solver and platform implementation}. By using these realization

levels, models, tools and modeling languages can be classified, and transformations between them can be set up and analyzed. The comparison also shows many similarities between the languages. The results led to a more detailed investigation on conjugate variables, such as force and velocity, and electric current and voltage, and how these are treated in various languages. In parallel to this work, a method to describe the simulation behavior of a MATLAB/Simulink model using SysML activity diagrams was developed as an approach to achieve integrated system models. Another result is an evaluation of the parametric diagrams of SysML for continuous-time modeling, which shows that they do not enable "physical modeling", i.e. modeling the topology of the system and getting the underlying equations out of this topology. By including physical ports and physical connectors to SysML internal block diagrams, this could be solved [S09].

31. Multi-vehicle helicopter platform (Salzburg + UC Berkley**)**
The Salzburg helicopter platform serves as a testbed for the models and languages that we develop. The system is extremely difficult to control and poses interesting challenges in terms of real-time computation and communication, power consumption, safety, and reliability. We have recently completed building ten identical vehicles and begun testing flight navigation controllers for fully autonomous flights. The helicopters will soon be available for multi-vehicle experiments with our new collaborative sensing language CSL. Developed in collaboration with UC Berkeley, CSL enables multi-vehicle control by a single operator. A description and analysis of CSL has recently been published. The work on CSL is a new activity.

32. Exotask system (Salzburg + IBM Research**)**
In collaboration with IBM Research, we have identified priority inversion in barriers as a major source of performance degradation in IBM's Java runtime system, which serves as execution environment of the Exotask system. A Salzburg PhD student has worked on this problem as part of an internship at IBM Research and recently published his findings.

33. Modularity in HTL(Salzburg + U. Porto + **IST)**
HTL is a hierarchical coordination language for distributed control systems. HTL has a fully compositional semantics, which forms the foundation for exploring modeling techniques that may support more capable and scalable HTL program development. The semantics of all HTL primitives such as programs, modules, modes, and tasks are defined separately from each other. Program correctness in terms of schedulability, absence of race conditions, and reliability can be asserted in a modular fashion. In collaboration with the University of Porto and IST, Salzburg has recently studied the cost of modularity in HTL and published the results.

34. Workload-oriented programming (Salzburg)
HTL is based on the notion of logical execution time (LET), which refers to the time a software task is specified to take from reading input to providing output. Workload-oriented programming takes the LET idea one step further and specifies workload-oriented execution times of process activities. The time to perform some activity is specified relative to the amount and type of workload involved in the activity. Salzburg has recently published a first draft of the programming model. This is a new activity.

35. Platform-Based Design and Frameworks: Metropolis and Metro II (Uni. Trento, UC Berkeley, UTC, National Instruments and Intel)
System-Level Design (SLD) means many different things to many different people. In our view, system-level design is about the design of a whole that consists of several components where specifications are given in terms of functionality with additional:

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

This definition is general since it relates to many different application domains, from semiconductors to systems such as cars and airplanes, buildings, telecommunication and biological systems. To deal with system-level problems, our view is that the issue to address is not developing new tools, albeit they are essential to advance the state of the art in design, rather it is the understanding of the principles of system design, the necessary change to design methodologies and the dynamics of the supply chain. Developing this understanding is necessary to define a sound approach to the needs of the system and component industry as they try to serve their customers better, to develop their products faster and with higher quality. 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. To demonstrate this view, we first presented the challenges in design for the system of the future and a manifesto for the need of a unified methodology. We then summarized a methodology, Platform-Based Design (PBD), that has been developed over the past decade and that we believe can fulfill the needs. Further, we presented 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 concluded the paper with two test cases in two diverse domains: semiconductor chips (a UMTS single-chip design) and energy efficient buildings (an indoor air quality control system).

36. COSI: A Modeling and Design Framework for Communication Design (**Trento**)
COSI (Communication Synthesis Infrastructure) is a software framework for interconnecting infrastructure modeling, analysis and synthesis. The framework allows developing 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.

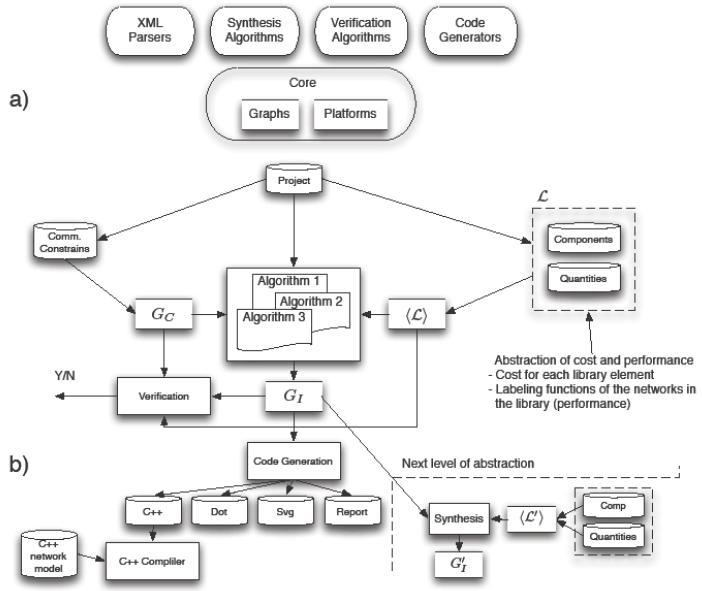

Figure 1. The COSI Platform-Based Design-like structure

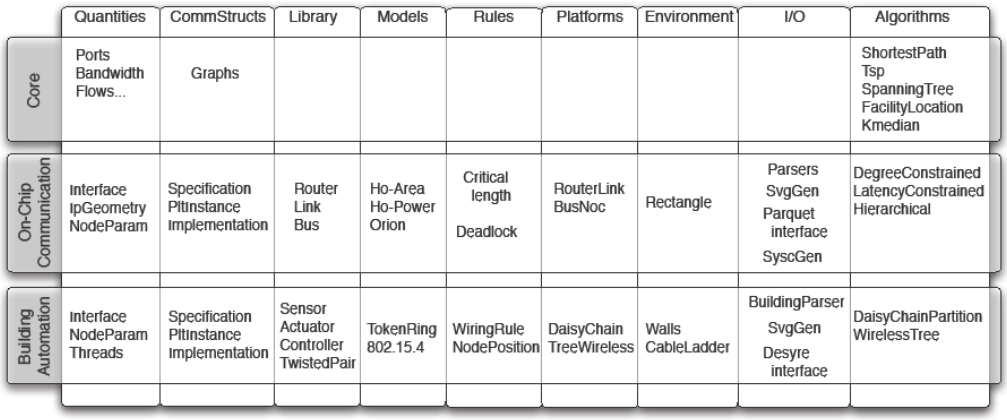

Figure 2. How the COSI framework has been used to generate specific synthesis tools.

We continue 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 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 system.

37. Metamodels: Languages, Tools and Applications (TRENTO, VERIMAG, INRIA, OFFIS, CEA LIST, UC BERKELEY, University of Virginia, Vanderbilt University**).**

As research, methodology, and tool development for embedded-system design progress, we argued in this work that a framework based on metamodels will unquestionably emerge as the standard. There were two companion approaches analyzed in this work that was the object of a special issue on metamodeling of IEEE Design and Test co-edited by Alberto Sangiovanni Vincentelli (Trento and Berkeley), S. Shukla (University of Virginia) and J. Sztipanovits (Vanderbilt University).

The first contribution [SVSSYM09] addressed the metamodel work in Ptolemy and Metro II together with the extensive work at Vanderbilt and Virginia. Metamodeling has two basic interpretations. The common interpretation refers to the modeling of modeling languages including the languages' concrete syntax (notations), abstract syntax, and semantics. Metamodels determine the set of valid models that can be defined with models' language and behavior in a particular domain. Generic functions in model-based design such as model building, model transformation, and model management are supported by meta-programmable tools. The tools' core functions are independent from the particular DSMLs and can be instantiated using metamodels. The second, less traditional interpretation relates to the use of models of computation (MoC) for system design and has a strict semantics connotation. For this reason, we refer to this interpretation as a semantic metamodel. Although MoCs are powerful in capturing specific designs, embedded electronic systems are inherently heterogeneous. Hence, their modeling requires multiple MoC-specific models, thus making the overall system's analysis problematic because its behavior is not a priori expressible in a mathematical formalism that can be inferred from the components' MoCs. Metamodeling in this context is a way to uniformly abstract away MoC specificities while consolidating MoC commonalities in the semantics metamodel. This metamodeling results in a mechanism to analyze and design complex systems without renouncing the properties of the components' MoCs. This metamodeling concept lets us compare different models of computation, provide mathematical machinery to prove design properties, and support platform-based design. It forms the basis of several actor-based design environments such as Ptolemy II and Metropolis

The goal of the second article [PBGB09] was to introduce metamodeling developments in Europe relevant to system-level design of electronic systems. This work was carried out as a

collaborative effort of most of the COMBEST partners, together in particular with researchers from CEA LIST, OFFIS, INRIA, VERIMAG and Trento. In particular, we analyzed current efforts in Europe for using metamodeling in the integrated development of critical systems such as automotive electronics. It distinguishes between lightweight versus heavyweight approaches, surveys a number of related current European projects, and gives details about the SPEEDS project to illustrate the role of metamodeling-driven system engineering. In this work, we argued that designers use component models because they are convenient ways to represent a design and because designers can choose the abstraction that best matches the characteristics of the system under development. Convergence of technologies into the same application area, however, results in heterogeneous specifications that use several models simultaneously for system description. The same degree of heterogeneity is present when the system description is partitioned into separate orthogonal aspects, or viewpoints. In this case, the fragmentation is at the component level and must be resolved by resorting to appropriate combinations of techniques that account for specification interdependencies. In this context, researchers have taken a step back and have begun to study and operate on the models themselves to understand their relationships and to put an order to an otherwise informal collection of methods and tools. To achieve these goals, they used the very same modeling techniques that had proven successful in design to construct models of models, or metamodels. These metamodels have quickly been embraced by methodologies such as the model-driven architecture (MDA) and platform-based design (PBD).
We therefore reviewed the role that models and metamodels have played and are playing in several research projects across Europe. Accordingly, we discussed language design techniques and their use in several industrial applications. We also described the modeling principles and the infrastructure underlying the Speculative and Exploratory Design in System Engineering (SPEEDS) European project, and highlighted the way metamodeling techniques have helped its implementation and applications.

38. Optimizing Extensibility in Hard Real-Time Distributed Systems (**Uni. Trento**, Intel, UC Berkeley, UTC)
Some applications such as the design of a car typically require upgrading an implementation platform to accommodate new functionality or to fix errors over a product lifetime that may extend over a five-year horizon. In this case, being able to adjust the design without undergoing a major re-design cycle is imperative for competitive advantage. We addressed the problem of defining the initial solution to the design problem so that it is as robust as possible with respect to addition of new tasks or modifications to existing ones. To do so, we introduce a robustness measure, the extensibility metric, and then develop an efficient algorithm that optimizes this metric. In this paper, we focused on hard real-time distributed systems that collect data from a set of sensors, perform computations in a distributed fashion and based on the results, send commands to a set of actuators. The tasks must satisfy tight end-to-end deadline constraints. Extensibility is defined as the amount by which the execution time of tasks can be increased without changing the system configuration while meeting the deadline constraints. With this definition, a design that is optimized for extensibility not only allows adding future functionality with minimum changes, but also is more robust with respect to the variance of task execution times. We considered systems based on run-time priority-based scheduling of tasks and messages. In particular, we assumed that input data (generated by a sensor, for instance) are available at one of the system's computational nodes. A periodically activated task on this node reads the input data, computes intermediate results, and writes them to the output buffer from where they can be read by another task or used for assembling the data content of a message. Messages - also periodically activated - transfer the data from the output buffer on the current node over the bus to an input buffer on a remote node. Local clocks on different nodes are not synchronized. Tasks may have multiple fan-ins and messages can be multi-cast. Eventually, task outputs are sent to the system's output devices or actuators. The extensibility optimization problem can be considered as part of the mapping stage in the

Platform-Based Design (PBD) design flow, where the functionality of the design (what the system is supposed to do) and its architecture (how the system does it) are captured separately, and then "joined" together, i.e., the functionality is "mapped" onto the architecture. In the application, function blocks communicate through signals, which represent the data dependencies. The architectural description is a topology of computational nodes connected by buses. In this paper, buses and nodes can have different transmission and computation speeds. Mapping allocates functional blocks to tasks and tasks to nodes. Correspondingly, signals can be mapped into local communication or packed into messages that are exchanged over the buses. Task and message priorities are assigned and the mapping is performed in such a way that the end-to-end latency constraints are satisfied in the worst-case. Task allocation, signal to message packing, message allocation and priority assignment are the design variables considered in this paper that are chosen with the objective of optimizing task extensibility.
The first stage of the proposed algorithm is based on MILP programming, where task placement (the most important variable with respect to extensibility) is optimized within deadline and utilization constraints. The second phase features two heuristic algorithms, which iteratively optimize signal-to- message packing and priority assignment. This algorithm runs much faster than randomized optimization approaches (a 20x reduction with respect to simulated annealing in our case studies). Hence, it is applicable to industrial systems as the case studies, which are of size comparable with the typical case of deployment of a set of additional functionalities in a commercial car, demonstrate in the experimental section. The first case study is a set of active safety functions deployed on a vehicle bus-architecture, with 9 ECUs, 41 tasks, and 83 CAN signals. In this case, optimization takes less than 1800 seconds, compared to more than 12 hours needed by the randomized optimization method, with results of comparable quality. The second test case is a safety-critical distributed control system deployed within a small truck. The key features of this system are the integration of slow and very fast (power electronics) control loops using the same communication network. In this example, we are interested in redesigning an existing system to understand the effects of adding communication and computational resources to the system. The shorter running time of the proposed algorithm allows using the method not only for the optimization of a given system configuration, but also for architecture exploration, where the number of system configurations to be evaluated and subject to optimization can be large. A further advantage of an MILP formulation (even if used only for the first stage) with respect to randomized optimization, is the possibility of leveraging mature technology in solvers, the capability of detecting the actual optimum (when found in reasonable time), or, when the running time is excessive, to compute at any time a lower bound on the cost of the optimum solution, which allows evaluating the quality of the best solution obtained up to that point.

39. Statistical Analysis of Controller Area Network Message Response Times (Uni Trento, UC Berkeley, GM)
Modern automobile architectures are composed by tens of Electronics Control Units (ECUs) connected by several buses, most of which are Controller Area Networks (CAN). The availability of multiple ECUs can be exploited by distributing control tasks of one domain (for example, power train) to several ECUs. In this case, a number of distributed functions are assigned to multiple tasks executing concurrently on different modules and communicating via messages transmitted on CAN. Distributed functions include time-critical controls, but most often, also functions that are characterized by requirements for average performance together with hard deadline constraints (as for most active-safety functions) and functions with soft real-time requirements (controls for enhanced driver comfort). The definition of a new architecture framework for one or more car product families is an extremely important step: ECUs, networks and the topology of connections must be defined and frozen years in advance of production. Later, during the architecture lifespan, functions are placed on ECUs and communication scheduled on the bus. This paper [ZDGSV09] presented a statistical approach to the early evaluation and selection of distributed embedded architectures for

next-generation automotive controls, where the application performance depends on the end-to-end latencies of active-safety functions. Automobile architecture must be evaluated and selected having in mind that they will have a lifespan of 5 to 10 years and that during this lifespan the communication and computation load is partly unknown because new functions are still being decided on and have not been designed as yet. Hence, when verifying that the architecture is sufficiently robust with respect to constraints on latency and performance targets of present and future functionalities, loads can only be roughly estimated by looking at past trends or by exploiting early indications of designers. In this paper, we considered an application model that is currently deployed in General Motors E/E architectures and is supported by the AUTOSAR standard. We described the use of statistical analysis to compute the probability distribution of Controller Area Network (CAN) message response times when only partial information is available about the electrical architecture of a vehicle as well as about its functionality. We provided results that showed our statistical inference allows predicting accurately the distribution of the response time of a CAN message, once its priority has been assigned, from limited information such as the bus utilization of higher priority messages.
This publication obtained the best paper award at the IEEE Symposium on Industrial Embedded Systems.

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

41. New Response Time Bounds for Fixed Priority Multiprocessor Scheduling (Uppsala)
We have developed a new technique for the estimation of worst-case response times on multiprocessor systems using fixed priority scheduling. The technique is proven to dominate theoretically state-of-the-art techniques for multiprocessor systems. Our experiments also show that the technique results in significant performance improvement compared with several existing techniques for multiprocessor schedulability analysis. The technique can also deal with task systems with arbitrary deadlines. This is a non-trivial extension even for single-processor systems. To our best knowledge, this is the first work for multiprocessor systems in this setting, which involves sophisticated techniques for the characterization and computation of response time bounds [GSY*09a].

42. Partitioning the shared caches on multicores for timing predictability (Uppsala)
The major obstacle to use multicores for real-time applications is that we may not predict and provide any guarantee on real-time properties due to the on-chip shared resources such as L2 cache. In this work, we propose to use cache space isolation techniques to avoid cache contention for hard real time tasks running on multicores with shared caches. We have presented a scheduling strategy for real-time tasks with both timing and cache space constraints, which allows each task to use a fixed number of cache partitions, and makes sure that at any time a cache partition is occupied by at most one running task. In this way, the cache spaces of tasks are isolated at run-time. We have developed a sufficient schedulability test for non-preemptive fixed-priority scheduling for multicores with shared L2

cache, encoded as a linear programming problem. Our experiments show that the test which employs an LP solver can easily handle task sets with thousands of tasks in minutes using a desktop computer [GSY*09b]

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

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

44. Source-to-Source Architecture Transformation for Performance Optimization in BIP (VERIMAG):

Source-to-source transformations have been considered as a powerful means for optimizing programs. In contrast to conventional optimization techniques, these can be applied for deeper semantics preserving transformations, which are visible to the programmer and subject to his direction and guidance. Source-to-source architecture transformations transform a component-based system into a functionally equivalent system, by changing the structure of its architecture. They may affect performance and quality attributes. They are useful for finding functionally equivalent systems that meet different extra-functional (platform dependent) requirements.

In [BJS09] we studied and implemented transformations for a subset of the BIP language where architecture is characterized as a hierarchically structured set of components obtained by composition from a set of atomic components. In BIP, composition is parameterized by interactions and priorities between the composed components. Composite components and interactions can be hierarchically structured. Hierarchical descriptions allow incremental reasoning and progressive design of complex systems. Nonetheless, they may lead to inefficient programs if structure is preserved at run time. For example, compared to functionally equivalent monolithic C programs, BIP runtime programs may be more than two times slower. This overhead is due to the computation of interactions between components by the Engine, which is the middleware implementing dynamically the operational semantics of the language.

The aim of the work has been to show that it is possible to synthesize efficient monolithic code from component-based software described incrementally. We study source-to-source transformations for BIP allowing the static composition of components and thus leading to more efficient code. These are based on the operational semantics of BIP, which allows computing the meaning of a composite component as a behaviorally equivalent atomic component.

45. Distributing priorities (VERIMAG)

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

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

One approach considered the use of “knowledge” that can be constructed using verification techniques (reachability analysis) and used by local components to decide whether to execute some interaction and which one, if more than one of them is locally enabled. In [BBPS09] compute knowledge 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. 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 old program. This transformation does not introduce any new executions or deadlocks and preserves the linear temporal logic properties, but it allows the choice of unfair executions.

We have also considered an implementation based on message passing which minimizes not, as usually, the number of messages but privileges short sequences of message exchanges. This algorithm handles some forms of confusion (and ignores others) and it also handles arbitrary conflicts. [BQG09].

We also started developing a method combining knowledge and message passing (work submitted to TACAS’10) where we provide an algorithm that computes an optimal communication strategy for collecting sufficient knowledge to take a decision about whether or which next step to execute. Here, we try to minimize the number of processes required to obtain the information required.

More generally, we suggest a programming methodology, based on a basic design (in this case, the architecture and the transitions) with added constraints (in this case, priorities). Model checking of knowledge properties is used to lift these added constraints by means of a program transformation. The resulted program behaves in an equivalent way, or approximates the behavior of the basic design with the constraints.

46. Synchronous Systems in BIP (VERIMAG)

The main principles of modeling synchronous systems in BIP have been introduced in [BSS09]. In this work, we have shown how the basic execution mechanisms underlying synchronous dataflow systems can be modeled in BIP. We define the class of *modal flow components*. They are a sub-class of BIP components where Petri nets are replaced by *modal flow graphs*. These correspond to a subclass of priority Petri nets for which deadlock-freedom and confluence can be decided at low cost. Modal flow graphs are structures expressing dependency relations between events within one computation step. Similar structures have been proposed and used in different contexts. An important difference between modal flow graphs and related formalisms is the use of three different modalities characterizing dependency between events. For a given set of ports *P*, a modal flow graph is a directed acyclic graph with nodes *P* and edges representing the union of three binary relations. Each relation expresses a different kind of causal dependency (modality) between pairs of ports *p* and *q*:

- *q strongly depends on p* if the execution of *p* must be followed by the execution of *q*. That is, *p* and *q* cannot be executed independently, only the sequence *pq* is possible;
- *q weakly depends on* p if the execution of *p* may be followed by *q*. That is either *p* can be executed alone or the sequence *pq*;
- *q conditionally depends on p* if when both *p* and *q* are executed, then *q* must follow *p*. Conditional dependency requires that if *p* and *q* occur then only the sequence *pq* is possible; otherwise *p* or *q* may be independently executed.

The semantics of a modal flow component is defined by an atomic BIP component further restricted by a priority order on ports. The Petri net is derived from the modal flow graph as follows. We define a transition for every port in the modal flow graph. Moreover, we define an extra transition, labeled by a distinguished *sync* port, to delimit successive computation steps. Places of the net are defined for minimal ports in the modal flow graph as well as for

every pair of dependent ports. The former are used to initialize the computation, whereas the latter are used to enforce the right order of execution between dependent ports. According to their definition, places can be tagged as initial, final, or both. The *sync* transition is enabled when only final places are marked. In this case, termination of a step consists in removing tokens from the final places and putting a token in each initial place. Finally, we consider a priority order on ports which ensures maximal progress in every computation step: first, all (regular) ports have higher priority than *sync* and second, every port has higher priority than all its dependent ports in the modal flow graph.

47. Contract-based verification for rich interaction models (Verimag):
In the context of the SPEEDS project, we have refined the general framework for contract-based reasoning that we have developed in Year 1. Previously, we started from contracts and notions of satisfaction of contracts and dominance between contracts as they are defined in the SPEEDS project and from similar notions in the literature. We had made some proposals for the expression of proper encapsulation in BIP and had given a proof rule for dominance in the resulting framework. Now 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. We also define general reasoning schemas for proving dominance (refinement between contracts) including circular and semi-circular reasoning; their applicability in a particular framework is checked by means of verification conditions depending on the properties of the behavior description formalism, the notion of refinement on behaviors, and the composition model. We also started to work on a contract-based design methodology.

48. Modeling platform properties with AADL and BIP (Verimag)
This year, e studied a general methodology and an associated tool for translating AADL (Architecture Analysis and Design Language) and annex behavior specification into the BIP (Behavior Interaction Priority) language. This allows simulation of systems specified in AADL and application to these systems of formal verification techniques developed for BIP, e.g. deadlock detection. Using model transformations allows performing analysis on the models prior to code generation. The tool generating BIP from AADL has been implemented in Java, as a set of plug-in for the open source Eclipse platform. Models generated may be timed or untimed. Timed models can be transformed into untimed models in which time progress is represented by a tick port that exists in all timed components and a connector connecting all tick ports. We provide two extensions of our translation:

1- Data flow communication between AADL components is not deterministic, thus leading to non deterministic execution in general and preventing the use of AADL for most critical systems. We provide a time-triggered protocol for enforcing deterministic data flow communication among AADL threads. It requires the existence of a unique global clock for all threads. It enforces a specific communication discipline **[CB09a]**.

2- AADL provides adequate syntax and semantics to express and support distributed embedded systems. We provide an extension of our translation for building and translating AADL systems into a distributed application using network communication protocol. This allows runtime analysis to fully assess system viability, to refine and to correct the behavior of distributed system **[CB09b]**.

-- Changes wrt Y1 deliverable --

This is new text, not present in Y1 deliverables.

2.2 Individual Publications Resulting from these Achievements

CEA

[CRGT 09] Arnaud Cuccuru, Ansgar Radermacher, Sébastien Gérard, and François Terrier, "Constraining Type Parameters of UML 2 Templates with Substitutable Classifiers", in proceeding of the 12th International Conference on Model Driven Engineering Languages and Systems (MoDELS'2009), LNCS 5795, pp. 644–649, Denver, Texas, USA, October 4-9, 2009, (Acceptance rate: 18%, Rank (CORE): A).

[RCGT] Ansgar Radermacher, Arnaud Cuccuru, Sébastien Gérard and François Terrier, "Generating Execution Infrastructures for Component-oriented Specifications With a Model Driven Toolchain: A case study for MARTE's GCM and real-time annotations", in 8th International Conference on Generative Programming and Component Engineering (GPCE 2009), Denver, Colorado, October 4-5, 2009, (Acceptance rate : 31%, Rank (CORE) : B).

[ESCG 09] Huascar Espinoza, Bran Selic, Daniela Cancila, and Sébastien Gérard, "Challenges in Combining SysML and MARTE for Model-Based Design of Embedded Systems", in proceeding of the international conference Model Driven Architecture - Foundations and Applications (ECMDA'2009), LNCS Volume 5562/2009, pp. 98-113, Enschede, The Netherlands, June 23-26, 2009.

[CRCGT 09] Wasim EL Hajj Chehade, Ansgar Radermacher, Arnaud Cuccuru, Sébastien Gérard, François Terrier, "Automating the generation of platform specific models", 4th IEEE international workshop UML and AADL, Potsdam, Germany, June 2nd, 2009.

CISS

[CCC09] Uli Fahrenberg, Kim Guldstrand Larsen, and Claus Thrane. A quantitative characterization of weighted Kripke structures in temporal logic. Abstract for invited talk, workshop on Quantitative logics, satellite event of ICALP 2009, Rhodes, Greece.

[CCC09] Uli Fahrenberg and Kim G. Larsen. Discount-optimal infinite runs in priced timed automata. Electronic Notes in Theoretical Computer Science, 239:179 { 191, 2009. Joint Proceedings of the 8th, 9th, and 10th International Workshops on Verification of Infinite-State Systems (INFINITY 2006, 2007, 2008)

[KRS09] Knoll, Istvan ; Ravn, Anders Peter ; Skou, Arne. Semantics for Communicating Actors with Interdependent Real-Time Deadlines. / In: Proceedings of Third IEEE International Symposium on Theoretical Aspects of Software Engineering, TASE 2009.. IEEE Computer Society, 2009. p. 29-35

[FL09] Ulrich Fahrenberg and Kim G. Larsen. Discounting in time. In Proceedings of 7th Workshop on Quantitative Aspects of Programming Languages, QAPL 2009, 2009.

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

[BKL09a] Nikola Benes, Jan Kretinsky, Kim G. Larsen, and Jiri Srba. Checking thorough refinement on modal transition systems is exptime-complete. In 6th International Colloquium on Theoretical Aspects of Computing (ICTAC'09), LNCS. Springer, 2009.

[BKL09b] Nikola Benes, Jan Kretinsky, Kim G. Larsen, and Jiri Srba. On determinism in modal transition systems. To appear in Theoretical Computer Science, 2009.

ESI

[CAA09a] T. B. Callo Arias, P. America, and P. Avgeriou: Defining execution viewpoints for a large and complex software-intensive system. In WICSA/ECSA 2009, Joint Working IEEE/IFIP Conference on Software Architecture & European Conference on Software Architecture, 2009

[CAA09b] T. B. Callo Arias, P. America, and P. Avgeriou: Constructing a Resource Usage View of a Large and Complex Software-Intensive System. In WCRE 2009: 16th Working Conference on Reverse Engineering, 2009

[Laa09] P. van de Laar: Supporting Evolving Product Families. In CSER 2009: 7th Annual Conference on Systems Engineering Research, 2009

[YGB+09] Y. Yang, M.C.W. Geilen, T. Basten, S. Stuijk, H. Corporaal. Exploring Trade-offs between Performance and Resource Requirements for Synchronous Dataflow Graphs. In 7th IEEE Workshop on Embedded Systems for Real-Time Multimedia, ESTIMedia 2009, pages 96-105, 2009

[SGB+09] H. Shojaei, A.H. Ghamarian, T. Basten, M.C.W. Geilen, S. Stuijk. R. Hoes. A Parameterized Compositional Multi-dimensional Multiple-choice Knapsack Heuristic for CMP Run-time Management. In 46th Design Automation Conference, DAC 2009, pages 917-922, 2009

[Hoo09] J. Hooman. Behavioural Modeling, Chapter 7 of Trader: Reliability of high-volume consumer products, Embedded Systems Institute, 2009

[MVB+09] N.Muhammad Y. Vandewoude, Y. Berbers, S. van Loo, Modelling Composite End-to-End flows with AADL, STANDRTS workshop on Euromicro Conference on Real-Time Systems (ECRTS 09), 2009

[GFV+09] M. Groothuis, R. Frijns, J. Voeten and J. Broenink. Concurrent Design of Embedded Control Software. In proceedings of the 3rd International Workshop on Multi-Paradigm Modeling, Electronic Communications of the EASST, volume 21, 2009

[VFH+09] J. Voeten, O. Florescu, J. Huang and H. Corporaal. Error Computation for Predictable Real-Time Software Synthesis. TIn: Simulation - Transactions of the Society for Modeling and Simulation International, 2009

[FVT+09] O. Florescu, J.P.M. Voeten, B.D. Theelen and H. Corporaal. Patterns for Automatic Generation of Soft Real-Time System Models. Simulation - Transactions of the Society for Modeling and Simulation International, Special issue on Multi-Paradigm Modeling: Concepts and Tools, volume 85, issue 11/12, pp 709-733, 2009

[ML09] G. Muller and P. van de Laar: Researching Reference Architectures and their relationship with frameworks, methods, techniques, and tools. In CSER 2009: 7th Annual Conference on Systems Engineering Research, 2009

INRIA

[BLPR09] N. Bertrand, A. Legay, S. Pinchinat and J.-B. Raclet. A Compositional Approach on Modal Specifications for Timed Systems. Proceedings of ICFEM: International Conference on Formal Engineering Methods, Springer. 2009. To appear.

[GR09] G. Goessler and J.-B. Raclet. Modal Contracts for Component-based Design. Proceedings of SEFM: Software Engineering and Formal Methods, IEEE Computer Society Press, 2009. To appear.

[BPR09] N. Bertrand, S. Pinchinat and J.-B. Raclet. Refinement and Consistency of Timed Modal Specifications. Proceedings of LATA: Language and Automata Theory and Applications, LNCS 5457, Springer, 2009, pp.152-163.

[RGSG09] P.S. Roop, A. Girault, R. Sinha, and G. Goessler. Specification enforcing refinement for convertibility verification. Proceedings of ACSD: IEEE International Conference on Application of Concurrency to System Design, Augsburg, Germany, July 2009.

IST

[CDH08] K. Chatterjee, L. Doyen, T. Henzinger. Quantitative Languages, in Computer Science Logic (CSL'08), 2008.

[CDH09a] K. Chatterjee, L. Doyen, T. Henzinger. Expressiveness and Closure Properties for Quantitative Languages, in Logic in Computer Science (LICS'09), 2009.

[CDH09b] K. Chatterjee, L. Doyen, T. Henzinger. Probabilistic Weighted Automata, in Concurrency Theory (CONCUR'09), 2009.

[CDH09c] K. Chatterjee, L. Doyen, T. Henzinger. Alternating Weighted Automata, in Fundamentals of Computation Theory (FCT'09), 2009.

[GHKS09] R. Guerraoui, T. Henzinger, M. Kapalka, and V. Singh. Transactions in the Jungle. Technical report, 2009.

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

[TLHL09] Stavros Tripakis, Ben Lickly, Thomas A. Henzinger, Edward A. Lee: On relational interfaces. EMSOFT 2009: 67-76.

KTH

[PT09a] Magnus Persson and Martin Törngren. Using Improved Resource Interfaces to Formally Describe Adaptability in Embedded Systems. 2nd Workshop on Adaptive and Reconfigurable Embedded Systems (APRES), October 11, 2009, part of the Embedded Systems Week (ESWEEK), Grenoble, France.

[PT09b] Magnus Persson and Martin Törngren. Using Improved Resource Interfaces to Formally Describe Adaptability in Embedded Systems (Invited paper - updated based on the corresponding APRES paper). Sigbed review - 21st issue, Volume 6, Number 3, Special Issue on the 2nd International Workshop on Adaptive and Reconfigurable Embedded Systems (APRES'09). http://sigbed.seas.upenn.edu/vol6_num3.html

[QPC*09] Model-Based Development of Middleware for Self-Configurable Embedded Real-Time Systems: Experiences from the DySCAS Project. Tahir Naseer Qureshi, Magnus Persson, DeJiu Chen, Martin Törngren and Lei Feng. Work-in-Progress session at Model-Driven Development for Distributed Real-Time Embedded Systems Summer School (MDD4DRES), Aussois, France, April 22, 2009. http://www.mdd4dres.info/_media/mdd4dreswip09_submission_13.pdf

[CTM*09] DeJiu Chen, Martin Törngren, Magnus Persson, Lei Feng and Tahir Naseer Qureshi. Towards Model-Based Engineering of Self-Configuring Embedded Systems. Model-Based Engineering of Embedded Real-Time Systems. Holger Giese, Bernard Rumpe, Bernard Schätz (eds), Springer Verlag, Scheduled to appear 2009.

[S09] Carl-Johan Sjöstedt. Modeling and Simulation of Physical Systems in a Mechatronic Context. PhD thesis, KTH. TRITA-MMK 2009:12, ISBN 978-91-7415-361-3. 2009

[SZJ+09] Ingo Sander, Jun Zhu, Axel Jantsch, Andreas Herrholz, Philipp A. Hartmanny, and Wolfgang Nebel. High-level estimation and trade-off analysis for adaptive real-time systems. In Proceedings of the 16th Reconfigurable Architectures Workshop, Rome, May 2009.

[ZSJ09] Jun Zhu, Ingo Sander, and Axel Jantsch. Buffer minimization of real-time streaming applications scheduling on hybrid CPU/FPGA architectures. In Proceedings of the Design and Test Europe Conference (DATE), April 2009.

[SAJ09] Ingo Sander, Alfonso Acosta, and Axel Jantsch. Hardware design and synthesis in ForSyDe. In Proceedings of Hardware Design and Functional Languages, York, UK, March 2009.

[Jan09] Axel Jantsch. Models of computation for distributed embedded systems. In Richard Zurawski, editor, Networked Embedded Systems. CRC Press/Taylor & Francis, 2009.

[JL09] Axel Jantsch and Zhonghai Lu, "Resource Allocation for Quality of Service in On-Chip Communication", Networks on Chip: Theory and Practice, Taylor & Francis Group LLC - CRC Press, edited by Fayez Gebali and Haytham Elmiligi, 2009.

[LMJ09] Zhonghai Lu, Mikael Millberg, Axel Jantsch, Alistair Bruce, Pieter van der Wolf, and Tomas Henriksson. Flow regulation for on-chip communication. In Proceedings of the Design Automation and Test Europe Conference (DATE), April 2009.

[LBJ09] Zhonghai Lu, Dimitris Brachos, and Axel Jantsch. A flow regulator for on-chip communication. In Proceedings of the System on Chip Conference, Belfast, 2009.

[QLD09a] Yue Qian, Zhonghai Lu and Wenhua Dou. Comparative Analysis of Worst-Case Communication Delay Bounds for 2D and 3D NoCs. In ``Workshop on 3D Integration and Interconnect-Centric Architectures'' in conjunction with ``International Symposium on High-Performance Computer Architecture 2009 (HPCA-15)'', Raleigh, North Carolina, USA, Feb., 2009.

[QLD09b] Yue Qian, Zhonghai Lu and Wenhua Dou. Analysis of Communication Delay Bounds for Network on Chips. Proceedings of 14th Asia and South Pacific Design Automation Conference (ASPDAC'09). Yokohama Japan, Jan. 2009.

[QLD09c] Yue Qian, Zhonghai Lu and Wenhua Dou. Applying Network Calculus for Worst-case Delay Bound Analysis in On-chip Networks. Proceedings of the 4th IEEE International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS'09). Cairo, Egypt, April 2009.

[QLD09d] Yue Qian, Zhonghai Lu, Wenhua Dou. Analysis of Worst-case Delay Bounds for Best-effort Communication in Wormhole Networks on Chip. Proceedings of the 3rd ACM/IEEE International Symposium on Networks-on-Chip (NOCS'09), San Diego, May 2009.

[QLD09e] Yue Qian, Zhonghai Lu and Wenhua Dou, Applying Network Calculus for Performance Analysis of Self-Similar Traffic in On-Chip Networks", IEEE/ACM/IFIP 2009 International Conference on Hardware-Software Codesign and System Synthesis (CODES+ISSS'09), Grenoble, France, Oct. 11-16, 2009.

[QLD09f] Yue Qian, Zhonghai Lu and Wenhua Dou, "From 2D to 3D NoCs: A Case Study on Worst-Case Communication Performance", IEEE/ACM 2009 International Conference on Computer-Aided Design (ICCAD'09), San Jose, Nov. 2-5, 2009.

Salzburg

[HJK+09] K. Hedrick, J. Jariyasunant, C.M. Kirsch, J. Love, E. Pereira, R. Sengupta, M. Zennaro. CSL: A Language to Specify and Re-Specify Mobile Sensor Network Behaviors. Proc. Real-Time and Embedded Technology and Applications Symposium (RTAS), 2009.

[RABK09] H. Roeck, J. Auerbach, D.F. Bacon, C.M. Kirsch. Avoiding Unbounded Priority Inversion in Barrier Protocols Using Gang Priority Management. Proc. International Workshop on Java Technologies for Real-time and Embedded Systems (JTRES), 2009.

[CKS09] S.S. Craciunas, C.M. Kirsch, A. Sokolova. A Workload-oriented Programming Model for Temporal Isolation with VBS. Online Proc. Workshop on Reconciling Performance with Predictability (RePP), 2009.

Trento

[SVS*09] A. Sangiovanni-Vincentelli, S. Shukla, J. Sztipanovits, G. Yang, D. Mathaikutty, "Metamodeling: An Emerging Representation Paradigm for System-Level Design", Special Section on Meta-Modeling, IEEE Design & Test, vol. 26, no. 3, pp. 54-69, May/June 2009.

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

[BDDD09] F. Balarin, A. Davare, M. D'Angelo, D. Densmore, T. Meyerowitz, R. Passerone, A. Pinto, A. Sangiovanni-Vincentelli, A. Simalatsar, Y. Watanabe, G. Yang and Q. Zhu. “Platform-Based Design and Frameworks: Metropolis and Metro II”. In *Model-Based Design for Embedded Systems,* chapter 10, page 259. CRC Press, Taylor and Francis Group, Boca Raton, London, New York, November 2009.

[PCSV09] A. Pinto, L. Carloni, and A. Sangiovanni-Vincentelli. "A Methodology for Constraint-Driven Synthesis of On-Chip Communications," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 28, No. 3, March 2009.

[ESV*09] S. Ergen, A. Sangiovanni-Vincentelli, X. Sun, R. Tebano, S. Alalusi, G. Audisio, M. Sabatini, "The Tire as an Intelligent Sensor" Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on Volume 28, Issue 7, July 2009 Page(s):941 – 955.

[SVD09] A. Sangiovanni-Vincentelli, and M. Di Natale, Challenges and Solutions in the Development of Automotive Systems, *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, Volume: 28, Issue: 7, pp. 937-940, July 2009.

[WDS*09] G. Wang, M. Di Natale, A. Sangiovanni-Vincentelli, "Improving the Size of Communication Buffers in Synchronous Models With Time Constraints," *IEEE Transactions on Industrial Informatics*, Volume 5, Issue 3, Aug. 2009 Page(s):229 - 240.

[WDM*09] G. Wang, M. Di Natale, P. J. Mosterman, A. Sangiovanni-Vincentelli, "Automatic Code Generation for Synchronous Reactive Communication*," ICESS*, pp.40-47, 2009 International Conference on Embedded Software and Systems, 2009.

[ZYS*09] Q. Zhu, Y. Yang, E. Scholte, M. Di Natale and A. Sangiovanni-Vincentelli, "Optimizing Extensibility in Hard Real-Time Distributed Systems", *15th IEEE Real-*

Time and Embedded Technology and Applications Symposium (RTAS), San Francisco, CA, April, 2009.

[ZZD*09] H. Zeng, W. Zheng, M. Di Natale, P. Giusto, A. Ghosal, A. Sangiovanni-Vincentelli. "Scheduling the FlexRay bus using optimization techniques". In *Proceedings of the 46th ACM/IEEE Design Automation Conference (DAC*), July 2009.

[ZDG*09] H. Zeng, M. Di Natale, P. Giusto, A. Sangiovanni-Vincentelli. "Statistical Analysis of Controller Area Network Message Response Times". In *Proceedings of the IEEE Symposium on Industrial Embedded Systems (SIES*), July 2009. [Best Paper Award].

[LDZ*09] W. Li, M. Di Natale, W. Zheng, P. Giusto, A. Sangiovanni-Vincentelli, and S.A. Seshia. "Optimizations of an application-level protocol for enhanced dependability in FlexRay," In *Procs. of the 2009 Design, Automation, and Test in Europe Conference and Exhibition (DATE'09*), pp.1076-1081, Nice, France, 2009.

[PCVS09] A. Pinto, L.P. Carloni, and A. Sangiovanni-Vincentelli. "A Methodology for Constraint-Driven Synthesis of On-Chip Communications," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 28, No. 3, March 2009.

Uppsala

[GSY*09a] Nan Guan, Martin Stigge, Wang Yi and Ge Yu. New Response Time Bounds for Fixed Priority Multiprocessor Scheduling. In the proc. of RTSS09, the 30th IEEE Real-Time Systems Symposium, December 1 - December 4, 2009 Washington, D.C., USA.

[GSY*09b] Nan Guan, Martin Stigge, Wang Yi and Ge Yu. Cache-Aware Scheduling and Analysis for Multicores. In the proc. of the 7th International Conference on Embedded Software, Oct. 12-16, Grenoble, France.

[GSY*09c] Nan Guan, Zonghua Gu, Wang Yi and Ge Yu. Improving Scalability of Model-Checking for Minimizing Buffer Requirements of Synchronous Dataflow Graphs. In the proc. of the 14th Asia and South Pacific Design Automation Conference, Jan. 19-22 2009. Yokohama, Japan.

[BGJ*09] Frank S. de Boer, Immo Grabe, Mohammad Mahdi Jaghoori, Andries Stam, and Wang Yi. Modeling and Analysis of Thread-Pools in an Industrial Communication Platform. In the proc. of the 10th International Conference on Formal Engineering Methods. Dec 9-12, 2009, Rio de Janeiro, Brazil.

VERIMAG

[BBPS09] Ananda Basu, Saddek Bensalem, Doron Peled, Joseph Sifakis. Priority Scheduling of Distributed Systems Based on Model Checking. Computer Aided Verification, 21st International Conference, CAV 2009, Grenoble, France, June 26 - July 2, 2009. Proceedings. Springer, Lecture Notes in Computer Science 5643.

[BSS09] Marius Bozga, Vassiliki Sfyrla, Joseph Sifakis: Modeling synchronous systems in BIP. EMSOFT 2009: 77-86.

[BJS09] M. Bozga, M. Jaber, J. Sifakis Source-to-Source Architecture Transformation for Performance Optimization in BIP. SIES 2009, July 8-10, Lausanne, Switzerland. IEEE.

[Sif09] Joseph Sifakis: Component-Based Construction of Heterogeneous Real-Time Systems in BIP. Petri Nets 2009

[BQG09] Imene Ben-Hafaiedh, Susanne Graf and Sophie Quinton. From Orchestration to Choreography: Memoryless and Distributed Orchestrators. Presented at Flacos'09,

Toledo, sep. 2009. Accepted for publication in the Journal of Logic and Algebraic Programming.

[BM09] T. Bouhadiba and Florence Maraninchi. Contract-based coordination of hardware components for the development of embedded software. In COORDINATION'09, the 11th international conference on Coordination Models and Languages, Lisbon, Portugal, 6 2009.

[CB09a] Mohamed Yassin Chkouri and Marius Bozga. **Deterministic Data Flow Communication in AADL**. In ICESS '09: Proceedings of the 2009 International Conference on Embedded Software and Systems, pages 93-100, 2009.

[CB09b] Mohamed Yassin Chkouri and Marius Bozga. **Prototyping of Distributed Embedded Systems Using AADL**. In Proceeding of Model Based Architecting and Construction of Embedded Systems (ACES-MB), 2009.

-- Changes wrt Y1 deliverable --

This is new text, not present in Y1 deliverables.

2.3 Interaction and Building Excellence between Partners

ESI + CISS: has started an investigation on model checking quantitative properties for stochastic dataflow models in the context of the Quasimodo project.

ESI + VERIMAG + OFFIS + University of Bologna + others collaborated in the GENESYS project for developing a reference architecture template and a suitable modeling framework.

ESI + CISS Through one of its projects affiliates (Group Frits Vaandrager, RU Nijmegen), ESI is cooperating with CISS on scheduling analysis for professional printers. A PhD student of RU Nijmegen working in the ESI research program visited CISS for one week.

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

CEA + KTH: within the ATESST2 project (http://www.atesst.org), KTH and CEA are working on the EAST-ADL language, a UML-base extension for enabling model-based design of automotive electronic system in a compliant way with Autosar and the MARTE standard.

IST Austria + INRIA are actively collaborating for developing theoretical background for studying robustness of embedded systems. INRIA (Dr. Axel Legay) had two visits of one week duration to IST Austria, and IST Austria (Dr. Dejan Nickovic) had two one-week visits to INRIA.

CISS + INRIA (Rennes) are actively collaborating on compositional specification theories for timed as well as stochastic systems. In both cases the theories may be seen as quantitative extensions of modal transition systems with corresponding quantitative notions of refinement.

CISS + LSV are actively collaborating on developing a rich theory for priced or weighted timed automata and games. In particular, extended settings with both negative and positive as well as exponential and linear cost-rates have introduced a range of new cost (or energy)

bounded problems to be formulated and partially solved. These problems are particularly relevant from the perspective of addressing energy-aware and -optimal schedules for autonomous embedded systems.

KTH + OFFIS: Within the CESAR project (https://cesarproject.eu/index.php) KTH and OFFIS are collaborating in the integration of results from the Speeds and the ATESST2 projects.

KTH + Volvo: Cooperation within both the ATESST2 and CESAR projects. This has also involved mobility of personnel. Since the autumn, PhD Lei Feng is working 50% for Volvo and 50% for KTH, acting as an industrial post-doc and bridge between Volvo and KTH.

KTH + CESAR partners (in addition to the above including EADS, Airbus, AVL, INRIA, CNRS, ABB and CRF) with longer term work in defining the CESAR reference technology platform (work towards tool interoperability, common meta-models and case studies (the CESAR project started in March 2009). The RTP will be equipped with existing and state of the art tools in the area of system design and verification techniques, with specific relevance to safety critical systems.

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

Salzburg + IST Joint work with T.A. Henzinger in exploring the fully compositional semantics of HTL with respect to language modularity.

Special Issue of the IEEE Trans on CAD on Automotive Applications (Uni. Trento, UC Berkeley, GM, TU Braunschweig, TU Vienna, Pirelli-Telecom Italia Berkeley Labs, Uni. des Saarlandes, Absint)

Uppsala + ETH Zurich worked together on combining UPPAAL with the Real Time Calculus (RTC), to improve the analysis precision of RTC and to enhance the scalability of the UPPAAL model checker.

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

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

-- Changes wrt Y1 deliverable --

This is new text, not present in Y1 deliverables.

2.4 Joint Publications Resulting from these Achievements

[Gen09] Roman Obermaisser and Hermann Kopetz (Eds). L. Benini, , S. Bensalem, M. Borth, et al. Genesys - A Candidate for an Artemis Cross-Domain Reference Architecture for Embedded Systems. Südwestdeutscher Verlag für Hochschulschriften (SVH), Saarbrücken, 2009. ISBN 978-3-8381-1040-0.

[LTS+09] J. Lapalme, B.D. Theelen, N. Stoimenov, J.P.M. Voeten, L. Thiele, E. Aboulhamid. Y-Chart Based System Design: A Discussion on Approaches. In: Nouvelles approches pour la conception d'outils CAO pour le domaine des systèmes embarqués. Université de Montréal, 2009. Invited article.

[OBG+09] Iulian Ober, Stefan Van Baelen, Susanne Graf, Mamoun Filali, Thomas Weigert, Sébastien Gérard, "Model Based Architecting and Construction of Embedded Systems", in M.R.V. Chaudron, editor, MoDELS 2008 Workshops, Lecture Notes in Computer Science (LNCS), vol. 5421, Springer-Verlag, pp. 1-4, Berlin, Germany, 2009.

[PBB+09] Robert Passerone, Imen Ben Hafaiedh, Albert Benveniste, Daniela Cancila, Arnaud Cuccuru, Wermer Damm, Alberto Ferrari, Sébastien Gérard, Susanne Graf, Bernhard Josko, L. Mangeruca, T. Peikenkamp, Alberto Sangiovanni-Vincentelli and François Terrier, Meta-models in Europe: Languages, Tools and Applications, in IEEE Design & Test of Computers (IEEE Computer Society), Special Issue on Metamodeling for Design and Test, Volume 26, Number 3, pp. 38-53, Mai/June 2009.

[BCH+09] R. Bloem and K. Chatterjee and T.A. Henzinger and B. Jobstmann. Better Quality in Synthesis through Quantitative Objectives. In Computer Aided Verification (CAV). pp. 140--156. 2009.

[BGH+09] R. Bloem, K. Greimel, T. Henzinger, B. Jobstmann. Synthesizing Robust Systems, In *Formal Methods in Computer Aided Design (FMCAD'09), 2009*

[DHLN09] L. Doyen, T. Henzinger, A. Legay, D. Nickovic. Robustness of Sequential Circuits, submitted for publication, 2009.

[HKMS09] T.A. Henzinger, C.M. Kirsch, E.R.B. Marques, A. Sokolova. Distributed, Modular HTL. Proc. Real-Time Systems Symposium (RTSS), 2009

[CDL+09] Benoit Caillaud, Benoit Delahaye, Kim G. Larsen, Mikkel Larsen, Axel Legay, and Andrzej Wasowski. Compositional design methodology with constraint Markov chains. under submission

[BFL+09] Patricia Bouyer, Ulrich Fahrenberg, Kim G. Larsen, and Nicolas Markey. Quantitative modeling and analysis of embedded systems. under submission

[BFL+09] Patricia Bouyer, Uli Fahrenberg, Kim Guldstrand Larsen, and Nicolas Markey. Exponentially priced timed automata. under submission

[CBL+09] P. Caspi, A. Benveniste, R. Lublinerman, and S. Tripakis. Actors without directors: A kahnian view of heterogeneous systems. In Hybrid Systems Computation and Control, HSCC09, volume 5469 of Lecture Notes in Computer Science, 2009

[ACG+09] M. Alras, P. Caspi, A. Girault, and P. Raymond. Model-based design of embeded control systems by means of synchronous intermediate model. In proc. of ICESS-09, 6th IEEE International Conference on Embedded Systems and Software, Hangzhou, China, 5 2009.

[PWP+09] Yiannis Papadopoulos, Martin Walker, David Parker, Henrik Lönn, Martin Törngren, DeJiu Chen, Rolf Johansson. Semi-Automatic FMEA Supporting Complex Systems with Combinations and Sequences of Failures. SAE paper number 2009-01-0738. SAE World Congress, 2009.

[WPP+09] Martin Walker, Yiannis Papadopoulos, David Parker, Henrik Lönn, Martin Törngren, DeJiu Chen, Rolf Johansson, Anders Sandberg. Semi-Automatic FMEA supporting complex systems with combinations and sequences of failures. SAE International Journal of Passenger Cars – Mechanical Systems. October 2009 2(1): 791-802.

[TCM+09] Martin Törngren, DeJiu Chen, Diana Malvius and Jakob Axelsson. Model based development of automotive embedded systems. Invited chapter. Handbook on Automotive Embedded Systems. Editors Nicolas Navet and Francoise Simonot-Lion. Taylor and Francis CRC Press - Series: Industrial Information Technology. 2009.

[CFJ+09] Philippe Cuenot, Patrik Frey, Rolf Johansson, Henrik Lönn, Yiannis Papadopoulos, Mark-Oliver Reiser, Anders Sandberg, David Servat, Ramin Tavakoli Kolagari, Martin Törngren, Matthias Weber. The EAST-ADL Architecture Description Language for Automotive Embedded Software. Invited chapter in the LNCS volume on "Model-Based Engineering of Embedded Real-Time Systems", Holger Giese, Bernard Rumpe, Bernard Schätz, Editors. To appear 2009

[RBB+09] J.-B. Raclet, E. Badouel, A. Benveniste, B. Caillaud, A. Legay and R. Passerone. Modal Interfaces: Unifying Interface Automata and Modal Specifications. Proceedings of EMSOFT: Conference on Embedded Software, ACM, 2009, pp.87-96.

[RBB+09] J.-B. Raclet, E. Badouel, A. Benveniste, B. Caillaud and R. Passerone. Why are Modalities Good for Interface Theories? Proceedings of ACSD: Application of Concurrency to System Design, IEEE Computer Society Press, 2009.

[MTSG09] Y. Ma, J.-P. Talpin, S. Shukla, T. Gautier. "Distributed Simulation of AADL Specifications in a Polychronous Model of Computation," International Conference on Embedded Software and Systems ICESS'09, pp.607-614, May 2009. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5066706&isnumber=5066609

[BPST09] J. Bijoy, H. Patel, S. Shukla, J.-P. Talpin. Generating Multi-Threaded code from Polychronous Specifications. Electr. Notes Theor. Comput. Sci. 238(1): 57-69 (2009)

[SVY+09] A. Sangiovanni-Vincentelli, G. Yang, S. Shukla, A. Mathaikutty, J. Sztipanovits. "Metamodeling: An Emerging Representation Paradigm for System-Level Design," IEEE Design & Test of Computers. vol.26, no.3, pp.54-69, May-June 2009. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5167508&isnumber=5167496

[ESS*09] Sinem Coleri Ergen, Alberto Sangiovanni-Vincentelli, Xuening Sun, Riccardo Tebano, Sayf Alalusi, Giorgio Audisio, and Marco Sabatini, *The Tire as an Intelligent Sensor*. Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on Volume: 28 Issue: 7 July 2009 Page(s): 941-955

[OEH*09] Roman Obermaisser, Christian El Salloum, Bernhard Huber, and Hermann Kopetz, *From a Federated to an Integrated Automotive Architecture* Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on Volume: 28 Issue: 7 July 2009 Page(s): 956-965

[WGR*09] Reinhard Wilhelm, Daniel Grund, Jan Reineke, Marc Schlickling, Markus Pister, and Christian Ferdinand, *Memory Hierarchies, Pipelines, and Buses for Future Architectures in Time-Critical Embedded Systems. Systems IEEE Transactions on CAD, Special Issue on DATE 08 Automitive Day Volume: 28 Issue: 7 July 2009 Page(s): 966-978*

[SRN09] Simon Schliecker, Jonas Rox, Mircea Negrean, Kai Richter, Marek Jersak, and Rolf Ernst, *System Level Performance Analysis for Real-Time Automotive Multi-Core and Network Architectures*. Architectures Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on Volume: 28 Issue: 7 July 2009 Page(s): 979-992

-- Changes wrt Y1 deliverable --

This is new text, not present in Y1 deliverables.

2.5 Keynotes, Workshops, Tutorials

Keynote: Reliable Embedded Multimedia Systems?
Twan Basten - Computer Engineering Seminar, University of Wisconsin - Madison, Madison, WI, 21 September 2009
http://homepages.cae.wisc.edu/~saluja/seminars/schedule.html

Keynote: Reliable Run-time Adaptation in Resource-constrained Embedded Systems
Twan Basten - Royal Institute of Technology (KTH), Stockholm, Sweden, 25 May 2009

Keynote: Reliable Run-time Adaptation in Resource-constrained Embedded Systems
Twan Basten - ECE Seminar, Carnegie Mellon University, Pittsburgh, PA, 17 September 2009
www.ece.cmu.edu/news/seminar/2009/fall/basten_09_17_09.pdf

Keynote: Design-Space Exploration of High-Tech Embedded Systems
Twan Basten - ESI Symposium, Eindhoven, Netherlands, 8 December 2009
http://www.esi.nl/frames.html?/events/esi_symposium_2009/

Keynote: Reliable Dynamic Embedded Data Processing Systems
Twan Basten - IPA Fall Days on Quantitative Methods for Embedded Systems, Noordwijk aan Zee, Netherlands, 26 November 2009
http://www.win.tue.nl/ipa/activities/falldays2009

Keynote: Reliable Run-time Adaptation in Resource-constrained Embedded Systems
Twan Basten - CeDICT Workshop on Dependable ICT Systems, Utrecht, Netherlands, 24 April 2009
http://nirict.3tu.nl/meetings-nirict/24-04-09CeDICT/

Keynote: Dataflow Analysis Revisited
Twan Basten - ST-Ericsson, Eindhoven, 19 February 2009

Keynote: Modeling and Exploration of Printer Data-Paths
Roelof Hamberg - ESI Symposium, Eindhoven, Netherlands, 8 December 2009
http://www.esi.nl/frames.html?/events/esi_symposium_2009/

Keynote: A Performance Analysis Tool for Scenario-Aware Streaming Applications
Bart Theelen - IPA Fall Days on Quantitative Methods for Embedded Systems, Noordwijk aan Zee, Netherlands, 25 November 2009
http://www.win.tue.nl/ipa/activities/falldays2009

Keynote: "A profile for embedded systems development"
Sébastien Gérard and Huascar Espinoza. Invited Talk. 4th International School on MDD for Distributed, Realtime and Embedded systems, Aussois (France), 20-24 April 2009.
http://www.mdd4dres.info/

Keynote: From Boolean to Quantitative System Specifications
Tom Henzinger - Invited talk - *Workshop on Quantitative Analysis of Software (QA'09), on June 28, 2009 in Grenoble, France*
http://www.eecs.berkeley.edu/~sseshia/qa09/

Keynote: "Multiparadigm modeling in the Mechatronics domain"
Martin Törngren*. Invited Talk.* Bellairs Computer Automated Multi-Paradigm Modeling workshop *2009.* http://msdl.cs.mcgill.ca/conferences/CAMPaM/2009/

Keynote: " "What are visionary and futuristic domains where advances in CPS will have broad impact?""
Christoph Kirsch**,** *Invited Panelist.* CPSWEEK 2009, San Francisco http://varma.ece.cmu.edu/CPS-Forum/ and
http://varma.ece.cmu.edu/CPS-Forum/Presentations/Kirsch.pdf

Keynote: Collaborate to Innovate, by Alberto Sangiovanni Vincentelli, annual customer meeting TSMC
San Jose', April 21st
This is the annual conference held by TSMC in United States. This year there were more than 2,000 attendants from all over the world. The keynote addressed the issues of system level design and the novel direction of research in the area of advanced electronics and energy efficient buildings. The angle taken was that the new challenges for the electronic and system industry can only be tackled with rigorous design methodologies and tools that support collaboration.

Lectio Magistralis: **EDA: 40 years of innovation, by Alberto Sangiovanni Vincentelli**
Strathclyde University, Glasgow, August 10, 2009
This lecture was given to the members of the Royal Society of Edinburgh and to other invited guests in the occasion of the Maxwell Award ceremony. Alberto Sangiovanni Vincentelli presented how EDA was born and what were its early challenges. In addition, the raise of the EDA industry and the key contributions to the field were outlined.

Symposium: European Universities and Researchers as Sources of Innovation in Finland, Italy and Silicon Valley
European Entrepreneurship & Innovation Thought Leaders Seminar, Stanford University,04/09
Alberto Sangiovanni Vincentelli presented his view on the innovation scenarios in US and Europe and what can be done to improve the communication between the two innovation communities especially in the area of embedded systems.

Keynote: Component-based construction of real-time systems in BIP.
Joseph Sifakis. -- 21st International Conference, CAV 2009, Grenoble, June 2009
http://www-cav2009.imag.fr/

Keynote: The quest for correctness-beyond a posteriori verification.
Joseph Sifakis. -- 16th International SPIN Workshop, Grenoble, June 2009
http://ti.arc.nasa.gov/event/spin09/

Keynote: Embedded systems design - Scientific challenges and work directions.
Joseph Sifakis. – DATE 2009, Nice, April 2009
http://www.date-conference.com/date09/

Keynote: Component-Based Construction of Heterogeneous Real-Time Systems in BIP.
Joseph Sifakis. – Petri Nets 2009, Paris, June 2009
http://petrinets2009.lip6.fr/

Keynote: Embedded systems design - Scientific challenges and work directions.
Joseph Sifakis. – SEFM 2009, Hanoi, November 2009
http://www.iist.unu.edu/sefm2009/

Conference: International Conference on Embedded Software (EMSOFT)
Grenoble -- October 12 - 16*, 2009*
The International Conference on Embedded Software (EMSOFT) brings together researchers and developers from academia, industry, and government to advance the science, engineering, and technology in embedded software development. EMSOFT is part of the 2009 Embedded Systems week.
http://www.emsoft.org/

Conference : ACM SIGPLAN/SIGBED Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES 2009)
Dublin, Ireland, June 19-20, 2009 .
The ArtistDesign-supported ACM SIGPLAN/SIGBED Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES) continued in 2009 its tradition of being the premier forum for presentation of research results on leading edge issues in embedded systems. The CfP attracted 81 submissions including 31 papers from the Americas, 33 from Europe, and 17 papers from Asia. Each paper was reviewed by 3 PC members and 1 external reviewer. The PC accepted 18 papers that cover a variety of topics, including programming languages and compiler optimizations, scheduling, architectures and multicores, and runtime system support in embedded systems.

http://www.cse.psu.edu/lctes09/

Workshop : ArtistDesign Workshop on Embedded Systems in Healthcare 2009
Eindhoven, The Netherlands, 7 December 2009.
The goal of the Workshop on Embedded Systems in Healthcare is to strengthen the connections between academic research and industry, or to be more precise, to increase the understanding in the academic world of industrial issues in embedded systems engineering and together come to a shared agreement on research directions that seem worthwhile to pursue. The speakers at the workshop work at different medical companies or are participants in the ArtistDesign network with extensive experience in healthcare. The topics include "How to design long lasting devices for a fast changing world?", "Cochlear Implant Systems: today's challenges in embedded firmware design", and "Embedded Contributions to an Intensive Care Safety Concept".

http://www.artist-embedded.org/artist/WESH-2009.html

Workshop : 2nd International Workshop on Model Based Architecting and Construction of Embedded Systems (ACES^{MB} 2009)

ACM/IEEE 12th Int. Conf. on Model Driven Engineering Languages and Systems
Denver, Colorado, USA – October 6th, 2009

The development of embedded systems with real-time and other critical constraints raises distinctive problems. In particular, development teams have to make very specific architectural choices and handle key non-functional constraints related to, for example, real-time deadlines and to platform parameters like energy consumption or memory footprint. In this context, the last few years have seen an increased interest in using model-based engineering (MBE) techniques. MBE techniques are interesting and promising for the following reasons: They allow to capture dedicated architectural and non-functional information in precise (and even formal) domain-specific models, and they support a layered construction of systems, in which the (platform independent) functional aspects are kept separate from architectural and non-functional (platform specific) aspects, where the final system is obtained by combining these aspects later using model transformations. The topics handled in the workshop were: Architecture description languages (ADLs); Domain specific design and implementation languages; Languages for capturing non-functional constraints; Component languages and system description languages.
http://www.artist-embedded.org/artist/Overview,1706.html

Workshop : Second IEEE International workshop UML and Formal Methods

11th International Conference on Formal Engineering Methods
Rio de Janeiro, Brasil – December 8th, 2009

Many interest groups from a research perspective are in favour of the creation of this workshop. For 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 second workshop will be open to various subjects as the main objective is to encourage new initiatives of building bridges between informal, semi-formal and formal notations.
http://www.artist-embedded.org/artist/Overview,1663.html

Workshop : Fourth IEEE International workshop UML and AADL
14th International Conference on Engineering of Complex Computer Systems
Potsdam, Germany – June 2nd, 2009

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 is 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,1579.html

Workshop: Dagstuhl Seminar "Design and Validation of Embedded Systems"
Dagstuhl -- September 30 – October 4*, 2009*
The aim of this seminar was to discuss topics related to systems with concurrency in a broad set of application domains. We had a broad participation reflecting the various approaches to the problem, including language design, compiler construction, program analysis, formal methods, and testing. To focus the discussions, the seminar also included participants from application areas (embedded reactive systems, robotics, middleware, operating systems, and virtual machines) who have strong interests in verification. We hope these discussions inspired researchers to come up with long-term and practical solutions for the design and verification of concurrent systems. The seminar gathered almost 50 participants.
http://www.dagstuhl.de/de/programm/kalender/semhp/?semnr=09361

Workshop: 2nd International Workshop on Verification and Validation of Planning and Scheduling Systems
Toulouse -- September 29th, 2009
This ARTIST workshop is held in conjunction with ICAPS 2009. Verification techniques, such as model checking, and planning techniques have many commonalities. Planning and scheduling (P&S) systems are finding increased application in safety- and mission-critical systems that require a high level of assurance. Experience has shown that most errors are in domain models, which can be inconsistent, incomplete or inaccurate models of the target domains. However tools and methodologies for verification and validation (V&V) of P&S systems have received relatively little attention. The objective of this workshop is to maintain an interaction between the V&V and P&S communities, to identify specialized and innovative V&V tools and methodologies that can be applied to P&S. Topics of interest include: V&V of domain models, using technologies such as static analysis, theorem proving, and model checking; consistency and completeness of domain models; domain model coverage metrics; regression, stress and boundary testing; runtime verification of plan executions; generation of robust plans; compositional verification of domain models; how to structure domain models which are more amenable to static analysis; inspection methods; the relationship between timed automata and domain models; investigations of the impact wrt. V&V of procedural versus declarative plan models; etc..
http://www-vvps09.imag.fr/

-- Changes wrt Y1 deliverable --

This is new text, not present in Y1 deliverables.

3. Milestones, and Future Evolution

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

Within each sub-activity, the partners will continue to develop and extend the results obtained in the first 2 years. We are also working on implementations of our previous results, and we plan to make new tool developments (either extensions of existing tools, or new prototypes) in the next year. This should trigger new research directions, and enhance the dissemination of the results. We give below a short list of the problems that will be addressed in Year 3.

Sub-activity A (*Component Modeling)*

CEA will 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.

CISS and VERIMAG have made initial progress towards the planned support for on-line testing of hybrid systems with respect timed automata specification that will be pursued further in the second year.

CISS will implement the timed specification theory developed in UPPAAL allowing for refinement and consistency checking between specifications of a given component to be made, as well as allowing for composition and compatibility between specifications of different components to be made.

CISS will together with INRIA (Rennes) investigate the possible implementation of the stochastic specification theory developed.

INRIA will continue to investigate a contract-based design flow by adding new operations on modal contracts which will be validated on small case studies. INRIA will consider the case of "dynamic" assume/guarantee contracts which may be violated by an implementation.

IST Austria plans to extend the theory of relational interfaces to a real-time setting.

IST Austria and INRIA plan to study the preservation of robustness by composition of sequential circuits.

Within the ATESST2 project, KTH will investigate the state of the art of model transformation technologies and continue the work on model transformations connecting EAST-ADL (UML/SysML) with models used for safety analysis and behavior modeling (Simulink/Modelica).

KTH is also together with partners including Volvo and CEA, further consolidating the support of the EAST-ADL modeling language for the forthcoming ISO26262 standard on functional safety.

Moreover, native behavior modeling capabilities of the EAST-ADL will be further investigated. As a cooperation between the CESAR and the ATESST2 project, the harmonization and integration of the EAST-ADL and the SPEEDS rich component model will be investigated with the idea to provide a proposal for the CESAR reference technology platform. Most of these above mentioned KTH activities relate both to component modeling and to resource modeling.

KTH will further develop the ForSyDe based modeling framework in SystemC, in cooperation with DUT and Tampere Technical University. The focus is on the integration of heterogeneous components, which can be modeled as continuous time, discrete time,

synchronous and untimed models. SystemC templates for these different types of component models will be developed as well as templates for interfaces between these different models of computation. The interfaces will define the time relations between the different modeling domains.

As continuation of its performance analysis activity, KTH will develop an on-chip infrastructure dimensioning technique. Given a set of application data flows with bandwidth and latency requirements, we will develop an optimization heuristic that dimensions the communication infrastructure, the various buffers and defines the arbitration policies that govern the access to shared resources such as memory controllers, switches, links and buffers.

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

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

VERIMAG will continue to develop a contract-based design methodology.

Sub-activity B (Resource Modeling)

CEA will explore how to model resources using MARTE and account for this modeling within analysis-aware processes. CEA will continue its work of integration of scheduling analysis within a model-based and component-based process.

CISS has developed and implemented tool support for the formalism of probabilistic timed automata. In the second year the planned investigation of a priced extension will be pursued.

CISS will work on the formalism of Time-Arc Petri Net and its use in modeling boolean resources will be made.

CISS will together with DTU work on applying timed automata technology to multi-processor schedulability and WCET analysis will be continued, involving usage of recently implemented support for stopwatches in UPPAAL.

ESI intends to development a multi-disciplinary design methodology for embedded mechatronic control systems that satisfy stringent resource constraints and performance requirements. The focus will be on scalability (allowing the scientific techniques to scale to systems of industrial scale and complexity), performance modeling (allowing (stochastic) system performance properties to be predicted in an accurate way), networked and distributed control (allowing the development of optimal networked and distributed control algorithms) and predictable synthesis (allowing correctness-preserving transformation from models to algorithms and hardware).

ESI will further develop its work on design-space exploration of high-tech embedded systems. The goal is to integrate CPNTools, Uppaal, and SDF3 into a common design-space exploration framework, to make those tools available for design-space exploration of high-tech embedded systems. The aim for year 3 is to support analyses by the various tools for professional printers, initially targeting the dimensioning and optimization of platforms for a fixed set of use cases.

Salzburg intends to work on developing CSL and workload-oriented programming further. CSL requires compiler and runtime system work. In particular, the CSL compiler needs to check more advanced correctness requirements while the runtime system needs to be

enhanced to work with heterogeneous computational platforms. We plan to refine workload-oriented programming and potentially apply it to multimedia applications.

Trento will explore how to evaluate unified architectures for distributed systems with particular attention to wireless protocols and wired infrastructure for energy efficient buildings, avionics and automotive.

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

Sub-activity C (Quantitative Modeling)

CISS will together with LSV work on a number of open problems concerning energy-bounded games for priced timed automata with negative and positive rates as well as linear and exponential rates.

CISS will continue work on developing and applying the general metric-based theory for weighted transition systems.

IST Austria and INRIA plan to extend their study of robustness to asynchronous circuits and other more quantitative modes.

Trento and INRIA plan to extend the work on Loosely Time Triggered Architectures to analyze the various options available for evaluating and contrasting these architectures with purely synchronous one and fully asynchronous ones.

-- Changes wrt Y1 deliverable --

This is new text, not present in Y1 deliverables.

3.2 Current and Future Milestones

- **CEA**
  will continue working on MARTE-based tool support. CEA will 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. **CEA** will explore how to model resources using MARTE and account for this modeling within analysis-aware process and will continue its work of integration of scheduling analysis within a model-based and component-based process
- **CISS**
  will implement the timed specification theory developed in UPPAAL allowing for refinement and consistency checking between specifications of a given component to be made, as well as allowing for composition and compatibility between specifications of different components to be made
- **ESI**
  will further develop its work on design-space exploration of high-tech embedded systems. The goal is to integrate CPNTools, Uppaal, and SDF3 into a common design-space

exploration framework, to make those tools available for design-space exploration of high-tech embedded systems.

- **INRIA, Trento and Parades**
  will study extensions of contract-based design approaches by considering modal specifications, extension to quantitative and dynamic aspects and methodological aspects.
- **IST and INRIA**
  plan to extend their study of robustness to asynchronous circuits and other more quantitative modes
- **KTH**
  will further develop the ForSyDe based modeling framework in SystemC, in cooperation with DUT and Tampere Technical University. The focus is on the integration of heterogeneous components, which can be modeled as continuous time, discrete time, synchronous and untimed models. SystemC templates for these different types of component models will be
- **Salzburg**
  intends to work on developing CSL and workload-oriented programming further. CSL requires compiler and runtime system work. In particular, the CSL compiler needs to check more advanced correctness requirements while the runtime system needs to be enhanced to work with heterogeneous computational platforms. We plan to refine workload-oriented programming and potentially apply it to multimedia applications
- **Trento**
  will continue its work on design frameworks for large and small-scale systems based on metamodeling and quantity management. In addition, the COSI framework will be extensively leveraged in applications such as avionics and energy efficient buildings.
- **Uppsala**
  will work on extending UPPAAL and TIMES for multiprocessor scheduling, in particular we will add the RTC analysis framework in the UPPAAL too
- **VERIMAG**
  plans to investigate and experiment thoroughly the spectrum of distributed implementations for BIP components. Particularly efficient solutions are foreseen for different classes of systems e.g., without conflicts on interactions, using shared-memory, synchronous systems

Generally, we have progressed this year according to the plans. But some of the milestones have not been addressed. In particular, no progress is reported on

- The extension of the existing bi-criterion for scheduling, to take into account forms of replication
- Predictable architecture based on Starpro.
- Methodology based on heterogeneous rich components for SYSML or EAST-ADL realizable using COTS design tools.

-- Changes wrt Y1 deliverable --

This is new text, not present in Y1 deliverables.

3.3 Main Funding

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

- **ACROSS ARTEMIS Project**
  It is the objective of the ACROSS project to develop and implement an ARTEMIS cross-domain reference architecture for embedded systems based on the architecture blueprint developed in the European FP7 project GENESYS. The ACROSS reference architecture will implement a *stable set of core services* cost- and energy efficiently in hardware as a foundation for the development of applications.
- **ADAMS**
  The main objective of the ADAMS project is to promote the industrial exploitation and enhancement of the MARTE and other relevant standards for the development of real-time and embedded systems using both, model and component design paradigms.
  http://www.adams-project.org
- **ArtistDesign**, Austrian Federal Ministry of Science and Research, Grant 651.394/0001-II/2/2009 (Supplemental Support).
- **ATESST (Advancing Traffic Efficiency and Safety through Software Technology)**
  ATESST2 is a two-year European project (FP7, Strep), coordinated by Volvo Technology and including OEMs, Suppliers/Tool vendors and Universities.
  http://www.atesst.org
- **CESAR - Cost-efficient methods and processes for safety relevant embedded systems**. CESAR is an Artemis project three year project resulting from the first call of Artemis. The project focuses on the gathering, and further development, of methods and tools for safety critical embedded systems. The project has a large number of industrial and academic partners.
  https://cesarproject.eu/index.php
- **COMBEST (funded by European Union IST STREP)**
  COMponent-Based Embedded Systems design Techniques. COMBEST aims at enhancing techniques for the correct design of embedded systems. Combest emerged from collaborations in SPEEDS and ARTIST. Verimag, ETHZ, U. Braunschweig, IST, INRIA, OFFIS, U. Trento are partners.
  http://www.combest.eu
- **Concurrent Programming with Threading by Appointment**
  Austrian Science Fund (FWF), Grant P18913-N15 (three PhD students).
- **Condor project**
  The Condor project is partially supported by the Dutch Ministry of Economic Affairs under the BSIK program. It concentrates in system performance and evolvability. Case studies are based on electron microscopes of FEI Company. Partners are ESI, Eindhoven University of Technology, Delft University of Technology, Katholieke Universiteit Leuven and University of Antwerp. Second participating industrial partner is Technolution, an SME company on technical automation and embedded systems.

  http://www.esi.nl/condor/.
- **CoDeR-MP** - Real-Time Applications on Multicore Platforms, Supported by the Swedish strategic research foundation

- **CREDO** (http://www.cwi.nl/projects/credo/), Modeling and analysis of evolutionary structures for distributed services, supported by EU
- **DaNES - Danish Network of Embedded Systems**
  Danish national project sponsored by the Danish Advanced Technology Foundation. The goal of DaNES is to determine, develop and test a model-driven and component-based development-process for the realization of the intelligent embedded systems of the future, cross-cutting the industrial sectors spanned by the participating partners. http://www.danes.aau.dk/
- **Darwin project.**
  The Darwin project addresses system evolvability, using MRI scanners of Philips Healthcare as sources for cases studies. Other partners are ESI, Philips Research, Delft University of Technology, Eindhoven University of Technology, University of Groningen (RuG), University of Twente, and the Vrije Universiteit Amsterdam. Partially supported by the Dutch Ministry of Economic Affairs under the BSIK program.
  http://www.esi.nl/darwin/.
- **Dynamically Self-Configuring Automotive Systems (FP6)**
  DySCAS is a research project funded by the European Commission within FP6. The project started June 1 2006 and will end in February 2009. A Final Workshop will be arranged in Brussels February 18, 2009. The main objective of the DySCAS project is the elaboration of fundamental concepts and architectural guidelines, as well as methods and tools for the development of self-configurable systems in the context of embedded vehicle electronic systems.
  http:/www.dyscas.org
- **Falcon project**
  The Falcon project focuses on system performance and reliability of a new generation of distribution centers. It is partially supported by the Dutch Ministry of Economic Affairs under the BSIK program. The carrying industrial partner is Vanderlande Industries. Other partners are ESI, Eindhoven University of Technology, Delft University of Technology and University of Twente.
  http://www.esi.nl/falcon/.
- **GASICS**
  European Project sponsored by European Science Foundation (ESF).
- **The JAviator Project, IBM Faculty Award 2007 (Helicopter Platform).**
- **Poseidon project**
  The Poseidon project is partially supported by the Dutch Ministry of Economic Affairs under the BSIK program. It concentrates on system evolvability and reliability of systems of systems, Thales Above Water Systems Division provides the industrial challenge, Second participating industrial partner is Noldus Technology. Other partners are ESI, Delft University of Technology, Eindhoven University of Technology, Free University of Amsterdam, University of Amsterdam, University of Maastricht, and University of Twente.
  http://www.esi.nl/poseidon/.
- **MARAE**
  MARAE is a French industrial project on robust methods to develop autonomous systems (2008-2010), with ARTIST partner VERIMAG in collaboration with ASTRIUM (EADS) and LAAS. This project is funded by FNRAE ("Fondation Nationale pour la Recherche en Aéronautique et l'Espace")

- **"Modeling and verification of timed systems"** supported by the Swedish research council
- **MoDES**
  Danish national project sponsored by the Strategic Research Council.
- **MT-LAB - Danish Network of Embedded Systems**
  DaNES. Danish national project sponsored by the Danish Advanced Technology Foundation. The goal of DaNES is to determine, develop and test a model-driven and component-based development-process for the realization of the intelligent embedded systems of the future, cross-cutting the industrial sectors spanned by the participating partners.
  http://www.danes.aau.dk/
- **Multiform**
  Project under the 7th Framework Programme of the European Committee. The main goal of the Multiform project is the integration and support for interoperability of tools and methods based on different modeling formalisms. Partners are ESI, University Dortmund, Eindhoven University of Technology, University Joseph Fourier, RWTH Aachen, Aalborg University, VEMAC and KVCA.
  http://www.ict-multiform.eu
- **Octopus project**
  Partially supported by the Dutch Ministry of Economic Affairs under the BSIK program. The Octopus project addresses system adaptability in the context of digital document printers of company Océ. Other partners are ESI, Delft University of Technology, Eindhoven University of Technology, Radboud University Nijmegen, and University of Twente.
  http://www.esi.nl/octopus/
- **Quasimodo.**
  Project under the 7th Framework Programme of the European Committee. The main objective is to develop new techniques and tools for model-driven design, analysis, testing and code-generation for advanced embedded systems where ensuring quantitative bounds on resource consumption is a central problem. Partners are ESI, CISS, Radboud University Nijmegen, University of Twente, CNRS & ENS, RTWH Aachen, University of Saarland. UL Bruxelles, Terma, Chess and Hydac
  http://www.quasimodo.aau.dk/
- **REVE project.**
  Safe reuse of embedded components in heterogeneous environments.
  http://www.ara-reve.org
- **RT-Simex**
  is a French National Research Agency funded project. This 3 years project started in January 2009 and involves Aonix, CEA LIST, INRIA, Obeo, UBO and Thales Research and Technology. The goal of the project is to provide a platform for real-time models simulation and debugging.
- **SMECY ARTEMIS Project**
  The goal of this ARTEMIS project is to launch an ambitious European initiative to allow Europe to catch up with Asia and USA (e.g. PARLAB in Berkeley, Parallel@illinois and Pervasive Parallelism Laboratory in Stanford) and to enable Europe to become the leader.
- **SNSF** (Swiss National Science Foundation).
- **SPEEDS IP project**
  The SPEEDS project aims at significant enhancement of model-based systems

engineering by semantics-based modeling for complex embedded systems using heterogeneous sub-system models, an by sound integration of existing and new tools using contract-based compositional analysis. Includes the ARTIST partners INRIA, OFFIS, PARADES and VERIMAG and affiliated industrial partners EADS and IAI.

http://www.speeds.eu.com/

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

4. Internal Reviewers for this Deliverable

- Kim Larsen (Aalborg)
- Martin Törngren (KTH)