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

Activity - Progress Report for Year 1

JPRA Activity (WP3)

Modeling

Clusters:

Modeling and Validation

Activity Leader:

Prof. Thomas A. Henzinger (EPFL, Switzerland)

http://mtc.epfl.ch/~tah/

Policy Objective

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

Versions

number	comment	date
1.0	First version delivered to the reviewers	December 19th 2008

Table of Contents

1. Overview of the Activity

1.1 ArtistDesign Participants and Roles

Dr. Ir. Twan Basten, (ESI Research Fellow, The Netherlands)
Resource and quantitative modelling (Octopus project).

Dr. Michael Borth (ESI Research Fellow, The Netherlands)
Resource and quantitative modelling (Poseidon and Genesys projects).

Prof. Dr. Ed Brinksma (Scientific Director of the ESI, The Netherlands)
Quantitative modelling.

Prof. Dr. Werner Damm (OFFIS, Germany)
Component-based design and semantic foundation, in particular non-functional aspects as real-time and safety.

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

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.

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

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

Dr. R. Hamberg, (ESI Research Fellow, The Netherlands)
Resource and quantitative modelling (Falcon and Octopus projects).

Prof. Thomas A. Henzinger (EPFL, Switzerland)
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.

Dr. Jozef Hooman (ESI Research Fellow, The Netherlands)
Resource modelling (Trader project).

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

Prof. Karl-Henrik Johansson, KTH, Stockholm, Sweden
Integrated models of behaviour, formal analysis and model refinements.

Prof. Christoph Kirsch (University of Salzburg, Austria)
Compositional timing and reliability modeling in the Giotto family of languages.

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

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

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

Dr. Ir. Jeroen Voeten (ESI Research Fellow, The Netherlands)
Quantitative modelling (Ideals project and Quasimodo).

Prof. Wang Yi (Uppsala University, Sweden)
Resource modelling and Timing Analysis.

1.2 Affiliated Participants and Roles

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

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

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

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

Prof. Dr. Koos Rooda, (TU Eindhoven, The Netherlands)
Systems engineering (Darwin project).

Prof. Dr. Paul van den Bosch (TU Eindhoven, The Netherlands)
Resource modeling (Condor project).

Prof. Dr. Paul van den Hof, (TU Delft, The Netherlands)
Performance modelling (Condor project).

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

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

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

Prof. Pierre Wolper (CFV, Belgium)
Computer-aided verification

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.

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 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.

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 centred around 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 a better understanding of component modelling, resource modelling, and quantitative modelling.

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 behavioural 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, eventtriggered, loosely time-triggered, etc. Research must further study 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 realvalued rewards (or costs), and Boolean-valued refinement relations are replaced by realvalued similarity metrics.

Quantitative models are also required for modelling stochastic behaviour, real-time behaviour, and hybrid (mixed discrete-continuous) behaviour. Our current models for such systems (Markov processes; timed automata; hybrid automata) tend to be brittle and overly sensitive towards arbitrarily small numeric perturburances. We need robust models for stochastic, timed, and hybrid systems.

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. multipriced 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 modelling.

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 Modelling)

CEA investigates the ability of MARTE, and especially its High-Level Application Modelling 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 (Technical Achievement 1).

CISS has worked on multipriced 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 (Technical Achievements 5,9,10,13,18).

CISS and EPFL are working on modal transistion systems as interface specifications (Technical Achievements 15,19).

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 (Technical Achievement 28).

KTH in cooperation with Volvo Techology and CEA have been further developing the EAST-ADL modelling 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 has specified a tool-independant meta-model for heterogeneous rich components. Rich components are specification entities which combine several, otherwise often separately represented aspects, like fiunctionality, 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 (Technical Achievements 29,30).

VERIMAG has worked on the expressiveness of BIP and defined a new notion of expressiveness for components. VERIMAG has applied BIP to modelling of architectures of autonomous robots (Technical Achievements 39,40,42).

Sub-activity B (Resource Modelling)

CEA is working on the usage of the Hardware Resource Modelling sub-profile of MARTE combined with other modelling parts in order to enable simulation of embedded systems (Technical Achievement 2).

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 (Technical Achievement 11).

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 (Technical Achievement 21).

ESI has worked on performance modelling. 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 (Technical Achievements 25,26).

INRIA is working on design and modeling for reliability of safety-critical embedded real-time systems. All the existing heuristics for the (length, reliability) bicriteria 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 (Technical Achievement 27).

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

VERIMAG has worked on a distributed semantics for BIP and enhanced the BIP execution engines to multithreaded execution (Technical Achievement 41).

Sub-activity C (Quantitative Modelling)

CEA is defining transformations of models to link models using the MARTE's extensions contained in its High-Level Application Modelling sub-profile towards a model using the extensions provided in the sub-profile for schedulability analysis (Technical Achievement 3).

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 (Technical Achievement 20).

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 (Technical Achievements 25,26).

VERIMAG has worked on the modelling of quantitative extrafunctional properties for software-intensive embedded product lines (Technical Achievement 43).

2. Summary of Activity Progress

2.1 Technical Achievements

1. A first component-oriented pattern for ACCORD (CEA)
We defined a first design pattern using a full component-based paradigm in order to support the concept of rtUnit as defined in the MARTE specification. "rtUnit" is the concept defined in the MARTE specification supporting parallelism specification and some dedicated model of computation.

2. A first MARTE-based framework for modelling and simulating hardware platforms (CEA)
We implement here the Hardware Resource Modelling (HRM) sub-profile of MARTE and define a transformation to link HRM-based model to the simics hardware simulation platform (http://www.virtutech.com/). All this experiment are done in the context of the UML2 editor Papyrus (http://www.eclipse.org/mdt/papyrus/)

3. Model-based schedulability analysis with MARTE (CEA)
We have defined the first transformation that enables to translate a model using the UML2 composite structure for enabling component-based description, and the MARTE's HLAM (High-Level Application Modelling sub-profile) to annotate the model with the required information to define the used MoCC into a model annotated with the extension defined in the MARTE's sub-profile for schedulability analysis. This latter is then translated into the specific input language of a dedicated schedulability analysis stool such as the RTDruid tool.

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

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

6. Complexity of Decision Problems for Mixed and Modal Specifications (**CISS** + ITU, Copenhagen and Imperial College London)
We consider decision problems for modal and mixed transition systems used as specifications:

the common implementation problem (whether a set of specifications has a common implementation), the consistency problem (whether a single specification has an implementation), and the thorough refinement problem (whether all implementations of one specification are also implementations of another one). Common implementation and thorough refinement are shown to be PSPACE-hard for modal, and so also for mixed, specifications. Consistency is PSPACE-hard for mixed, while trivial for modal specifications. We also supply upper bounds suggesting strong links between these problems.

7. Testing Real-Time Systems Using UPPAAL (**CISS** + Uni. Uppsala)
This chapter presents principles and techniques for model-based black-box conformance testing of real-time systems using the Uppaal model-checking tool-suite. The basis for testing is given as a network of concurrent timed automata specified by the test engineer. Relativized input/output conformance serves as the notion of implementation correctness, essentially timed trace inclusion taking environment assumptions into account. Test cases can be generated offline and later executed, or they can be generated and executed online. For both approaches this chapter discusses how to specify test objectives, derive test sequences, apply these to the system under test, and assign a verdict.

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

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

10. Optimal infinite scheduling for multi-priced timed automata (**CISS + ESI** + LSV)
This work is concerned with the derivation of infinite schedules for timed automata that are in some sense optimal. To cover a wide class of optimality criteria we start out by introducing an

extension of the (priced) timed automata model that includes both costs and rewards as separate modelling features. A precise definition is then given of what constitutes optimal infinite behaviours for this class of models. We subsequently show that the derivation of optimal non-terminating schedules for such double-priced timed automata is computable. This is done by a reduction of the problem to the determination of optimal mean-cycles in finite graphs with weighted edges. This reduction is obtained by introducing the so-called corner-point abstraction, a powerful abstraction technique of which we show that it preserves optimal schedules.
We prove the decidability of the minimal and maximal reachability problems for multi-priced timed automata, an extension of timed automata with multiple cost variables evolving according to given rates for each location. More precisely, we consider the problems of synthesizing the minimal and maximal costs of reaching a given target location. These problems generalize conditional optimal reachability, i.e., the problem of minimizing one primary cost under individual upper bound constraints on the remaining, secondary, costs, and the problem of maximizing the primary cost under individual lower bound constraints on the secondary costs. Furthermore, under the liveness constraint that all traces eventually reach the goal location, we can synthesize all costs combinations that can reach the goal.

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

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

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

13. Discount-Optimal Infinite Runs in Priced Timed Automata (CISS)
Discount-optimal infinites scheduling for priced timed automata has been shown decidable using region-based techniques (so-called corner-point abstraction). Using discounting in

optimization criteria is a often used in Control Theory, and leads to a simple fixed-point characterization in the setting of weighted timed automata. The fixed-point characterization suggests an efficient algorithm in contrast to limit-ratio optimality.

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

15. Timed Interface Theory (CISS)
An interface theory for real-time systems using timed games have been developed. Here UPPAAL TIGA supports compatibility, refinement as well as consistency checking of component specifications.

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

17. Design Verification Patterns (CISS)
Design Verification Patterns are formal specifications that define the semantics of design patterns. For each design pattern, the corresponding verification pattern give a set of proof obligations. They must be discharged for a correct implementation of the pattern. Additionally there is a set of properties that may be used in the design and verification of applications that employ the pattern. The concept is illustrated by examples from general software engineering and more specialised properties for embedded software.

18. Model-based Schedulability Analysis of Safety Critical Hard Real-Time Java Programs (CISS)
We describe the implementation of SARTS, a model based schedulability analysis tool used for hard real-time systems. SARTS is used to translate hard real-time systems, implemented in Java, to a timed automata model in UPPAAL.
The system being analyzed must be implemented in SCJ2, a safety critical profile for Java developed in this project, based on SCJ. The target hardware is the time predictable Java processor JOP, developed specifically for hard real-time systems.
Several experiments have been conducted to illustrate the accuracy of SARTS compared to existing tools. It is shown how the model based approach can result in a more accurate analysis, than possible with traditional analyses.

19. Interface theories with component reuse (EPFL)

Interface theories have been proposed to support incremental design and independent implementability. Incremental design means that the compatibility checking of interfaces can proceed for partial system descriptions, without knowing the interfaces of all components. Independent implementability means that compatible interfaces can be refined separately, maintaining compatibility. General theories, which do not focus on a specific formalism for specifying interfaces but rather on what such formalisms can do, for interface-based design have been proposed by EPFL. We have now shown that these interface theories provide no formal support for component reuse, meaning that the same component cannot be used to implement several different interfaces in a design. We therefore added a new operation to interface theories in order to support such reuse. For example, different interfaces for the same component may refer to different aspects such as functionality, timing, and power consumption. We gave both stateless and stateful examples for interface theories with component reuse. To illustrate component reuse in interface-based design, we showed how the stateful theory provides a natural framework for specifying and refining PCI bus clients [DHJP08].

20. Quantitative generalizations of languages (EPFL)

Quantitative generalizations of classical languages, which assign to each word a real number instead of a boolean value, have applications in modeling resource-constrained computation. We use weighted automata (finite automata with transition weights) to define several natural classes of quantitative languages over finite and infinite words; in particular, the real value of an infinite run is computed as the maximum, limsup, liminf, limit average, or discounted sum of the transition weights. We define the classical decision problems of automata theory (emptiness, universality, language inclusion, and language equivalence) in the quantitative setting and study their computational complexity. As the decidability of language inclusion remains open for some classes of weighted automata, we introduce a notion of quantitative simulation that is decidable and implies language inclusion. We also give a complete characterization of the expressive power of the various classes of weighted automata. In particular, we show that most classes of weighted automata cannot be determinized [CDH08].

21. Transactional memories (EPFL)

We introduce the notion of permissiveness in transactional memories (TM). Intuitively, a TM is permissive if it never aborts a transaction when it need not. More specifically, a TM is permissive with respect to a safety property p if the TM accepts every history that satisfies p. Permissiveness, like safety and liveness, can be used as a metric to compare TMs. We illustrate that it is impractical to achieve permissiveness deterministically, and then show how randomization can be used to achieve permissiveness efficiently. We introduce Adaptive Validation STM (AVSTM), which is probabilistically permissive with respect to opacity; that is, every opaque history is accepted by AVSTM with positive probability. Moreover, AVSTM guarantees lock freedom. Owing to its permissiveness, AVSTM outperforms other STMs by upto 40% in read dominated workloads in high contention scenarios. But, in low contention scenarios, the bookkeeping done by AVSTM to achieve permissiveness makes it, on average, 20-30% worse than existing STMs [GHS08].

22. Timed games (EPFL)

We consider concurrent two-player timed automaton games with omega-regular objectives specified as parity conditions. These games offer an appropriate model for the synthesis of real-time controllers. Earlier works on timed games focused on pure strategies for each player. We study, for the first time, the use of randomized strategies in such games. While pure (i.e.,

nonrandomized) strategies in timed games require infinite memory for winning even with respect to reachability objectives, we show that randomized strategies can win with finite memory with respect to all parity objectives. Also, the synthesized randomized real-time controllers are much simpler in structure than the corresponding pure controllers, and therefore easier to implement. For safety objectives we prove the existence of pure finite-memory winning strategies. Finally, while randomization helps in simplifying the strategies required for winning timed parity games, we prove that randomization does not help in winning at more states [CHS08].

23. Challenges in embedded systems design (EPFL)

We discuss two main challenges in embedded systems design: the challenge to build predictable systems, and the challenge to build robust systems. We suggest how predictability can be formalized as a form of determinism, and robustness, as a form of continuity [Hen08].

24. Open implication (EPFL)

We argue that the usual trace-based notions of implication and equivalence for linear temporal logics are too strong and should be complemented by the weaker notions of open implication and open equivalence. Although open implication is harder to compute, it can be used to advantage both in model checking and in synthesis. We study the difference between trace-based equivalence and open equivalence and describe an algorithm to compute open implication of Linear Temporal Logic formulas with an asymptotically optimal complexity. We also show how to compute open implication while avoiding Safra's construction. We have implemented an open-implication solver for Generalized Reactivity(1) specifications. In a case study, we show that open equivalence can be used to justify the use of an alternative specification that allows us to synthesize much smaller systems in far less time [GBJV08].

25. Reference architecture views (ESI)

In the Darwin project a diversity of initial views (from software, hardware to mechanical insights) were defined for the architecture of medical devices at Philips Healthcare. This is a result in the Quantitative modeling activity.

26. Modeling for analysis (ESI)

Several projects, a.o. Trader and Octopus, came up with new concepts and approaches for modeling embedded systems for the purpose of conducting analysis. This is a result of the Performance and Quantitative modeling activities.

27. Design and modeling for reliability of safety-critical embedded real-time systems (INRIA)

We have proposed a new framework for the (length,reliability) bicriteria static multiprocessor scheduling problem. Our first criterion remained the schedule's length, crucial to assess the system's real-time property. For our second criterion, we have considered the global system failure rate, seen as if the whole system were a single task scheduled onto a single processor, instead of the usual reliability, because it does not depend on the schedule length like the reliability does (because of its computation in the classical exponential distribution model). This provides a better control of the replication factor of each individual task of the dependency task graph given as a specification, with respect to the desired failure rate.

To solve this bicriteria optimization problem, we have taken the failure rate as a constraint, and we minimize the schedule length. We have thus been able to produce, for a given dependency task graph and multiprocessor architecture, a Pareto curve of non-dominated solutions, among which the user can choose the compromise that fits his/her requirements best. Compared to the other bicriteria (length,reliability) scheduling algorithms found in the literature, the algorithm we present here is the first able to improve significantly the reliability, by several orders of magnitude, making it suitable to safety critical systems.

28. Convertibility verification for component-based embedded systems (INRIA)
We have proposed a generalization of this convertibility verification problem, by using a new refinement called specification enforcing refinement (SER) between a protocol composition and a desired specification. The existence of such a refinement is shown to be a necessary and sufficient condition for the existence of suitable a converter. We also propose an approach to automatically synthesize a converter if a SER refinement relation exists. The proposed converter is capable of the usual disabling actions to remove undesirable paths in the protocol composition. In addition, the converter can perform forcing actions when disabling alone fails to find a converter to satisfy the desired specification. Forcing allows the generation of control inputs in one protocol that are not provided by the other protocol. Forcing induces state-based hiding, an operation not achievable using DES control theory.

29. Definition of a standalone Meta model for heterogeneous rich components (OFFIS)
The meta-model enables the blackbox-specification of components encapsulating the internal behavior by providing interface specifications based on a contract approach in terms of assumptions/promises containing functional and non-functional viewpoints. In addition, the meta-model also enables the graybox-specification of components by providing concepts to specify how a component is composed by subsystems. The semantics of the meta-model is provided in an automata-based form, and it is used as a common basis for analysis techniques. The meta-model has been elaborated in particular w.r.t. the safety viewpoint.

30. Definition of a UML/SysML Profile for the meta-model (OFFIS)
A UML profile was defined which extends the SysML Profile by a capability to specify heterogeneous rich components. The expressiveness of the profile corresponds to the standalone meta-model, that is, it enables the specification of heterogenous rich components by using industrial UML/SysML COTS-tools.

31. Stable helicopter platform (Salzburg + TU Timisoara + IBM Research + Stanford Uni. + Palo Alto Research Center (PARC))
The Salzburg helicopter platform serves as a testbed for implementing low- and high-level control functionality in the Exotask system. The system is extremely difficult to control and poses interesting challenges in terms of real-time constraints, power consumption, safety, and reliability. We have recently been able to conduct stable, computer-assisted flights with manual pilot input for navigation. The key challenge is to set up the correct combination of complex sensors, filters, controllers, and actuators. The platform is now ready for implementing higher-level control functionality in the Exotask system using additional sensors such as GPS and UWB localization systems, and distance lasers.

32. Compositional HTL semantics (Salzburg + Uni. Porto **+ EPFL)**
HTL is a hierarchical coordination language for distributed control systems. HTL semantics has originally been defined using a non-compositional, operational approach. The drawback of this

method is that methodological aspects such as the semantics of modular program modification and validation cannot be described. We have therefore taken a new, fully compositional approach of defining HTL semantics, which forms the foundation for exploring modelling 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 now defined separately from each other. Program correctness in terms of schedulability, absence of race conditions, and reliability can now be asserted in a modular fashion.

33. Runtime patching (Salzburg + Uni. Porto**)**
Higher-level control functionality such as collision avoidance and cooperative control require support of systematic program adaptation. We have proposed a methodology for patching HTL programs at runtime based on compositional HTL semantics. Runtime patching allows a large variety of program modifications, can be performed incrementally, and has a well-defined semantics unlike related approaches. Runtime patching will become the foundation of systematic program adaptation in the Exotask system.

34. Approximating Behaviors in Embedded Systems (PARADES, Uni. Trento)
Poor understanding and the lack of a precise definition of the abstraction and refinement maps used in a design flow are likely cause of major design errors and delays. Design flows are often providing little, if any, guarantee of satisfying a given set of constraints and specifications, without resorting to extensive simulation or tests on prototypes. However, in the face of growing complexity, this approach will have to yield to more rigorous methods. In addition, abstraction and refinement should be designed to preserve, whenever possible, the properties of the design that have already been established. This is essential to increase the value of early, high level models and to guarantee a speedier path to implementation.
We approached abstraction and refinement relationships in the form of *conservative approximations* from a formal standpoint. Conservative approximations are closely related to abstract interpretations, and preserve refinement verification from an abstract to a concrete model while avoiding the occurrence of false positive results. This property of an abstraction is useful because, presumably, refinement verification is more efficient at the abstract level than it is at the concrete. We showed how to derive models of computation and the corresponding abstraction and refinement maps starting from simple models of behavior. We focused in particular on models that include both continuous and discrete behaviors, and are therefore appropriate for the design of hybrid systems.

35. Design Space Exploration with Common Semantics Domain: the UMTS Case (PARADES, Uni. Trento, UC Berkeley**)**
To cope with the increasing complexity of electronic systems and time-to-market requirements, platform-based design (PBD) was proposed as a powerful design methodology. The core concepts in PBD are (1) the separation of concerns between functionality and architecture, which facilitates design reuse at all design levels, and (2) the successive refinement of the design by mapping functionality onto architecture. Optimal mapping optimizes a set of objective functions while satisfying constraints on the mapped design. Formalized design methods gain traction in the designer community when they facilitate automating the design process from specification to implementation, as witnessed by the RTL to layout ASIC flow. While logic synthesis and layout synthesis, which can be seen as special cases of optimized mapping, have been widely researched and many excellent algorithms have been made available, the mapping problem at the system level is typically solved in an ad-hoc and implicit manner based on designer experience. We developed a formal mapping procedure that enables the development of automatic tools. The mapping procedure is based on a two-stage process. First a common semantics domain between function and architecture models is determined

and an appropriate set of primitives is selected to represent the abstraction level. Since both architecture elements and function can be expressed in terms of the primitives of the common semantics domain, mapping is formulated and solved as an optimal covering problem where the function model is covered by a minimum cost set of architecture components. We demonstrate the use of the formal approach for the optimal mapping problems in two widely different application domains which feature different models of computationfor representation as well as different implementation platforms. This process is general in the sense that it can be applied at all levels of abstraction and for a variety of system level design problems. In our case studies, Metropolis (a design framework for platform-based design) was used to validate our approach. And the insights gained from these case studies motivated the development of Metro II, the next-generation of Metropolis.
http://chess.eecs.berkeley.edu/

36. Implementing Synchronous Specifications on Asynchronous Platforms (PARADES, INRIA, Scuola di Sant'Anna, Cadence Berkeley Labs, UC Berkeley**)**
Synchronous systems offer clean semantics and an easy verification path at the expense of often inefficient implementations. Capturing design specifications as synchronous models and then implementing the specifications in a less restrictive platform allows us to address a much larger design space. The key issue in this approach is maintaining semantic equivalence between the synchronous model and its implementation. We addressed this problem by showing how to map a synchronous model onto a loosely time-triggered architecture that is fairly straightforward to implement as it does not require global synchronization or blocking communication. We show how to maintain semantic equivalence between specification and implementation using an intermediate model (similar to a Kahn process network but with finite queues) that helps in defining the transformation. Performance of the semantic preserving implementation was analyzed for the general case and for a few special cases.

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

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

38. Multiprocessor scheduling (Uppsala)
In [GYGY08], new test conditions for schedulability checking of real-time tasks on multiprocessor platforms have been established. Simulation experiments demonstrate that the test conditions improve significantly existing test bounds for global non-preemptive multiprocessor scheduling.

39. A notion of expressivity for composition formalisms (Verimag):

Comparisons between different formalisms and models are often implemented by flattening their structure and reducing them to behaviorally equivalent models e.g., an automaton and a Turing machine. This leads to a notion of expressiveness which is not sufficient for component-based systems – where separation between behavior and coordination mechanisms is essential.

We propose a notion of glue expressiveness for component-based frameworks, characterizing their ability to coordinate components. Glue is a closed-under-composition set of operators, mapping tuples of behavior into behavior. Glue operators preserve behavioral equivalence. They only restrict the behavior of their arguments by performing memoryless coordination.

We propose an SOS-style definition of glues, where operators are characterized as sets of SOS-rules, specifying the transition relation of composite components from the transition relations of their constituents. We provide expressiveness results for the glues used in BIP and for process algebras such as CCS, CSP and SCCS. We show that for the expressiveness criteria considered, the glues used in these process calculi are less expressive than the general SOS glue. Furthermore, glue used in BIP has exactly the same strong expressiveness as any glue that can be defined with the SOS characterization [BS08]. This is an indication that the concepts of BIP are as general as one may need.

40. BIP for modelling architectures of autonomous robots (Verimag)

The AMAES project (http://www-verimag.imag.fr/~krichen/AMAES/) aims at more dependable software architectures for autonomous robots designed to perform high level tasks on their own, or with very limited external control. Autonomous robots are complex systems that require the interaction/cooperation of numerous heterogeneous software components. Nowadays, robots are getting closer to humans and as such are becoming critical systems which must meet safety properties including in particular logical, temporal and real-time constraints.

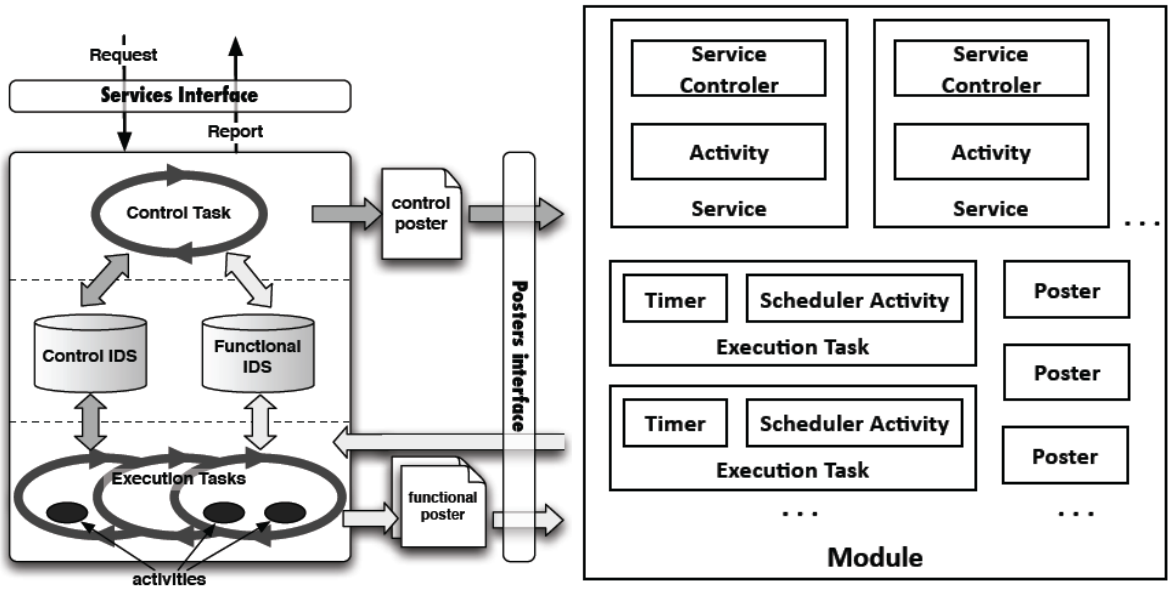

Figure 2.1-1: A module of the Genom architecture and its componentisation in BIP

In [BGL+08], [BIS08] we present an evolution of the LAAS Architecture for Autonomous System and its tool GenoM. We proposed a modelling paradigm based on BIP to enforce the separation between coordination and computation (execution of sequential code). We show how we are able to seamlessly integrate BIP into the preexisting methodology. We have componentized the functional level of a robot, synthesized an execution controller and

validated essential safety properties using the DL-finder tool (see validation deliverable). This approach has been integrated in the LAAS architecture and we have performed a number of experiments by simulation but also on a real robot (DALA).

41. A distributed semantics for BIP (Verimag): The operational semantics of the BIP language (see http://www-verimag.imag.fr/~async/bip.php for results on BIP) has originally been defined in such a way that interactions – defined by a data exchange between a set of components that is followed by local steps of individual components – are executed atomically. This means that the decision about the set of possible next steps is posed only in states in which all components are in a stable state. This semantics has been implemented previously in the BIP engine. In order to support distributed implementation, Verimag proposes two alternative semantics allowing a pipelined execution of atomic steps. In both semantics, additional intermediate partial states are introduced by cutting each transition of an individual component into two steps such that in the new intermediate state a component is not ready for any communication – meaning that in such a state the global state is only partly defined. The first semantics ignores the distinction between partially defined and global states and computes the set of enabled transitions in a state using the information on components in a defined state only. The second semantics implements interactions in the partial state model by using message passing primitives. The main result of the work consists of conditions for which the models are observationally equivalent. We study performance trade-offs and provide experimental results illustrating the application of the theory on a prototype implementation [BBBS08].

42. Modelling platform properties with AADL and BIP (Verimag)

AADL has been proposed as a standard for modelling platform architecture of embedded applications in the avionics domain. We propose methods for generating code and carrying out analysis of AADL specifications using BIP. We derive from extended AADL descriptions, component-based predictable implementations of mission-critical embedded systems associated with certification issues running on Lightweight-CCM, a real-time embedded component-oriented software platform. This year the existing AADL-BIP translation has quite evolved. As the BIP language has been extended to enforce component encapsulation, the structure of the BIP2 models obtained by the translation is now much closer to the original AADL model and avoids the previous explosion of the number of connector and priority definitions.

We have also further developed our state exploration engine and are now able to fully generate state diagram from AADL descriptions. The user interface of the BIP exploration engine has been considerably improved, and a debug feature has been added. The AADL2BIP translation and its state exploration have been experimented on an example related in a paper that will be presented at ACES-MB-08 [CRB+08].

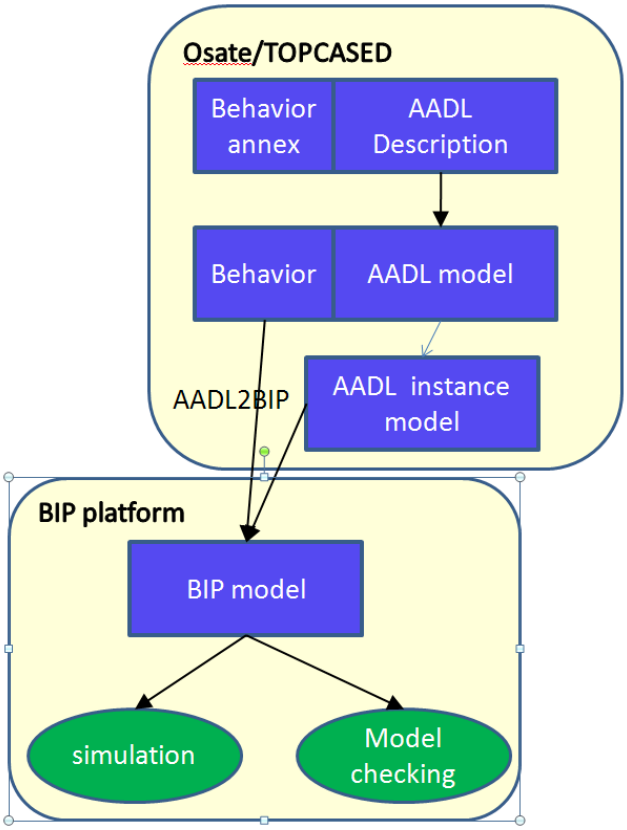

Figure 2.1-2 Validation of AADL specification in BIP and Lustre

The overall tool chain depicted in the figure above is integrated under Eclipse in the TopCased environment (http://topcased.gforge.enseeiht.fr/).

43. Quantitative modelling of embedded software (Verimag)

We have worked on two research directions concerning the modelling of quantitative properties of embedded software. The design and implementation of software-intensive embedded product lines requires dealing with a variety of constantly changing application- and system-dependent quantitative non-functional requirements and constraints that need to be verified throughout the development process. Moreover, because product lines are built upon a set of core services which are improved, customized, extended and integrated to come up with differentiated products, there is a need to resort to component-based approaches. However, many embedded applications (e.g., video compression) are most likely specified in a transformational data-oriented style. The componentization of such applications is therefore deferred to the implementation phase, where performance and platform constraints are taken into account. In [YAD+08] we presented a formally-grounded method to carry out this process. The approach consists in integrating (1) the component-based language and execution engine BIP, and (2) the coordination language and code-generation infrastructure FXML/Jahuel. This enables verification of quantitative properties using the associated BIP tool-suite.

AADL is an aerospace standard for model-driven design of complex real-time embedded systems. Currently, behavioral properties of AADL models can be specified inside the system description using AADL concepts or outside it using external textual languages, and verified using schedulability analysis or (Time Petri Net-based) model-checking tools. Our work [MOY+08] (1) proposes Visual Timed Scenarios (VTS) as a graphical property specification language for AADL, and (2) devises an effective translation from VTS to Time Petri Nets (TPN)

which enables model-checking properties expressed in VTS over AADL models using TPN-based tools integrated into AADL-compliant IDEs (e.g. TOPCASED).

44. Component Modeling (KTH + ForSyDe)

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 in a very general and theoretically sound way [SJ08,SJ07,HOH+07]. A performance analysis method and accompanying tools for reconfigurable systems [ZSJ08b] and for more general, heterogeneous multi-core systems [ZSJ08a] has been developed as well. Furthermore, formal re-timing transformations for design refinement have been developed and their correctness has been proved [RSJ08,RSJ07a,RSJ07b]. Finally, a method for refining abstract ForSyDe communication into NoC based architecture has been developed and demonstrated [LSSJ07].

45. Modeling of a middleware for self-configuring embedded systems (KTH)

As part of the DySCAS research project, a middleware architecture for the development of dynamically (self-) configurable systems is being developed. By dynamic configuration we refer to the ability of a system to during run-time change the number of components (software/hardware), their connections and the properties which characterize their execution and communication. To support the development of this system, and as a basis for analysis and future design-time configuration, systems models have been developed in UML, encompassing structure and behaviour. Experiments with mappings to Simulink behavioural models for simulation, and to formal models for model checking have been carried out, see Feng et al (2008-CDC) and Anthony et al (2008), further documentation and publication is under way.

46. Embedded systems modelling with the EAST-ADL (KTH)

As part of the ATESST and ATESST2 projects, KTH has been part in developing the EAST-ADL embedded systems modelling language. The basis for the language is a domain information model capturing entities, relations and properties. This model is then use as the basis for defining a UML profile, constituting the modelling language East-ADL. The scope of the modeling language is broad and encompasses functions down to software/hardware implementation components, requirements and environment models. The component modelling in the EAST-ADL has been enriched with error models, for describing component failure modes, how failures propate along nominal and abnormal architectural paths, and the sources of failures. The use of UML behaviour models, as a potential basis for native behaviour modelling in the EAST-ADL has been investigated. Two approaches for describing continuous-time systems in the UML have been investigated. It has been shown how UML activity diagrams can be used, and their mapping to Simulink models. Limitations in the current parametric diagrams have also been discovered. See references; Chen et al (2008), Sjöstedt et al (2008), Törner et al. (2008), Frey et al (2008), Lars-Olof Berntsson et al (2008).

47. Performance analysis - Quantitative Modeling (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 [JL08] and several case studies and architecture specific techniques. In the medical application domain ECG analysis has been studied thoroughly [ABP+07] and has resulted in a design methodology [APB+08] and performance analysis and design space exploration method

[ABJB08]. For on-chip communication networks a TDM based technique has been developed for guaranteeing minimum bandwidth and maximum latency services [LJ07,LJ08] 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 comlex memory controllers and analyzing performance of memory transactions [HvdWJB07]. 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 [SLJZ07,SLJ+07].

2.2 Individual Publications Resulting from these Achievements

CEA

[R08] Sébastien Revol. Profil UML pour TLM SystemC: Contribution à l'automatisation du flot de conception et vérification des System on Chip. PhD report, Université Joseph Fournier, Grenoble, France, Juin 2008.

[RTRGT08] S.Revol, S.Taha, A.Radermacher, S.Gerard, F.Terrier. Unifying HW analysis and SoC design flows by bridging two key standards: UML and IP-XACT. DIPES, Milan, Italie, Sept. 2008.

CISS

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

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

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

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

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

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

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

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

[BKO+08] Thomas Bøgholm, Henrik Kragh-Hansen, Petur Olsen, Bent Thomsen, Kim G. Larsen: Model-Based Schedulability Analysis of Safety Critical Hard Real-Time Java Programs. JTRES 2008: Proceedings of the 6th International Workshop on Java Technologies for Real-Time and Embedded Systems, p. 106—114, 2008.

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

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

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

EPFL

[GHS08] Rachid Guerraoui, Thomas A. Henzinger, and Vasu Singh. Permissiveness in transactional memories. Proceedings of the 22nd International Symposium on Distributed Computing (DISC), Lecture Notes in Computer Science 5218, Springer, 2008, pp. 305-319.

[DHJP08] Laurent Doyen, Thomas A. Henzinger, Barbara Jobstmann, and Tatjana Petrov. Interface theories with component reuse. Proceedings of the 8th Annual Conference on Embedded Software (EMSOFT), ACM Press, 2008, pp. 79-88.

[CDH08] Krishnendu Chatterjee, Laurent Doyen, and Thomas A. Henzinger. Quantitative languages. Proceedings of the 17th International Conference on Computer Science Logic (CSL), Lecture Notes in Computer Science 5213, Springer, 2008, pp. 385-400.

[CHS08] Krishnendu Chatterjee, Thomas A. Henzinger, and Vinayak S. Prabhu. Trading infinite memory for uniform randomness in timed games. Proceedings of the 11th International Workshop on Hybrid Systems: Computation and Control (HSCC), Lecture Notes in Computer Science 4981, Springer, 2008, pp. 87-100.

[Hen08] Thomas A. Henzinger. Two challenges in embedded systems design: Predictability and robustness. Philosophical Transactions of the Royal Society A 366:3727-3736, 2008.

ESI

[ACT08] L. Arts, M. Chmarra, T. Tomiyama, Modularization Method For Adaptable Products, ASME 2008 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference. 2008

[CAT08a] M. K. Chmarra, L. Arts, T. Tomiyama, Towards Adaptable Architecture, ASME 2008 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference. 2008

[CAT08b] M. K. Chmarra, L. Arts, T. Tomiyama, Towards Design-time and Runtime Adaptability, EDIProD' 2008 - Engineering Design in Integrated Product Development. 2008

[ET08] M.S. Erden, T. Tomiyama, Revisiting the Divide and Conquer Strategy to Deal with Complexity in Product Design, IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications. 2008

[BRR08] D.A. van Beek, M.A. Reniers, J.E. Rooda, R.R.H. Schiffelers, Concrete syntax and semantics of the compositional interchange format for hybrid systems, International Federation of Automatic Control. 2008

T.J. van Beek, T. Tomiyama, Requirements for Complex Systems Modeling, CIRP Design Conference. 2008

[BB08a] G.M. Bonnema, P.D. Borches, Design with Overview - how to survive in complex organizations, Proceedings of INCOSE. 2008

[BB08b] P.D. Borches, G.M. Bonnema, Living' Architecture Overviews - Supporting the Design of Complex Systems, CIRP Design Conference. 2008

[CAA08] T. B. Callo Arias, P. Avgeriou, P. America, Analyzing the Actual Execution of a Large Software-Intensive System for Determining Dependencies, Working Conference on Reverse Engineering (WCRE 2008)

[Clo08] M.B.G. Cloosterman, Control over Communication Networks: Modeling, Analysis, and Synthesis, PhD Thesis Eindhoven University of Technology. 2008

[CBA08]S. Ciraci, P. van den Broek, M. Aksit, Framework for Computer-Aided Evolution of Object-Oriented Design, IEEE Workshop on Quality Oriented Reuse of Software. 2008

[Mul08a] G. Muller, How reference architectures support the evolution of Product Families, CSER. 2008

[Mul08b] G. Muller, Right Sizing Reference Architectures; How to provide specific guidance with limited information, INCOSE Proceedings. 2008

[Mul08c] G. Muller, When and What to Standardize; An Architecture Perspective, INCOSE Proceedings. 2008

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

[GWD08] B. Graaf, S. Weber and A. van Deursen, Model-Driven Migration of Supervisory Machine Control Architectures Journal of Systems and Software 81(4):517-535. 2008

[Gul08] G. Gulesir, Evolvable Behavior Specifications Using Context-Sensitive Wildcards, PhD Thesis University of Twente. 2008

[Ham08] R. Hamberg, Tilt-tray Sorters modelled with UPPAAL, ESI Report Nr. 2008–2

[HH08] J. Hooman, T. Hendriks, Model-Based Run-Time Error Detection, LNCS Vol. 5002: 225-236, 2008.

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

[Hen08] T. Hendriks, The Impact of Independent Model Formation on Model-based Service, 7th WSEAS Int. Conf. on ARTIFICIAL INTELLIGENCE, KNOWLEDGE ENGINEERING and DATA BASES (AIKED'08), University of Cambridge, UK, Feb 20-22, 2008Interoperability

[Ign08] G. Igna, Towards Data Path Analysis Using Uppaal, Formal Methods 2008

[IKY08] G. Igna, V. Kannan, Y. Yang, T. Basten, M. Geilen, F. Vaandrager, M. Voorhoeve, S. de Smet, and L. Somers, Formal Modeling and Scheduling of Data Paths of Digital Document Printers, FORMATS. 2008

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

[MBP08] M. van Amstel, M. van den Brand, Z. Protic, T. Verhoeff, Transforming Process Algebra Models into UML State Machines: Bridging a Semantic Gap? ICMT2008 - International Conference on Model Transformation. 2008

[PVH08] T. Punter, J. Voeten, J. Huang, Quality in Model Driven Engineering, Chapter 2, in: J. Rech, C. Bunse (Eds), Model-Driven Software Development: Integrating Quality Assurance, Information Science Reference, 37-56, August 2008.

[ST08] H. Sozer, B. Tekinerdogan, Introducing Recovery Style for Modeling and Analyzing System Recovery, 7th Working IEEE/IFIP Conference on Software Architecture (WICSA). 2008

[TSA08] B. Tekinerdogan, H. Sozer, M. Aksit, Software Architecture Reliability Analysis using Failure Scenarios, Journal of Systems and Software. 2008

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

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

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

KTH

[ZSJ08a] Jun Zhu, Ingo Sander, and Axel Jantsch, "Energy efficient streaming applications with guaranteed throughput on MPSoCs", Proceedings of the International Conference on Embedded Software, October 2008.

[ZSJ08b] Jun Zhu, Ingo Sander, and Axel Jantsch, "Performance Analysis of Reconfiguration in Adaptive Real-Time Streaming Applications", Proceedings of the 6th Workshop on Embedded Systems for Real-Time Multimedia, October 2008.

[RSJ08] Tarvo Raudvere, Ingo Sander, and Axel Jantsch, "Application and Verification of Local Non-Semantic-Preserving Transformations in System Design", IEEE Tran sactions on Computer Aided Design of Integrated Circuits and Systems, vol. 27 , no. 6, pp. 1091-1103, 2008.

[SJ08] Ingo Sander and Axel Jantsch, "Modelling Adaptive Systems in ForSyDe", Electronic Notes in Theoretical Computer Science, vol. 200, no. 2, pp. 39-54, February 2008.

[SJ07] Ingo Sander and Axel Jantsch, "Modelling adaptive systems in ForSyDe", Proceedings of the First Workshop on Verification of Adaptive Systems (VerAS), pp. 39-54, Kaiserslauten, 2007.

[HOH+076] Andreas Herrholz, Frank Oppenheimer, P. A. Hartmann, Andreas Schallenberg, Wolfgang Nebel, Christoph Grimm, Markus Damm, J. Haase, Fernando Herrera, Eugenio Villar, Ingo Sander, Axel Jantsch, Anne-Marie Fouilliart, and Marcos Martinez, "The ANDRES Project: ANalysis and Design of run-time REconfigurable, heterogeneous Systems", Proceedings of the The International Conference on Field-Programmable Logic, Reconfigurable Computing, and Applications (FPL), August 2007.

[RSJ07a7] Tarvo Raudvere, Ingo Sander, and Axel Jantsch, "A Synchronization Algorithm for Local Temporal Refinements in Perfectly Synchronous Models with Nested Feedback Loops", Proceedings of the Great Lake Symposium on VLSI (GLSVLSI), 2007.

[RSJ07] Tarvo Raudvere, Ingo Sander, and Axel Jantsch, "Synchronization after design refinements with sensitive delay elements", Proceedings of the International Conference on HW/SW Codesign and System Synthesis, Salzburg, Austria, September 2007.

[LSSJ07] Zhonghai Lu, Jonas Sicking, Ingo Sander, and Axel Jantsch, "Using Synchronizers for Refining Synchronous Communication onto Hardware/Software Architectures", Proceedings of the 18th IEEE/IFIP International Workshop on Rapid System Prototyping, Porto Alegre, Brasil, May 2007.

[JL08] 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, 2008.

[ABP07] Iyad Al Khatib, Davide Bertozzi, Francesco Poletti, Luca Benini, Axel Jantsch , Mohamed Bechara, Hasan Khalifeh, Mazen Hajjar, Rustam Nabiev, and Sven Jons son, "Hardware/Software Architecture for Real-Time ECG Monitoring and Analysis Leveraging MPSoC Technology", Transactions on High-Performance Embedded Arc hitectures and Compilers (HiPEAC), vol. I, no. 1, pp. 239-258, LNCS 4050, 2007.

[APB08] Iyad Al Khatib, Francesco Poletti, Davide Bertozzi, Luca Benini, Mohamed Bech ara, Hasan Khalifeh, Axel Jantsch, and Rustam Nabiev, "A Multiprocessor System-on-Chip for Real-Time Biomedical Monitoring and Analysis: ECG Prototype Arc hitectural Design Space Exploration", ACM Transactions on Design Automation o f Embedded Systems, vol. 13, no. 2, April 2008.

[ABJP07] Iyad Al-Khatib, Davide Bertozzi, Axel Jantsch, and Luca Benini, "Performance Analysis and Design Space Exploration for High-End Biomedical Applications: C hallenges and Solutions", Proceedings of the International Conference on Hardware - Software Codesign and System Synthesis, September 2007.

[LJ07] Zhonghai Lu and Axel Jantsch, "Slot Allocation Using Logical Networks for TDM Virtual-Circuit Configuration for Network-on-Chip", International Conference on Computer Aided Design (ICCAD), November 2007.

[LJ08] Zhonghai Lu and Axel Jantsch, "TDM Virtual-Circuit Configuration for Network- on-Chip", IEEE Transactions on Very Large Scale Integration Systems, vol. 16, no. 8, August 2008.

[HvdWJB07] Tomas Henriksson, Pieter van der Wolf, Axel Jantsch, and Alistair Bruce, "Network Calculus Applied to Verification of Memory Access Performance in SoCs", Proceedings of the 5th IEEE Workshop on Embedded Systems for Real-Time Multimedia, October 2007.

[SLJZ07] Huimin She, Zhonghai Lu, Axel Jantsch, and Dian Zhou, "A Network-based System Architecture for Remote Medical Applications", Proceedings of the Asia-Pacific Advanced Network Meeting, 2007.

[SLJ+07] Huimin She, Zhonghai Lu, Axel Jantsch, Li-Rong Zheng, and Dian Zhou, “Traffic Splitting with Network Calculus for Mesh Sensor Networks", International Workshop on Wireless Ad Hoc, Mesh and Sensor Networks, December 2007.

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

INRIA

[GK08] A. Girault and H. Kalla. A Novel Bicriteria Scheduling Heuristics Providing a Guaranteed Global System Failure Rate. IEEE Trans. on Dependable Secure Computing. To appear. 2008.

OFFIS

[JM08] B. Josko, Q. Ma, A. Metzner. Designing Embedded Systems using Heterogeneous Rich Components. Proceedings of the INCOSE International Symposium, Utrecht, 2008.

PARADES

[San08] A.Sangiovanni-Vincentelli. Is a Unified Methodology for System-Level Design Possible? IEEE Design and Test of Computers, Special Issue on Design in the Late and Post-Silicon Eras, Vol. 25, N. 4, pp. 346-358, July-August 2008.

[BFM+08] L. Benvenuti, A. Ferrari, E. Mazzi and A. Sangiovanni-Vincentelli. Contract Based Design for Computation and Verification of a Closed-loop Hybrid System. Proceedings of Hybrid Systems: Computation and Control (HSCC'08), April, 2008.

[PCS08] C. Pinello, Luca P. Carloni and Alberto Sangiovanni-Vincentelli. Fault-Tolerant Distributed Deployment of Embedded Control Software. IEEE Transactions on CAD, Vol. 27, N. 5, pp. 906-919, May 2008.

[SFH+08] A. Speranzon, C. Fischione, K. H. Johansson and Alberto L. Sangiovanni-Vincentelli. A Distributed Minimum Variance Estimator for Wireless Sensor Networks. IEEE Journal on Selected Areas of Communications, VOl. 26, N. 4, pp. 609-622, May 2008.

Salzburg

[ABIKRRT08] J. Auerbach, D.F. Bacon, D. Iercan, C.M. Kirsch, V.T. Rajan, H. Roeck, R.

Trummer. Low-Latency Time-portable Real-time Programming with Exotasks. To appear in ACM Transactions on Embedded Computing Systems (TECS), 2008.

[CKRT08] S.S. Craciunas, C.M. Kirsch, H. Roeck, and R. Trummer. The JAviator: A High-Payload Quadrotor UAV with High-Level Programming Capabilities. Proc. AIAA Guidance, Navigation and Control Conference and Exhibit (GNC), 2008.

[KLM08] C.M. Kirsch, L. Lopes, and E.R.B. Marques. Semantics-Preserving and Incremental Runtime Patching of Real-Time Programs. Proc. Workshop on Adaptive and Reconfigurable Embedded Systems (APRES), 2008.

Verimag

[BGL+08] Ananda Basu, Matthieu Gallien, Charles Lesire, Thanh-Hung Nguyen, Saddek Bensalem, Felix Ingrand and Joseph Sifakis. Incremental Component-Based Construction and Verfication of a Robotic System. ECAI 2008 The 18th European Conference on Artificial Intelligence, Patras, Greece, July 21 - 25, 2008.

[BBS+08] Saddek Bensalem, Marius Bozga, Joseph Sifakis, Thanh-Hung Nguyen. "Compositional Verification for Component-Based Systems and Application". ATVA 2008: 64-79

[BBBS08] A. Basu, P. Bidinger, M. Bozga, J. Sifakis. Distributed Semantics and Implementation for Systems with Interaction and Priority. In FORTE'08

[BS08a] Simon Bliudze and Joseph Sifakis. Causal semantics for the algebra of connectors. Technical report, Verimag, 2007. To appear in *Proc. Software Technologies Concertation on Formal Methods for Components and Objects* (FMCO 2007), 2008.

[BS08b] Simon Bliudze and Joseph Sifakis, A Notion of Glue Expressiveness for Component-Based Systems. In *Proc. of the 19th International Conference on Concurrency Theory* (CONCUR'08), LNCS 5201, 508–522, Springer, 2008.

[BIS08] Saddek Bensalem, Felix Ingrand and Joseph Sifakis. Autonomous Robot Software Design Challenge 6th IARP/IEEE-RAS/EURON, Joint International Workshop on Technical Challenge for Dependable Robots in Human Environments, Pasadena, USA, May 17-18, 2008.

[CRB+08] M.Y. Chkouri, A. Robert, M. Bozga, and J. Sifakis. Translating AADL into BIP: Application to the Verification of Real-time Systems. 1st Workshop on Model Based Architecting and Construction of Embedded Systems, ACES-MB at Models 2008

[Gra08] Susanne Graf. Omega -- Correct development of Real Time Embedded Systems. In SoSyM, int. Journal on Software & Systems Modelling vol. 7 (2) 2008

[MOY+08] D. Monteverde, A. Olivero, S. Yovine, V. Braberman. VTS-based Specification and Verification of Behavioral Properties of AADL Models. In: Model Based Architecting and Construction of Embedded Systems (ACES-MB 2008), Toulouse, France, September 29, 2008

[YAD+08] S. Yovine, I. Assayad, F.-X. Defaut, M. Zanconi, A. Basu. A formal approach to derivation of concurrent implementations in software product lines. Process Algebra for Parallel and Distributed Processing, M. Alexander & W. Gardner, eds., Chapman and Hall/CRC Press, Taylor and Francis Group LLC, December 2008.

2.3 Interaction and Building Excellence between Partners

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.

CEA + Verimag: co-organizing workshops related to model-based development of real-time and embedded systems (see below the description of the ACESMB 2008 workshop).

EPFL + INRIA are actively collaborating for developping a rich interface theory for component-based design, for both asynchronous and synchronous communication. INRIA (Prof. A. Benveniste) visited EPFL on Feb 28th-29th, and EPFL (Dr. L. Doyen and Dr. B. Jobstmann) visited INRIA on Oct 27th.

EPFL + Trento are working together in the area of heterogeneous modelling, with particular focus on the combination of models of computation that employ different communication semantics. A joint meeting was held in Trento on Oct 14-16th 2008.

Salzburg + TU Timisoara + IBM Research + Stanford Uni. + Palo Alto Research Center (PARC) significantly improved flight control performance of the Salzburg helicopter platform, which is now fit for more advanced Exotask-based experiments.

Salzburg + Uni. Porto + EPFL defined a fully compositional semantics of HTL as foundation for extensions of the Exotask system including modular reliability modeling.

Salzburg + Uni. Porto described a systematic methodology for patching HTL programs at runtime, which is instrumental to supporting higher-level control functionality in the Exotask system.

PARADES + Uni. Trento developed heterogeneous modelling techniques using conservative approximations to guarantee system properties.

PARADES + Uni. Trento + UC Berkeley pursued design-space exploration with quantitative comparisons; automatic mappings of functionality to implementations; and multi-processing architecture modelling using common semantic domains.

PARADES + UC Berkeley + Cadence Berkeley Labs + INRIA + Scuola di Sant'Anna worked on automatic mapping of functional requirements on distributed platforms characterized by heterogeneous components and hierarchical communication infrastructures.

PARADES + EPFL + UC Berkeley worked on reliability in the context of distributed systems.

Uppsala + ETH Zurich collaborated on modular performance analysis. Jointly, we have established a fixed point theorem on the existence of fixed points for component networks containing feedback cycles.

Uppsala + North Eastern Uni. China initiated a collaboration on multiprocessor scheduling.

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** are collaborating intensely in the SPEEDS project where for developing a modelling framework, a design methodology and system level validation techniques.
- In the newly started 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 + EPFL + 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 which was offered from the beginning in original de Alfaro-Henzinger framework. We aim at offering also the possibility to associate multiple interfaces to a component, via conjunction. Also, we want to support Assume/Guarantee reasoning in a way compliant with engineering practice, with the help of *residuation theory*. A joint paper is in preparation.

- Other projects with an analogous role include the still ongoing OpenEmBeDD and the now terminated Persiform projects.

Alberto Sangiovanni Vincentelli has visited VERIMAG. INRIA and VERIMAG researchers spent significant amount of time visiting Rome to carry out research work in the area of methodologies and tools for embedded system design. Alberto Ferrari has visited Grenoble and other locations to maintain connectivity with the rest of the research community.

Dr. Pierre America participated and provided a presentation during the ArtistDesign workshop Intercluster activity: Integration Driven by Industrial Applications. Title of his presentation was Embedded Systems in Healthcare.

Dr. Ir. Twan Basten is guest editor for special issue of ACM Transactions in Embedded Computing Systems (TECS), link at http://www.es.ele.tue.nl/~tbasten/:. This special issue was initiated during the 2nd Artist Workshop on Models of Computation and Communication, held in Eindhoven, July 3-4, 2008. However, submission for the special issue is open for everyone and the upcoming period

Dr. Ir. Twan Basten participated in the ArtistDesign WFCD 2008 workshop, held on 19th of October during the Embedded Systems Week.

Dr. Michael Borth participated and provided a presentation during the ArtistDesign Workshop Intercluster activity: Integration Driven by Industrial Applications, 13-14 November, Rome. His presentation was titled: Future Car Platform Development.

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

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

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

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

2.4 Joint Publications Resulting from these Achievements

[TPB+08] S. Tripakis, C. Pinello, A. Benveniste, Alberto Sangiovanni-Vincentelli, P. Caspi and M. Di Natale. Implementing Synchronous Models on Loosely Time Triggered Architectures. IEEE Transactions on COMPUTERS, Vol. 57, N. 10, pp. 1300-1314, October 2008.

[PCS08] A. Pinto, L. Carloni and A. Sangiovanni Vincentelli. COSI: A Framework for the Design of Interconnection Networks. IEEE Design and Test of Computers, vol. 25, n. 5, Sept-Oct. 2008, pp. 402-415.

[PS08] R. Passerone and A. Sangiovanni-Vincentelli. Approximating Behaviors in Embedded System Design. In Concurrency, Graphs and Models, Pierpaolo Degano, Rocco De Nicola and Jose' Meseguer (editors), Lecture Notes in Computer Sciences, vol. 5065, pp. 721--742, Springer-Verlag, Berlin, Heidelberg, 2008.

[BCD+07] Albert Benveniste, Paul Caspi, Marco Di Natale, Claudio Pinello, Alberto Sangiovanni-Vincentelli and Stavros Tripakis. Loosely Time-Triggered Architectures based on Communication-by-Sampling MoCC and Properties. In Proceedings of the Embedded Systems Software Conference (EMSOFT'07), Salzburg, Austria, October, 2007.

[GHI+07] Arkadeb Ghosal, Thomas A. Henzinger, Daniel Iercan, Christoph Kirsch and Alberto Sangiovanni-Vincentelli. Separate Compilation of Hierarchical Real-Time Programs into Linear-Bounded Embedded Machine Code. In Proceedings of Automatic Program Generation for Embedded Systems (APGES), Salzburg, Austria, October, 2007.

[CGI+08] Krishnendu Chatterjee, Arkadeb Ghosal, Daniel Iercan, Christoph Kirsch, Thomas A. Henzinger, Claudio Pinello and Alberto Sangiovanni-Vincentelli. Logical Reliability of Interacting Real-time Tasks. In Proceedings of Design, Automation and Test in Europe (DATE'08), Munich, Germany, March, 2008.

[PDF+08] A. Pinto, M. D'Angelo, C. Fischione, E. Scholte, A. Sangiovanni-Vincentelli. Synthesis of Embedded Networks for Building Automation and Control. Proc. of American Control Conference (ACC 08), Seattle, Washington, June 2008.

[BBC+08] L. Benvenuti, D. Bresolin, A. Casagrande, P. Collins, A. Ferrari, E. Mazzi, A. Sangiovanni-Vincentelli and T. Villa. Reachability Computation for Hybrid Systems with Ariadne. In Proceedings of the 17th IFAC World Congress (IFAC 2008), Seoul, South Korea, July, 2008.

[GYGY08] Nan Guan, Wang Yi, Zonghua Gu and Ge Yu. New Schedulability Test Conditions for Non-Preemptive Scheduling on Multiprocessor Platforms. Proc. of 29th IEEE Real-Time Systems Symposium, Barcelona.

[JPTY08] Bengt Jonsson, Simon Perathoner, Lothar Thiele, and Wang Yi. Cyclic dependencies in modular performance analysis. Proc. of the 8th International Conference on Embedded Software, Atlanta, USA, 2008.

[PPS08] M. Poulhiès, J. Pulou and J. Sifakis, “BUZZ: analyzable embedded component-based software", PROGRESS COMES'08 Workshop, 16-17 Juin 2008, SigTuna Sweden Mälardalen University.

[GBJV08] K. Greimel and R. Bloem and B. Jobstmann and M. Vardi. Open Implication. Proceedings of International Colloquium on Automata, Languages and Programming (ICALP'08), Lecture Notes in Computer Science 5126, Springer, pp. 361--372.

[CDL+07] Franck Cassez, Alexandre David, Kim Guldstrand Larsen, Didier Lime, Jean-François Raskin: Timed Control with Observation Based and Stuttering Invariant Strategies. ATVA 2007: 192-206.

[BLM08] Patricia Bouyer, Kim Guldstrand Larsen, Nicolas Markey: Model Checking One-clock Priced Timed Automata. Logical Methods in Computer Science 4(2:9), 2008.

[BFL+08] Patricia Bouyer, Ulrich Fahrenberg, Kim Guldstrand Larsen, Nicolas Markey, Jirí Srba: Infinite Runs in Weighted Timed Automata with Energy Constraints. FORMATS 2008: 33-47.

[BBL08] Patricia Bouyer, Ed Brinksma, Kim Guldstrand Larsen: Optimal infinite scheduling for multi-priced timed automata. Formal Methods in System Design 32(1): 3-23 (2008).

[CMMSS08] O. Constant, Q. Ma, L. Morel, M. Skipper, C. Sofronis. SPEEDS L-1 Meta-model. SPEEDS deliverable D2.1.2, May 2008.

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

[M+08] C. Mrugalla *et al.*: SPEEDS Meta-model – Profile Definition. SPEEDS deliverable D2.1.4, May 2008.

[CJL+08] DeJiu Chen, Rolf Johansson, Henrik Lönn, Yiannis Papadopoulos, Anders Sandberg, Fredrik Törner, Martin Törngren (2008 – Safecomp). Modelling Support for Design of Safety-Critical Automotive Embedded Systems. SAFECOMP 2008: The 27th International Conference on Computer Safety, Reliability and Security. 22-25 September 2008, Newcastle upon Tyne, UK.

[AWC+08] Richard Anthony, Paul Ward, DeJiu Chen, James Hawthorne, Mariusz Pelc, Achim Rettberg, Martin Törngren (2008). A Middleware Approach to Dynamically Configurable Automotive Embedded Systems. The First Annual International Symposium on Vehicular Computing Systems. July 22-24, 2008 - Trinity College Dublin, Ireland.

[SST+08] Carl-Johan Sjöstedt, Jianlin Shi, Martin Törngren, David Servat, DeJiu Chen, Viktor Ahlsten, Henrik Lönn. Mapping Simulink to UML in the Design of Embedded Systems: Investigating Scenarios and Structural and Behavioral Mapping. Invited paper. OMER 4 Post Workshop Proceedings, 2008.

[TCJ08] Fredrik Törner, D.J. Chen, Rolf Johansson, Henrik Lönn, Martin Törngren. Supporting an Automotive Safety Case through Systematic Model Based Development - the EAST-ADL2 Approach. SAE World Congress, 2008. SAE paper number 2008-01-0127.

[FJL+08] Patrik Frey, Rolf Johansson, Henrik Lönn, Philippe Cuenot, Carl-Johan Sjöstedt, Martin Törngren. Engineering Support for Automotive Embedded Systems -Beyond AUTOSAR. Fisita 2008 – World Automotive Congress. 14-19 Sept. Munich, Germany.

[BBD+08] Lars-Olof Berntsson, Hans Blom, DeJiu Chen, Philippe Cuenot, Jörg Donandt, Ulrich Eklund, Ulrich Freund, Patrick Frey, Sebastien Gerard, Pontus Jansson, Rolf Johansson, Henrik Lönn, Mark-Oliver Reiser, Dennis Selin, David Servat, Carl-Johan Sjöstedt, Patrick Tessier, Ramin Tavakoli, Fredrik Törner, Martin Törngren, Matthias Weber. EAST ADL 2.0 Specification. Advancing Traffic Efficiency and Safety through Software Technology (ATESST). EC P6 Contract number: 2004 – 026976. 2008 http://www.atesst.org

2.5 Keynotes, Workshops, Tutorials

Keynote: "Embedded Systems in Healthcare"
Pierre America - ArtistDesign workshop Intercluster activity: Integration Driven by Industrial Applications, Rome, 13-14 November 2008.
http://www.artist-embedded.org/artist/Agenda,1532.html

Keynote: "*Future Car Platform Development*"
Dr. Michael Borth, ArtistDesign Workshop Intercluster activity: Integration Driven by Industrial Applications, Rome, 13-14 November 2008.

Keynote: "Quantitative Testing Theory".
Ed Brinksma, Invited Talk. ARTIST2 Summer School Autrans (near Grenoble), France. September 8-12, 2008.
http://www.artist-embedded.org/artist/ARTIST2-Summer-School-2008.html

Keynote: "Designing Predictable and Robust Systems"
Thomas A. Henzinger - Invited lecture, Third International Workshop on Foundations of Component-based Design (WFCD), Atlanta, Georgia, USA, October 2008.
http://www.artist-embedded.org/artist/Objectives-and-Scope,1346.html

Keynote: "Grand Challenges for Real-Time Systems"
Thomas A. Henzinger - 20th Euromicro Conference on Real-Time Systems (ECRTS), Prague, Czech Republic, July 2008. http://dce.felk.cvut.cz/ecrts08/

Keynote: "Challenges in Embedded Systems Design: Predictability and Robustness"
Thomas A. Henzinger - Invited lecture, Royal Society Meeting: From Computers to Ubiquitous Computing, London, United Kingdom, March 2008.
http://royalsociety.org/event.asp?id=6065&month=3,2008

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

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

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

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

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

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

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

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

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

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

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

Keynote: "Verification, optimization and synthesis for timed systems: from theory to tools"
Kim G. Larsen.. Invited talk given at the receipt of Dr Honoris Causa from LSV, ENS Cachan. Cachan, France. November 26, 2007.

Keynote:
Joseph Sifakis - 45th Design automation Conference, Anaheim, June 2008
http://www.dac.com/45th/PDFs/45thAdvPrgPoster.pdf

Keynote: "Embedded Systems Challenges and Research Directions"
Joseph Sifakis - Onassis Foundation, The 2008 Lectures in Computer Science:Embedded Systems: Theory and Applications, July 2008, Heraklion Greece
http://www.forth.gr/onassis/lectures/2008-07-21/programme.html

Turing Lecture*:*
Joseph Sifakis - Embedded Systems Week, Atlanta, 20 October 2008
http://www.esweek.org/

Workshop : UML & AADL 2008
13th IEEE International Conference on Engineering of Complex Computer Systems
Belfast, Northern Ireland - April 2nd, 2008
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. This workshop seeked contribution from researchers and practitioners interested in all aspects of the representation, analysis, and implementation of DRE system behaviour and/or architecture models.
http://www.artist-embedded.org/artist/Topics,1199.html

Workshop : ACESMB 2008, 1st Int. Workshop on Model Based Architecting and Construction of Embedded Systems
ACM/IEEE 11th Int. Conf. on Model Driven Engineering Languages and Systems
Toulouse, France - September 29th, 2008
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. This workshop seeked contribution from researchers and practitioners interested in all aspects of the representation, analysis, and implementation of DRE system behaviour

and/or architecture models.
http://www.artist-embedded.org/artist/ACES-MB-08.html

Workshop : RTSS'08 track on Design and Verification of Embedded Real-Time Systems Real-Time Systems Symposium
Barcelona, Spain- November 30th - December 3rd, 2008.

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

Workshop SLA++P 2008: Model-driven High-level Programming of Embedded Systems European Joint Conference on Theory and Practice of Software ETAPS 2008
Budapest, Hungary – April 5th, 2008

SLA++P is a workshop dedicated to synchronous languages and the model-driven high-level programming of reactive and embedded systems. Firmly grounded in clean mathematical semantics, synchronous languages are receiving increasing attention in industry ever since they emerged in the 80s. Lustre, Esterel, Signal are now widely and successfully used to program real-time and safety critical applications, from nuclear power plant management layer to Airbus air flight control systems. At the same time, model-based programming is making its way in other fields of software engineering, too, often involving cycle-based synchronous paradigms. The purpose of the SLA++P workshop is to bring together researchers and practitioners who work in the field of languages and tools for the model-driven development of embedded applications both in hardware and software. The workshop is not limited to synchronous approaches but open to other engineering design approaches with strong semantical foundations providing a way to go from a high-level description to provable executable code.

http://www.artist-embedded.org/artist/SLA-P-2008,1231.html

Workshop: 1st International Workshop on Model Based Architecting and Construction of Embedded Systems
Toulouse -- September 29th, 2008
This ARTIST workshop is held in conjunction with MODELS 2008 as a follow-up workshop of the SVERTS and MARTE workshops organised in previous years, the objective of this workshop is to bring together researchers and practitioners interested in model-based software engineering for real-time embedded systems. We are seeking contributions relating to this subject at different levels, from modelling languages and semantics to concrete application experiments, from model analysis techniques to model-based implementation and deployment. Given the criticality of the application domain, we particularly focus on model-based approaches yielding efficient and provably correct designs. Concerning models and languages, we welcome contributions presenting novel modelling approaches as well as contributions evaluating existing ones. The organisers of this workshop are partners from the ASSERT and SPICES project; the ARTIST partners are CEA and Verimag.

http://www.artist-embedded.org/artist/ACES-MB-08.html

Tutorial: Contract-Based System Design - The SPEEDS Approach -- INCOSE 2008
Utrecht, The Netherlands – June 16, 2008
The aim of this half day tutorial was to disseminate the results of the SPEEDS project towards the community of the potential users of the developed technology. The tutorial focused on the contracts based development methodology being worked-out within the project. It aimed specifically at iterative development as opposed to the traditional waterfall requirement flow down. At the centre of the methodology is the definition of a rich component model which allows the capture of functional and non functional system properties in the form of contracts.
http://www.incose.org/symp2008/

Tutorial: Contract Based System Design - The SPEEDS Approach
M. Winokur, S. Graf, B. Josko. INCOSE 2008, Utrecht, The Netherlands, June 2008.

3. Milestones, and Future Evolution

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

Within each sub-activity, the partners will continue to develop and extend the results obtained in Year 1. 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 summary of the problems that will be addressed in Year 2.

Sub-activity A (*Component Modeling)*

CEA will refine and experiment its component-based design pattern for supporting MoCC as defined in the MARTE specification, and especially its High-Level Application Modelling sub-profile.

CISS will extend the on-line testing technique of UPPAAL Tron to hybrid systems. Refinement checking based on conformance testing.

EPFL will study the connection between interface-based design and modal automata. We are going to compare the expressive power of classical interface and modal automata, and investigate the use of modal automata as an alternative language for compositional design. Both synchronous and asynchronous communication will be studied.

INRIA will work on the design and programming of a predictable embedded architecture. Computing the worst-case execution time of a program running on a modern embedded processor is extremely difficult because of the intrinsic features of these processors: multiple level caches, pipelines, and so on. The problem is that many embedded applications are safety critical ones where time predictability is an essential feature in order to validate them.

KTH in collaboration Volvo and CEA will further develop the East-ADL modelling language and ontology for embedded systems. Relations and transformations to external tools such as Simulink will be developed focusing on behaviour modelling. To successfully use model-based development, there is a need for methods and guidelines. Existing methodologies will be surveyed during 2009.

OFFIS will update and extend the HRC meta-model over the next 12 months based on the feedback from the pilot projects in SPEEDS. Also, the HRC-based specification approach with contracts will be extended to increase compatibility between different development methods. Target for the next year are EAST-ADL and adaptations to the use for the AUTOSAR platform.

Salzburg intends to work on integrating the results obtained in Year 1 into a flight control system that includes higher-level control aspects such as non-trivial navigation. The purpose of this work is to demonstrate modeling capabilities of the HTL language and to explore further enhancements. We also plan to advance more conceptual work on the HTL semantics and runtime patching. In particular, we are interested in studying semantical and complexity-theoretical aspects of runtime patching more formally.

Sub-activity B (Resource Modelling)

CEA will improve the integration of this framework for simulating both software and hardware platforms based on MARTE within the open-source tool Papyrus.

CISS will continue working on time, probabilities and cost: we will consider extensions of timed automata with both probabilities as well as cost and consider probabilistic reachability

problems involving both time and cost-bounds. For controller synthesis problems, we will work on timed games with partial observability and with dynamic computation of the "cheapest" observations that will ensure controllability.

EPFL has built a verification technique for various transactional memory implementations that exist in the literature. Currently, we specifically look at whole-transactional programs. We plan to extend our work to a more general scenario, where transactions also interact with non-transactional pieces of code.

Sub-activity C (Quantitative Modeling)

CEA will improve the first transformation of models defined to bridge the MARTE's High-Level Application Modelling sub-profile and the MARTE's Schedulability Analysis Modelling sub-profile.

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

EPFL will work on extensions of the results for quantitative generalizations of classical languages. Several questions will be investigated: closure properties, models of computation beyond nondeterminsitic automata (e.g., alternating and probabilistic automata), decision problems (such as universality), sufficient condition for a cut-point language to be regular, expressive power of subclasses of quantitative languages.

3.2 Current and Future Milestones

- A MARTE-based framework for MARTE MoCC Support. *CEA has defined a first design pattern for enabling the modelling with UML2 extended with MARTE different MoCC as defined in the MARTE specification.*
- A MARTE-based framework for embedded system simulation. *CEA has implemented within Papyrus the hardware resource modelling sub-profile of the MARTE specification and defined a transformation of model generating the required configuration files for building a simics-like model of the modelled hardware platform s and so be able to simulate this latter.*
- A Model-based framework for schedulability analysis. *Within this first year, CEA has implemented a first transformation of model enabling to go from a model using the High-Level Application Modelling sub-profile of MARTE towards a model dedicated to perform schedulability analysis.*
- Design and modeling for reliability of safety-critical embedded real-time systems. **We plan to extend our bicriteria (length,reliability) scheduling heuristics with new features to take into account temporal replication and k-out-of-n type replication.**
- Convertibility verification for component-based embedded systems. **We plan to extend our specification enforcing refinement based method with new features to cope with data inconsistencies between the protocols.**
- Design and programming of a predictable embedded architecture. **We plan to propose a predictable architecture based on the StarPro reactive processor. To propose an extension of the C programming language with timing constructs, to be compiled onto the aforementioned architecture.**

- VERIMAG *has, as promised, started the investigation of relations between sub-classes of component-based systems and transformations relating these classes (e.g. untimed and timed systems, event triggered and data triggered, synchronous and asynchronous)*. **Results will be presented at the end of the next year. VERIMAG will also investigate code generation techniques for BIP models taking into account user requirements and the characteristics of the target platform. We will study code generation techniques for multi-thread and distributed implementation of specific classes of systems, in particular for timed systems (collaboration with EPFL and Salzburg on Giotto).**
- Quantitative generalizations of classical languages. *Definition of the framework, and study of the expressive power and decision problems*. **Closure properties of quantitative languages. Extension of the framework to handle alternating automata, comparison of the expressive power of alternating and nondeterministic automata for quantitative languages.**
- Rich interface theory. *Interface theory for component reuse, with synchronous communication*. **Modal automata as a more powerful model for interface-based design. Synchronous and asynchronous models of communication.**
- Transactional memory. *We have built specifications for correctness in transactional memories. Our first basic scheme checked correctness at a programming level abstraction: we assumed that read and write commands issued by a programmer are executed atomically. In our second step, we verified transactional memories at a hardware level of atomicity: we assume only what is guaranteed by the hardware. Our second scheme goes beyond verification - it allows a verifier to introduce memory barriers, as required, in the transactional memory in order to make the transactional memory correct*. **Our immediate milestone is to formalize correctness of transactional memories in a general framework, where transactions interact with non-transactional code. Then, we shall extend our verification scheme to this framework. This shall involve handling issues like language memory models and the privatization problem.**
- **A method based on heterogenous rich components broadly applicable in concrete development scenarios based on languages like SYSML or EAST-ADL and realizable with COTS development tools. Date: October 2009.**

3.3 Main Funding

- **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
- **COMBEST (funded by European Union IST STREP)**
  COMponent-Based Embedded Systems design Techniques
  http://www.combest.eu
- **Concurrent Programming with Threading by Appointment**
  Austrian Science Fund (FWF), Grant P18913-N15 (One postdoc and two PhD students).
- **Condor project**
  Partially supported by the Dutch Ministry of Economic Affairs under the BSIK program.
- **DaNES - Danish Network of Embedded Systems**
  DaNES. Danish national project sponsored by the Danish Advanced Technology Foundation.

- **Darwin project.**
  Partially supported by the Dutch Ministry of Economic Affairs under the BSIK program.
- **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**
  Partially supported by the Dutch Ministry of Economic Affairs under the BSIK program.
- **GASICS**
  European Project sponsored by European Science Foundation (ESF).
- **Genesys**
  Project under the 7th Framework Programme of the European Committee.
- **The JAviator Project, IBM Faculty Award 2007 (Helicopter Platform).**
- **MoDES**
  Danish national project sponsored by the Strategic Research Council.
- **MT-LAB**
  Danish national project sponsored by Villum-Kahn Rasmussen Foundation.
- **Multiform**
  Project under the 7th Framework Programme of the European Committee.
- **Octopus project**
  Partially supported by the Dutch Ministry of Economic Affairs under the BSIK program.
- **Quasimodo.**
  Project under the 7th Framework Programme of the European Committee. http://www.quasimodo.aau.dk/
- **REVE project.**
  Safe reuse of embedded components in heterogeneous environments.
  http://www.ara-reve.org
- **SNSF** (Swiss National Science Foundation).
- **SPEEDS IP project**
  with the ARTIST partners INRIA, OFFIS, PARADES and VERIMAG and affiliated industrial partners EADS and IAI. http://www.speeds.eu.com/

4. Internal Reviewers for this Deliverable

Thierry Jeron (INRIA Rennes, France)

Martin Torngern (KTH Stockholm, sweden)