IST-004527 ARTIST2
Network of Excellence
on Embedded Systems Design

Activity Progress Report for Year 4

JPIA-Platform / JPRA-Cluster Integration / JPRA-NoE Integration

Platform for Component Modelling and Verification

Clusters:

Real Time Components

Activity Leader:

Susanne Graf (Verimag)
http:www-verimag.imag.fr/~graf/

Policy Objective (abstract)

Integrate the relevant European research on tools for modelling and analysis of component-based real-time systems by building tool supported semantic based platform for standard modelling notations that are relevant for the design of embedded systems.

These platforms will support transformations from modelling standards to semantic kernel languages to leverage associated powerful analysis tools, in particular some of those from the "Testing and Verification" cluster.

Table of Figures

Table of Contents

1. Overview of the Activity

1.1 ARTIST Participants and Roles

Susanne Graf (VERIMAG)

Contributions of her team: Semantic level formalisms including general component composition, formal verification methods and tools, in particular the IF/BIP validation platform for real-time and embedded systems

Saddek Bensalem (Verimag)

Contributions of his team: efficient methods for deadlock detection, and architecture paradigms for autonomous robots

Michael Perin (Verimag)

Contributions of his team: security of smartcard applications

Laurent Mounier (Verimag)

Contributions of his team: test and test case generation, simulation models for sensor networks

Olivier Constant (Verimag)

Contributions: modelling for performance evaluation and model transformations

Sébastien Gérard (CEA LIST)

Activity Leader for "Development of UML for Real-time Embedded Systems" (Cluster Integration)

Contributions of his team: *Model driven engineering of real time systems, UML standard for embedded systems*

Francois Terrier (CEA LIST)

Contributions of his team: *Component based modeling and analysis of embedded systems*

Jacques Pulou (France Telecom R&D)

Contributions of his team: connection of performance analysis tools to UML case tools and the Fractal/Think platform

Thierry Coupaye (France Telecom R&D)

Contributions of his team: his team has developed the architecture description language Fractal and its implementation Think. Contribution to the platform in the collaboration with Verimag on the integration of validation tools through the translation from THINK to BIP

Noël Plouzeau (INRIA)

Contributions of his team: Model transformations and aspect orientation, tools

Bernhard Josko (OFFIS,)

Contributions of his team: OFFIS toolset for modeling of embedded systems and validation

Alberto Sangiovanni-Vincentelli (PARADES)

Contributions of his team: Platform-Based Design, UML Platforms and the Metropolis framework, industrial applications.

Wang Yi (Uppsala)
Contributions of his team: Connection between modelling and verification tools, Times tool

Bengt Jonsson, Uppsala University,
Contributions of his team: Component Modeling and Verification

1.2 Affiliated Participants and Roles

Julio Medina (U. of Cantabria)
Contributions of his team: Schedulability Analysis and Component-Based solutions inside the standardization effort for the UML Profile for Modelling and Analysis of Real-Time and Embedded Systems: MARTE (prospective standard of the OMG).

David Lesens (EADS)
Contributions of his team: Proposal of case studies concerning architecture modelling (integration of AADL and UML) and timing analysis in the ASSERT project. Participated in a common publication [HJR+07]

Alain Leguennec (Esterel Technologies)
Contributions of his team: collaboration on the SPEEDS platform

Veronique Fabre (Thales)
Contributions of her team: collaboration on the extension of Persiform platform in the context of OpenEmBeDD

Martin Torngren (KTH).
KTH is a core partner in the Control for Embedded systems cluster of ARTIST2.
Contributions of his team: Collaboration on the “safety critical” platform, in particular in the context of the ATESST project.

1.3 Starting Date, and Expected Ending Date

Started: September 1st, 2004

Expected Ending date: end of the project

Developing standard modelling and validation platforms is a long term effort. Several important projects have just started or will start their developments close to the end of ARTIST 2. In particular,: the SPEEDS IP project, ending after the conclusion of ARTIST2, is expected to contribute significantly to the platform and a large French project of the System@tic pole of competitivity, Usine Logicielle (Software Factory), started at the end of 2005 with a 3 to 5 year time horizon.

The work plan of the Artist platform activity is meant to be adapted on a regular basis to take into account relevant events outside ARTIST, such as the emergence of new standards or new technical trends. An important objective is providing a discussion forum to allow exchange and sharing of ideas between projects working on related methods and tools.

1.4 Baseline

Before ARTIST started, UML was becoming a standard for model-based development, also in the context of real-time and embedded systems, even if it was lacking a number of concepts needed for this purpose and supporting validation tools. In the context of real-time embedded systems, there existed a number of UML based CASE tools (e.g., Artisan, Rhapsody, RoseRT, and TAU) and a large number of analysis and validation tools, mostly coming from academia. With a few exceptions, they were dedicated to specific profiles taking into account a small subset of UML and are weakly integrated in the development flow.

Several of the platform participants had already started considerable efforts for integrating analysis and validation into the development flow --- in particular in the framework of IST projects AIT-WOODES (CEA: Accord Methodology and tool support, OFFIS: verification tool for UML in Rhapsody), OMEGA (VERIMAG: IF verification tool for real-time UML, OFFIS: verification tool for UML), and Metropolis (PARADES: UML platform).

1.5 Problem Tackled in Year 4

In the previous years, we collaborated on two transversal topics and on three platforms.

The transversal topics are related model representations shared by tools and to backend engines:

- Topic 1: Modelling languages and semantic frameworks and their implementations
- Topic 5: Tranversal validation technology (partly shared with T&V cluster)

Each of the platforms provides one or several loosely coupled tool chains. The common denominator of each tool chains is the application domain, that is, the kind of problems to be tackled and also the modelling concepts used. Indeed, the tools of the platforms generally either share a common modelling framework, or are based on complementary (respectively similar) frameworks which show potential for convergence or integration (see also Figure 1, in Section 2.1):

- Topic 2: A platform for the development of safety-critical embedded systems
- Topic 3: A platform for the analysis of performance critical service-based systems
- Topic 4: A platform for the certification of smart-card applications

In fact, the first platform is mainly about generic techniques whereas the two other platforms target more specific application domains. A long term goal is reaching a state where they are indeed instances of a common platform. However, since this approach needs a significant amount of dedicated resources, it is outside the scope of Artist.

Globally, the work has continued according to the last 18 month plan, the tool chains which started to be developed have been further extended and connected.

Topic 1: Modelling languages and semantic frameworks and their implementations

There will be less work on the modelling formalisms themselves in this last year. There will be some work on consolidation and some extensions, in particular for HRC which has not yet be assessed so far. There will be work on tooling for and evaluation of usage of languages for languages, in particular

- Integration of scheduling analysis tools with Papyrus to exploit UML MARTE models and the defintion and prototyping of the model transformation needed to translate a UML model annotated with extensions of the MARTE's sub-profile dedicated to schedulability analysis and an external formalism dedicated to that purpose.

- In the SPEEDS project, we have made important progress during this year: the HRC framework for modelling heteregenous system has bee finalised and the definition of a SySML profile for HRC is almost terminated. HRC defines a rich framework for structural composition englobaing synchronous composition and BIP-like composition, a state-machine based language for the description of behaviours of components, and a property language for the definition of contracts. The use of HRC and translations from HRC to specification formats of several analysis tools makes analysis available to users of SySML as long as they conform to the HRC SySML profile and its semantics. There exist also first implementations of academic and tool vendor tools for hosted simulation which consists in composing component implementations provided by code generators of different tools according to the composition model of HRC by means of an appropriate API that has been defined in the project.
- We have developed a theory for semantic preserving distribution of BIP specifications and we have extended the execution engine so as to run BIP specifications in a multi-threaded fashion so as to allow new interactions before all current interactions are terminated. We have also defined a general framework for contract-based reasoning for frameworks with BIP definable composition operators
- Extension of the Metropolis II framework to deal with distributed systems. A demonstration of this extension is available for the analysis of the airconditioning system of the Don Pederson Center in Berkeley. We have developed an optimization framework, based on an ILP formulation, to select the communication and synchronization model for an automotive distributed system that leverages the trade-offs between the purely periodic and the precedence constrained data-driven activation models to meet the latency and jitter requirements of the application.

Topic 2: Platform for analysis of safety critical embedded systems

The main work on this platform has been carried out within the following – related – projects: the IP project SPEEDS, the ITEA project SPICES, the French National ANR project OpenEmBeDD, and the System@tic/Usine Logicielle project ATTEST.

- In OpenEmBeDD, the development of generic support for model-based development, in the form of editors and model-transformation frameworks, has continued, and several validation tools are being made available for designers using the modelling frameworks supported by the platform.
- In SPEEDS, several analysis tools have been extended for and adapted to be able to validate verification problems posed in the context of contract-based verification. In particular, we have proposed translations from a property specification language called CSL into HRC state machines and transformations from contract analysis problems (consistency, compatibility, contract dominance, contract satisfaction) into analysis problems as they can be solved by existing tools. The planned “process advisor” whose task it is to define the verification problems to be solved at each development step has not progressed as anticipated.**.** The ultimate goal is making available these validation techniques, as well as code generation techniques to the designers in commercial tools, in particular those considered in SPEEDS, that is SCADE and Rhapsody. We expect that the work done within the SPEEDS project will contribute to a stronger integration of tools.
- The work on the BIP/THINK/Buzz tool chain has focussed on the validation of the BUZZ approach on a lightweight concrete operating system such as TinyOS and we have significantly improved the existing link between BUZZ and the BIP-based analysis and verification tools. In the projects SPICES and OpenEmBeDD and we have improved the translation from AADL to BIP.

- Another line of work on the MARTE profile is its integration along the entire system development process through defining requirements and traceability support within a model-driven appraoches based on the UML. Within the context of the MemVaTEx French project, CEA-LIST has defined a MARTE extension to deal with requirements and traceability issues. This latter is compatible with MARTE, SysML and EAST-ADL2, and a plug-in has been implementyed within the open source tool for UML2 Papyrus in order to support these extensions

Topic 3: platform for analysis of performance critical embedded systems

- After the end of the Persiform project, the work on this platform will consist in the assessment of the usability of the tool chain in the context of an OpenEmbedd case study. This may lead to some modifications. We also plan to progress on the use of performance models in functional analysis.
- In the context of the ARESA project on the analysis of energy consumption of wireless sensor networks, we have now developed the framework for the validation of wireless sensor networks (WSNs) with respect to energy consumption. This framework both integrates a global and accurate model of WSN, and component-based abstraction techniques to verify energy related properties.

Topic 4: Platform for certification of smart-card applications

- The work on this platform has been carried out in the EDEN-2 project. The work of this last year of the project has consisted mainly in tackling the problem of generation of certificates from verification results.

Topic 5: Transversal validation technology

- The work on specific analysis engines that will be used in the context of several platforms will include at least the following ones:
- Refinement of charactisation of the capabilities of the symbolic execution kernel Agatha to deal efficiently with hybrid formalisms as used in automotive industry (with particular focus on Matlab/Simulink). Finalise a first prototype for component-based test generation from heterogenous specifications of systemsand its evaluation in automotive domain.
- As planned, the compositional deadlock detection/verification methods based on a combination of structural analysis of component behaviours and structural analysis of connectors has been improved and in the DeadlockFinder tool [BBNS08].
- Uppsala studied (1) state-based vs. stream-based models, and their transformation for compositional performance analysis, (2) fixed point computations in modular performance analysis in the framework of Real-Time Calculus developed by ETH, Zurich, and (3) schedulability analysis for multiprocessor platforms.
- The work on analysis algorithms for hybrid Systems with large discrete state spaces (OFFIS in cooperation with the CvO University Oldenbrug, MPI Saarbrücken and the University Freiburg) has continued to cover larger models and richer classes of models, by incorporating new representations (zonotopes in addition to linear constraints) and tightening the integration between Boolean manipulations, first-order reasoning, SAT-modulo-theory solving and abstraction refinement. Algorithms for the minimization of the combined representations of state sets with linear constraints and boolean and-

inverter graphs, concerning mainly the efficient detection and elimination of redundant of linear constraints have been designed and implemented. The extension of the representation formats to also include zonotope-based is in implementation, while the integration of SAT-modulo-theory solving and abstraction refinement.is still in preparation.

- Development of a general package (COSI) for the analysis and synthesis of optimal interconnect and communication schemes for SoCs and distributed systems. The package is integrated in the Metropolis II framework and interfaced to the PARADES Desyre simulation tool. .

Deviations from the plans

- The evaluation of the capability of the Executable UML profil to support description of heterogeneous MoCs and demonstrate consistency, which is closely tied to an ongoing OMG specification, the Executable UML Foundation. As this latter has been delayed several times (it should be finalized for the end of 2008), we decided to postpone this action, and we do expect to be able to handle this one in the context of the ARTIST Design NoE. .
- In the Eden 2 project, the initially planned functional validation of critical applications on smart cards has made only little progress due to difficulties encountered in hiring the appropriate development engineers. The planned work has been substituted by work on another important topic which is generation of certificates. .
- We could not implement this year the planned BUZZ extension allowing the user to take into account security specifications (of type access control and authentication). But we have now started a PhD thesis on this topic.
- OFFIS planned studying failure models suitable for compositional safety analysis by deriving from compositional safety analysis (underway) existing failure models are enriched to improve the compositionality of the safety analysis (i.e. producing less pessimistic results). This study has been postponed. .

1.6 Comments from Year 3 Review

1.6.1 Reviewers' Comments

4.4.1 D4-RTC-Y3 Component Modelling and Verification (Platform)

ACCEPTED
The document is of very good quality. It clearly presents and details the activities of year 3, the various actions of dissemination and collaboration inside and outside the Artist2 perimeter. It has to be noted that the project Persiform ended successfully and that activities on the platform for the analysis of performance of critical system is now driven by a new activity on simulation on wireless sensor network. The activities on dissemination and collaboration are important as shown by the number of papers from partners and from collaboration between partners and by other various communication activities (workshop, schools …).

The only point which is not very clear is the relationship with tool vendors (what is the nature of collaboration) and the industrial sector at large. However as discussed during the review meeting, this is not dependent on the Artist2 partners. Note that the listing of references by alphabetical order would improve the readability of the document.

1.6.2 How These Have Been Addressed

In this year's deliverable, we have included some details on collaborations with tool vendors and we took care of better respecting the alphabetical order of references within each section.

We understand the relative concern that the reviewers expressed about the involvement of tool vendors in ARTIST being relatively small (tool vendors are only associated partners). In some of the projects contributing to ARTIST, however, tool vendors contribute with a significant effort; some technology transfer is taking place from the project to both tool providers and industrial users of the developed technology. Examples of significant involvement of tool providers are:

- In the French Eden and Eden 2 projects, Trusted Logic – a tool provider in the domain of certification – played an important role; transfer of results of the project has already taken place.
- A main goal of the SPEEDS project is to provide a tool independent layer to represent design components. For that, SPEEDS provides a common meta-model (HRC) including different viewpoints (functional as well as non-functional ones). This common metamodel allows to connect commercial tools with various analysis tools. In the SPEEDS project, several tool vendors contribute significantly to the tool integration problem by providing interfaces to import and export HRC models by a number of design tools (such as SCADE, Rhapsody, RT-Builder,Matlab/Simulink.) which allows to analyse the design models using a set of appropriate tools, some of which are new.
- Cadence Design Systems Europe is a founding member of PARADES and contributes with tools and ideas to the research described here.
- The INTERESTED project has been built to exactly match the goals defined within the Objective ICT-2007-3.3b ("Suites of interoperable design tools for rapid design and prototyping"), namely creating a reference and open interoperable embedded systems tool-chain, fulfilling the needs of the industry for designing and prototyping embedded systems: http://www.interested-ip.eu/

Besides transfer to and involvement of tool providers, we can mention other recent or ongoing industrial involvement and exploitation:

- Two industrial partners are involved in the ARESA project (Orange Labs and Coronis), and a part of their activity is to develop new energy efficient solutions for wireless infrastructures (from the nodes architecture to the software communication stacks). A dedicated and global simulation tool like Glonemo will help them to early evaluate a given design, before any concrete deployment.
- In the ASSERT project, we have adapted the OMEGA-IF tool chain for the validation of real-time UML specifications to the UML profile used in the ASSERT project and we have enriched the library for the description of architectures. This tool is presently being adapted to UML2 and the latest Rhapsody version for ESA.
- Within SPEEDS we discussed with several industrial partners of the automotive domain how the SPEEDS modeling approach can be linked with AUTOSAR.

2. Summary of Activity Progress

2.1 Reminder: Work in Year 1

The main objective of the first year of the project was to obtain an inventory of potentially interesting tools, possibly to do some initial developments within these tools towards a possible integration and finally to define a concrete vision of the ARTIST platform for component-based design and validation. This has been done during the meetings hold in Grenoble in October 2004, in Paris in January 2005 and in Rennes, end of June 2005. The June 2005 meeting has been hold in common with the hard real time and the adaptive real time clusters.

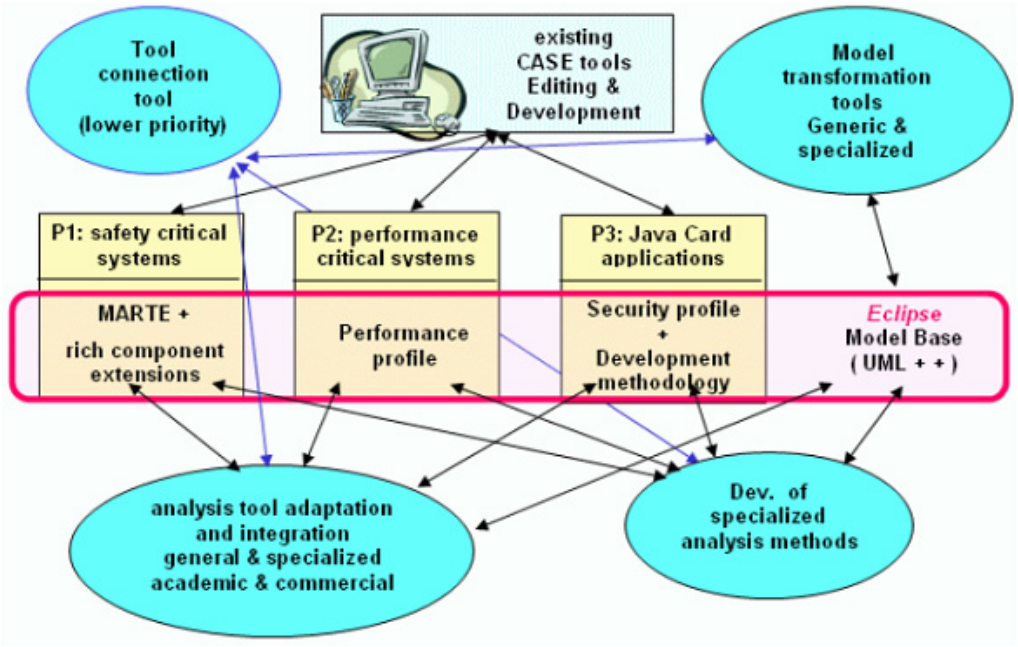


Figure 2.1-1: Planned platform architecture

We had chosen the option to first connect a restricted set of model-based analysis and validation tools with the help of tools implementing UML compatible model transformation technology and possibly – if this turns out to be useful – tools allowing to generate complex functionalities from basic ones by means of abstract specifications. The set of participating tools is always to be considered preliminary; new tools were expected to join the platform over time.

Due to the large span of applications covered by the tools to be integrated into to the platform, this integration was not intended to be a strong integration in the classical sense of an integrated toolset, but rather a set of components that can be used in combination with specific components to form different tool chains. A baseline of the tools is that they are UML compatible or will be connected to such a format. Some components are designed to be specific to particular tool-chains and whereas others are useful in several ones.

Presently considered tool chains used in case studies had been identified by the following working titles:

- A *platform for the analysis of safety-critical embedded systems* (platform-1). This platform was planned to be developed mainly in the context of the future OpenEmBeDD (started in 2006), CAROLL, ASSERT and SPEEDS (starts in 2006), with contributions from SAVE and ASTEC.

- A *platform for the analysis of performance critical service-based systems* (platform-2). The Persiform project began developing this platform. The plan defined for the second year was to provide a mapping to a commercial performance analysis tool.
- A *platform for the certification of smart-card applications* (platform-3). This platform was planned to be developed principally in the EDEN project and its successor EDEN-2.

The relevant subsets of UML used in the context of these three environments are specific to the concerned target application types. The first one will focus on system specifications, where the behaviour of individual components are specified by means of state-machines and requirements by state-machines and possibly Sequence diagram. This Profile will consist of the MARTE profile and the Rich Component concept to be developed in SPEEDS. The second platform will focus on early performance specifications described in terms of activity diagrams. It is being developed in the Persiform project. The main focus of the third is the expression of security properties which are developed in the EDEN project.

The performance annotations in platform-2 will use a subset of the timing annotations in MARTE. For the description of design specifications in platforms-2 and 3 (considered in a later stage), it may be interesting to consider a subset of the profile of platform-1, but this has to be studied further. Also the profile concerning architecture modelling may be shared, but again this will be considered later.

The analysis tools should in principle be sharable amongst the platforms thanks to the mapping into a semantic level model. Our initial focus is on the following tools Agatha (CEA) for scheduling analysis and test case generation, IF/BIP (VERIMAG) for simulation and verification of timed specifications, HERMES (VERIMAG) for the verification of secrecy properties, TIMES (Uppsala) and MAST (U. Cantabria) for scheduling analysis, OFFIS tools for model-checking, safety and fault analysis, and Metropolis (PARADES) for simulation, architectural design exploration and connection to external model-checkers like SPIN. There is some overlap in the functionalities of the validation tools, but they are based on different algorithms and have different strengths and weaknesses. Some new analysis methods, specific to the needs of the specific applications will be built.

The tool jETI (U. Dortmund) is intended for a high-level integration of tool functionalities. It allows the specification of complex functionalities from functionalities provided by different tools. This kind of user-level tool integration was totally absent in earlier projects and requested by users. This activity will not be the first priority in the near future, but it will be definitely considered.

An overview on the initial version of the targeted architecture, indicating both shared and specific parts are given in Fig. 1 above. The developed tools will be ported to Eclipse.

During the first year of ARTIST, we have done only a limited amount of integration. The main progress was on individual components for these platforms, whose description can be found in the year 1 deliverables.

2.2 Reminder: Work in Year 2

The outcomes and achievements of the second year have been structured into five main topics, enumerated below.

1. Semantic foundations for modelling languages and frameworks

An important issue for our platform is achieving tool chains for related profiles by mapping them to a small set of semantic level formalisms used in validation and code generation tool chains. This year, we have done significant work on the languages and formalisms to be used to realise thiese platforms. We have considered both languages and meta-models for users

and formalism used for the definition of their semantics and for formal treatments for verification, simulation and code generation. Notice that in some cases the separation between user language and semantic formalism is quite narrow, as concepts useful for validation often end up being lifted to the user level.

The work on the ***MARTE UML profile*** involved CEA, INRIA, *Cantabria,* and *Carleton University* Canada (Dorina Petriu and Murray Woodside), with significant feedbacks from *INRIA* and *VERIMAG.* The work has well progressed in 2006, both on the general analysis profile and for schedulability related issues; implementation is underway. It benefits from the support of two large French projects, the Usine Logicielle (Software Factory) project and the OpenEmbeDD platform project. These two projects also support the development of an Action Language Editor (Eclipse component) to instantiate the UML action semantics on domain usage (syntax and refined semantics). The work on MARTE is completed for the automotive domain by the development of the "EAST-ADL 2" UML profile for automotive architecture and component modelling. Based on the *Autosar*^{TM} meta-model, it aims to provide a higher level of software component modelling and to better support behavioural modelling aspects. The CEA, INRIA and Thales teams are contributing to the elaboration of a new standard: ***Executable UML foundation*** that aims at providing a formal framework for defining anexecution semantics of UML profiles in order to help harmonizing other standards.

Within the OPRAIL project, a UML profile called ***Safe-UML*** to be used in the context of safety critical system is being developed. The experiences with Safe-UML will be used within SPEEDS to derive efficient analysis techniques for UML/SysML. Safe-UML is a restriction of general UML to be used for enabling a CENELEC-conformant development of safety-critical rail systems. As UML is intended to cover the entire design process, when it is deployed in a particular domain of application, it has to be instantiated for a concrete, tool-supported environment. The profile focuses on structural diagrams (class diagrams) and behavioural diagrams (state charts). Models following this profile shall be compliant to standards (e.g. code compliance with the German railway guidelines MÜ8004 for the generated code) and it is expected that verification tools based on Safe-UML can be improved significantly from a performance point of view in relation to a general UML verifier.

Developing the concept of **rich component models** into a mature framework for system design is pursued within IP-SPEEDS by RTC partners INRIA, OFFIS, PARADES, and VERIMAG. The research activity is centered on the development of a meta-model for rich components, called ***HRC***. This includes defining a notion of component for which different *viewpoints* (e.g., functional, times, and safety) can be synchronized, and different viewpoints for different components can be formally composed. It should comply with existing or de-facto standards, including the Autosar real-time component model and SysML.

The ***BIP framework*** (Behaviour, Interaction, Priority) developed at VERIMAG is used in OpenEmbeDD, SPEEDS and other projects being set up for providing a mapping from user level languages to the semantic level, preserving the structure. It addresses two fundamental sources of heterogeneity: one is the composition of subsystems with different execution and interaction semantics. The second is the use of models that represent a system at different degrees of detail and are related to each other in an abstraction (or equivalently, refinement) hierarchy. The BIP framework provides a semantic framework for these systems of heterogeneous components. A virtual machine for executing BIP specifications has been implemented and connected to validation tools. Initial results concerning highly efficient methods were obtained for guaranteeing deadlock freedom.

PARADES has been instrumental in transferring the knowledge of the ***Metropolis framework*** and related design methodology to a set of industrial designs and to the HRC modeling effort in SPEEDS. During the design of the industrial projects for PARADES partners (ST and United Technology), it was evident that the user-interface and architecture of Metropolis was intended for experts in the methodology supported by Metropolis and in the semantics of the tool.

PARADES was instrumental in inspiring the transition form Metropolis to Metropolis II, where the architecture of the environment is intended to facilitate the job of the system architects and developers. The principles upon which Metropolis II rests are mathematically the same as Metropolis but the implementation of the semantics is essentially different. In particular, the aim is (1) to take into account heterogeneity --- IPs may be specified in different languages or conform to different models of computation, (2) to be able of taking different parts of a design and refining/abstracting them so that these relationships can be verified, and (3) to relate architectural platform and functionality in different ways to explore different realizations of the system with respect to quantitative extrafunctional properties.

BIP and Metropolis are intended to be used for supporting rich components and for providing verification and synthesis services.

2. Platform for the analysis of safety critical embedded systems

The research activities carried out for this platform are building upon UML profiles, in particular MARTE and HRC. The main efforts during the 2nd year concern back-end tool chains, starting from one of the envisaged semantic level formats and integrating validation and code generation tools.

Two important collaborative projects for this platform have started this year: The French National project ***OpenEmbeDD*** (http://openembedd.inria.fr) and the ***SPEEDS IP*** (http://www.speeds.eu). The work on these projects during the second ARTIST year focused on enabling modelling principles and not yet on tools.

The INRIA team developed a tool chain using tools of several ARTIST teams (IF, Kronos, Giotto, Kermeta). The chain aims at supporting a complete software design process for real-time components, from service specifications down to executable software components in Java or C. The component implementation process uses a two-step method: designers construct an abstract implementation using timed automata, which is checked against the specification using the IF and Kronos tools from *VERIMAG*. A concrete implementation, to be executed on Giotto platform designed by the *EPFL* team, is generated by model transformations using tools from *INRIA Triskell team*. The tool chain implementation by INRIA has been completed.

The ***BIP framework*** has been implemented as follows: a front-end for editing and parsing BIP and generating C++ code to be executed and analyzed on a backend platform and a back-end platform consisting of an engine and the infrastructure for executing the generated C++ code. It has been entirely implemented in C++ on Linux and uses POSIX threads. The execution engine iteratively executes the following step. At a given state, it monitors the state of atomic components and finds all the enabled interactions by evaluating the guards on the connectors. Then, between the enabled interactions, priority rules are used to eliminate the ones with low priority. Amongst the maximal enabled interactions, it executes one and notifies the atomic components involved in this interaction. The notified components continue their local computation independently and eventually reach new control states. The current implementation is suited for the state space exploration-based analysis of systems but not for embedded operating systems kernels and low-level services.

A ***BIP/THINK collaboration*** between FTRD and VERIMAG has started this year. The goal of this joint effort is to obtain simultaneously the executable embedded code of an OS and its behavioural model for analysis and verification. Today a transformation exists from BIP (used for analysis) to THINK. This project is now financed in a project in the context of EMSOC.

The ***UPPAAL tool*** for verification of timed automata has been upgraded by the Uppsala team to handle UML specifications and integrated in the Eclipse platform. The UPPAAL modelling language has been extended with hierarchical state machines, to support modelling of hierarchical structures and abstract behaviours of components.

3. Platform for the analysis of performance critical systems

This platform is presently developed in the context of the French Persiform (http://www-persiform.imag.fr) project (with ARTIST partners FTRD, INRIA and VERIMAG). The aim of this project is the integration of performance evaluation and formal verification in requirement and design activities. A first aim is to connect commercial performance analysis tool (event-based simulation) to functional UML modelling tools for high-level performance analysis. For this purpose, a profile for the use of activity diagrams has been defined and a formal semantics has been defined through a mapping to a restricted class of coloured Petri nets plus annotations with probabilities and distribution concerning timing and resource usage. The Annotated Petri nets are then transformed into performance evaluation platform SES Workbench (http://www.mmsolutions.com/english/workbench.htm). Alternatively MSC can be handled a transformation into the same class of annotated Petri nets. These transformations are based on the construction of meta-models for the different languages and transformation rules.

4. Platform for the certification of smart-card applications

The work on this platform is supported by collaboration between CEA and VERIMAG on functional validation of critical applications on smart cards. This work is carried out in the context of a national project, EDEN 2. EDEN 2 capitalizes on the work done in its precursor, EDEN, in order to reach a consolidated implementation for industrial exploitation. It has not progressed according to the plans that included the definition of a UML profile for security properties, Rather than working on the profile during the first year, it was decided to focus on the validation engine.

5. Generic validation technology for non functional properties and component systems

The development of new verification techniques is not the primary goal of the component platform. The focus here is on the connection of existing verification tools to the modelling languages considered in the platform.

Last year, we started to reimplement ***UPPAAL, TIMES, and also CATS*** in the Eclipse tool platform. The ambition is to integrate them in one tool environment, which supports hierarchical modelling and compositional analysis. Nevertheless, this is a long term effort. For adapting UPPAAL for asynchronous models we need to check the boundedness of channels, and to synthesize the maximal size of memory blocks necessary to implement the channels. Preliminary results show that the expressive power of these systems with two channels is Turing-equivalent. Preliminary results have been obtained on methods based on approximations. As an abstraction for communication interfaces, we have adopted arrival curves from network calculus. The CATS tool and the compositional analysis techniques based on stream transducers will be evaluated in realistic setting and integrated with UPPAAL. The plan is to collaborate with EPFL on the real-time calculus.

The symbolic execution kernel of ***Agatha*** has been extended to support analysis of systems with a heterogeneous model of computation. Developed by CEA through three national projects (STACS, Usine Logicielle and EDEN 2), it is implemented as an Eclipse component for test generation from UML models. Within the EDEN 2 project it is connected to the VERIMAG IF tool in the context of the platform 3 for certification of smart-card applications.

In the context of the ***BIP framework***, we derived sufficient conditions for guaranteeing properties of component systems by exploiting the structure of the BIP framework that strictly separates the description of behaviour of components from the way they interact and execute. We have considered so far liveness, local progress, local and global deadlock, and robustness.

2.3 Reminder: Work of year 3

As in the second year, the outcomes and achievements of the third year are presented in the form of five main topics, including a theme on modelling languages and semantic frameworks, 3 platforms enumerated below, and a theme on transversal validation technology closely related to work on the three platforms. Each platform is centered on a particular application domain or technology used and provides one or several loosely coupled tool chains (see also Figure 1, in Section 2.1):

- A platform for the development of safety-critical embedded systems
- A platform for the analysis of performance critical service-based systems
- A platform for the certification of smart-card applications

In fact, the constituents of first platform are rather generic, in the sense that they do not address particular application domains, whereas the two other platforms target more specific application domains or aspects of system development.

1. Modelling languages and semantic frameworks and their implementations

- The MARTE UML profile for modelling real-time systems has been finalised and partially implemented [TRGD07], [TGDT07], [TETG07], [TG06]. Also work on a complementary profile for fault tolerance and safety requirements has been continued, as well as the work on an executable UML profile [LETG07], [CMTG07c], [CMTG07b], [CMTG07a].
- In the SPEEDS project, a **rich component model** (called HRC, standing for Heterogeneous Rich Components) has been defined [BCSM07] and implemented as a standalone metamodel. This component model features
- The BIP framework providing a rich framework for incremental component composition based on a three layered structure developed by VERIMAG has been enriched with hierarchical connectors and a notion of component encapsulation [BS07a], [BS07c], [GQ07]; BIP connectors are now part of the HRC metamodel. The execution and simulation platform for BIP has been significantly improved and several case studies have been carried out.
- Metropolis II [DDM+] that is centered on the coordination of components has been finalised. A simulator is being defined that operates based on the operational description “filtered” by the constraints. The Metropolis meta-model concepts have been provided as input to the HRC modelling effort in SPEEDS.

2. Platform for the analysis of safety critical embedded systems

In the second year, the main focus was on the user and semantic level formalisms, an effort which has continued in year 3. But the essential effort was dedicated analysis tools implemented in tool chains, integrating validation and code generation tools. The main work on the mappings from user level profiles to semantic level formalisms has started towards the end of year 3 for the MARTE profile and and a bit later for HRC.

- In the first 18 months of the French National project OpenEmbeDD with ARTIST Partners CEA, France Telecom, INRIA, Thales, and VERIMAG (http://openembedd.inria.fr), we defined the platform architecture, we put into place generic techniques and we started the implementation of mappings from the user level formalisms to intermediate formats using model transformation techniques such as Kermeta and ATL We started work on translations from AADL to BIP and a study of the translation of a Scicos model into BIP.
- In the first 18 months of the SPEEDS IP project with ARTIST partners INRIA, OFFIS, PARADES, and VERIMAG (http://www.speeds.eu.com) whose aim is the integration of analysis in the system development process and design methodology, we defined the global architecture of the tool infrastructure and we started the development of methods exploiting the HRC contracts and the distinction of view points. We started to conceptually

integrate some existing validation techniques also some work on new, specific verification technology (see also results on validation technology).

- The INRIA team has in collaboration with Verimag and EPFL extended the *IF, Kronos, Giotto, Kermeta chain* to include support for BIP components as inputs for validation, and code- and monitor generation [SBD06], [SBD07].
- The collaboration between FTRD and Verimag with the objective to compile BIP component systems to Fractal/Think for execution on microcontrollers has continued by means of a common PhD work. The transformation from BIP (used for analysis) to Think (used for compilation on an OS) has been implemented In order to extend Think with behaviour description and to better to capture the concepts provided by standard ADLs, the Buzz language allowing the interconnection of passive and active components in a synchronous, asynchronous, delayed, … fashion has been developed [BMP+07]. The semantics of Buzz has been defined by means of a translation from Think to BIP. In parallel, in the Spices ITEA project (http://www.spices-itea.org/public/news.php) work has started on the direct translation of AADL to BIP and Lustre [HJR+07].
- In the AMAES project (http://www-verimag.imag.fr/~krichen/AMAES/) with Artist partner Verimag, we have started to work on the application of BIP to autonomous Robot systems by prescribing a particular architectural style and providing specific analysis techniques. This methodology considers that the global system architecture can be obtained as the hierarchical composition of larger components from a small set of classes of atomic components which we describe with BIP. A main contribution is a methodology for componentizing and architecting autonomous robot that integrates smoothly into the design process and leads to analysable system architectures [BK*07].

3. Platform for the analysis of performance-critical systems

This platform consists of two parts which are for the time being not related. A tool chain allowing the integration of a state-of-the-art performance simulator into the design flow of service oriented systems and a simulation-based approach for evaluating energy related properties in sensor networks.

- The main body of the work in this area was carried out in the context of the French Persiform project (http://www-persiform.imag.fr) with ARTIST partners FTRD, INRIA and VERIMAG. This project has now successfully terminated. A platform for performance evaluation of functional specifications of services to be integrated into existing service platforms has been developed by means of a transformation chain from a service oriented UML profile into a graphical model in the performance analysis tool HyPerformix Workbench (http://www.hyperformix.com/products/workbench/) (see also figures 2.4.6 and 2.4.7). The transformation chain has been significantly improved this year, and mainly been realized using the model transformation framework ATL which required the development of (reusable) intermediate meta-models. This platform has now been successfully demonstrated on case studies [CGM07]. Extremely positive feedback from potential users has been received.
- Recently, we started to work on simulation and validation of energy related properties of sensor networks for the purpose of estimating network lifetime [DB*07], [MSZ07], Network lifetime is determined by the energy consumption due to commutations in individual nodes and communication activities. This is carried out in the ARESA project with ARTIST partners FTRD and Verimag (http://www.citi.insa-lyon.fr/project/aresa/). We address the problem of developing accurate prototypes of WSNs, that can be formaly analyzed, and that can be transformed by dedicated abstraction mechanisms, able to simplify the model complexity while preserving (or at least over-approximating) the energy consumption. We started using a global synchronous approach to the problem and have developed a simulator has been (http://www-verimag.imag.fr/~samper/Glonemo/).

4. Platform for the certification of smart-card applications.

The work on this platform on functional validation of critical applications on smart cards is supported by the Eden and Eden-2 projects with ARTIST partners CEA and VERIMAG (http://www.eden-rntl.org/). The aim in Eden-2 is to reach a consolidated implementation for industrial exploitation. This year, we have defined a methodology for the certification of smart-applications according to the International standard known as the *Comon Criteria* (CC) for security and developed tools for its support [FGG07], [GGRT06] (see also figure 2.4.9).

The methodology uses formal methods to reach the highest level of certification (Evaluation Assurance Level 7+): full formal development. It is supported by several verification tools which aim at helping developers of JavaCard applications to produce the evidences requested for such a certification. All the tools are integrated in the Eclipse environment and support the entire development from UML specifications to the verdict of the verification tools and certification documents. The TLFIT tool helps to produce the documentation required for certification, it eases the traceability of the security requirements from their expression in natural language to the specification of the formal security policy and its final implementation.

Advances have also been made on the automatic generation of test objectives. CEA has worked on test case concretisation along the system specification refinement process and on unitary test derivation of components according the respective concrete use of each component inside the system ([FGG07], [GGRT06]).

5. Transversal validation technology for platforms

We describe here a set of validation methods and tools which are developed in the context of one of the platforms. We group the description here, as most of them – are already or may in the future – be shared amongst several platforms, at least after some adaptation. We expect that the development of intermediate representations will help making adaptation easier.

- In Uppsala, the main effort has been on validation techniques for timed systems, in particular resource-related analysis to cover a broad range of resources such as processors, buffers and memory blocks etc. Due to undecidability of most interesting problems [FKPY07, KSY07], approximation and abstraction methods have been developed. A prototype tool ***CATS***, www.timestool.com/cats, for compositional timing and performance analysis has been developed for systems modeled using timed automata and the real time calculus developed at EPFL. The tool combines timing and performance analysis [HP07].
- The symbolic execution kernel Agatha has been integrated in the Usine Logicielle Eclipse platform (National project of the System@tic Paris-Région pole of competitivity - www.usine-logicielle.org). It allows exploiting UML models in order to generate requirement test cases.
- We have designed and partly implemented a tool which verifies absence of deadlocks for BIP specifications (http://www-verimag.imag.fr/~async/BIP/bip.html). We have developed abstract criteria based on dependency graphs [GGM+07a], [GGM+07]; it turned out that the number of potential cycles is generally to high to make hte naive methods practical. Finally, we have considered methods exploiting the global Petrinet defined by a BIP system for checking deadlock freedom for BIP component systems.
- OFFIS has worked in collaboration with other partners on efficient validation algorithms for timing and hybrid system analaysis. Uppaal has been extended by methods for directed model-ckecking [KD*07, KD*07b], techniques for validation of hybrid systems with large discrete spaces have been obtained by combining techniques [DD*07], [Seg07]. Cyclic timed automata have been used as a bridge between timed automat and timed event streams allowing the combined use of analysis techniques based on them.

2.4 Final Results

2.4.1 Technical Achievements

The problems tackled in the fourth year are presented according to the previously defined structure, i.e., 3 platforms concerned with specific application domains (see Figure 1 in section 2.1). The main objectives were: (1) to continue the integration, (2) to continue the work in projects OpenEmbedd, SPEEDS, ATESST,... and to start work on the new projects Combest and Genesys. In addition, we have initiated and recently started new collaborations.

As in the previous years, the overall achievements are divided into 5 topics:

1. Modelling languages and semantic frameworks and their implementations
2. Platform for the analysis of safety critical embedded systems ,
3. Platform for the analysis of performance critical systems,
4. Platform for the certification of smart-card applications,
5. Transversal validation technology for platforms.

Topic 1: Modelling languages, semantic frameworks and their implementations

The work on the platform interacts with and depends on several activities related to UML-based modelling languages and the development of (simpler) formalisms for a semantic level representation of component-based models. An important goal is composing tool chains in which user level modelling concepts are mapped to a small set of (rich) semantic level formalisms which provides the mechanisms to implement the validation and code generation tool chains. More detailed accounts on the languages and semantic frameworks is given in other deliverables, in particular the deliverable on standardisation the deliverable on “Component-Based Design of Heterogeneous Systems”. These are the languages and corresponding tools that are used in the different platforms either as frontends or backends.

Since its adoption by the OMG (Object Management Group), the *MARTE profile* is entered in a second stage which consists of two aspects: Firstly, the implementation of the profile itself within different UML tools has been made available and others are in development by tool vendors. Readers may have a look on the following link for up-to-date information related to that subject, http://www.omgmarte.org/Tools.htm. Secondly, CEA has developed gateways from the Papyrus tool extended to support MARTE thanks to its specific plug-in towards two schedulability analysis tools, SymTA/S and MAST.

CEA has developed an extension of the EAST-ADL2 language for dealing with requirements and traceability. All extensions have been implemented in a specific UML profile related to the MeMVaTEx methodology (http://www.memvatex.org).

CEA has also continued implementing a UML profile for the EAST-ADL2 language in the context of the open-source UML2 tool, Papyrus (http://www.papyrusuml.org).

HRC (Heterogeneous Rich Components) are being defined in the SPEEDS project (http://www.speeds.eu.com) to form the foundations for the component based construction of complete virtual system models. Its main objectives are: 1) to define a semantic-based common meta-model, 2) to develop a framework for multiple viewpoint (functional and non-functional) component engineering, 3) to enable full-scale reuse of components, 4) to offer, from COTS modelling tools, access to meta-model compliant components and, 5) to assess early project risks at subsystem level to secure concurrent design processes.

The HRC meta-model has been defined first as a stand-alone meta-model [CMMSS08] and has been implemented as an Eclipse plug-in. As SysML is becoming an important standard for

systems engineering, a SysML profile version of HRC has been defined this year [Metal08] to permit users to model with any UML tool.

In order provide users a means for formulating contracts in a (design) tool independent way, a pattern based language CSL for the expression of assumptions and promises in contracts has been defined, as well as a transformation from CSL into HRC [CG08] which will be exploited by the analysis tools. Obviously, such a pattern-based language is adequate for the representation of relatively simple properties. Representing arbitrary stateful properties with this language is possible, but not practical. At a later point of time, many more patterns might be added, and individual users may choose what is most suitable for them. This is possible because tools work on HRC models.

The BIP (http://www-verimag.imag.fr/~async/index.php?view=components) *component framework* is based on the strict separation between the behaviour of individual components, an interaction model defining how information flow may take place and dynamic priority rules for the expression of execution models. Previously, we have defined a notion of *hierarchical connector* that has been been integrated to HRC and connector algebras that allow transforming a system architecture specification according to any required (hierarchical) grouping of components [BS07a], [BS07c]. In this period, we have defined a notion of expressivity appropriate for component systems and shown expressivity results for BIP [BS08]. We have also defined distributed (partial order) semantics for BIP and provided conditions under which these distributed semantics are observationally equivalent to the global semantics [BBBS08].

In the context of SPEEDS, we have started to develop a general framework for contract-based reasoning. In the previous year we had made some proposals for the expression of proper encapsulation in BIP and had given a proof rule for dominance [GQ07]. This year, we have generalised the contract-related concepts defined in HRC and defined a contract framework by (1) a behaviour description formalism, (2) a set of composition operators $\gamma \in \Gamma$ with a composition on Γ as in BIP, such that each γ represents a composition $[\gamma]$ on behaviours, and (3) a notion of refinement under context on behaviours. In this setting, the notions of satisfaction and dominance become derived notations. Circular reasoning is defined as a property of refinement under context preorder, and a set of proof rules are given representing sufficient conditions for proving dominance in any framework allowing circular reasoning. We study 2 particular instance of that framework: the first one – corresponding to the simplest framework considered in SPEEDS - uses I/O automata to describe behaviours with the usual composition operator and a notion of refinement based on trace inclusion. In the second one behaviours are defined by modal transition systems, allows all composition operators definable in BIP – that means any composition definable by SOS rules – and refinement under context is obtained as a strengthening of the usual notion of simulation between MTS. This framework allows the expression of both safety and progress properties and their compositional verification [QG08].

The semantics of Metropolis II [DDM+] is centered on the connection and coordination of components [SV]. We use the same definitions for events, actions, and services as Metropolis. An action is a primitive concept. It roughly corresponds to a piece of code in the design. Variables (state) may be explicitly associated with an action. An event represents the execution of the beginning or the end of an action by a particular process. A service is a set of sequences of actions, with a unique begin/end event pair. Variables in the scope of the begin event can be used as service arguments. Variables in the scope of the end event can be used as return values. Events, and by extension, services, may be annotated by quantities of interest. Quantities capture the cost of carrying out particular operations and are implemented using quantity managers. Quantity managers are special components that provide annotation services. Schedulers are similar to quantity managers, but instead of a quantity they provide

scheduling and arbitration of shared resources. Depending on the MoC used and the needs of the design, different quantity managers and schedulers can be used.In Metropolis II designs are specified by instantiating and connecting different components, and then annotating and constraining their interactions. Metropolis II can describe with these primitive concepts both functionality and architectures. Quantity managers are essential for defining and manipulating non functional quantities. The links between functions and architectures needed to support their implementation is provided by the *mapping* mechanism that associates events between functional and architecture net-lists.

Because of the generality of the functional and architectural modeling approach of Metropolis II, the extension to deal with distributed systems involves the derivation of models and quantities that are relevant for the application. Because the framework allows the integration of foreign tools, we linked it to the Modelica simulation engine to simulate the behavior of the temperature in the rooms of the Don Pederson Center of the Department of EECS at the University of California at Berkeley. The simulator provides a way of associating the quantity "temperature" to the objects of the systems (the rooms). We also modeled the set of sensors that can be used to monitor the control system that form a library in the sense of Platform-Based Design. The communication infrastructure can then be selected optimally by using another external tool, COSI, which will be described below.

A component of the PBD methodology is to decompose the design process in refinement steps where the functionality (what the system is supposed to do) is **mapped** into an assembly of components (how the system does it) out of a library of available parts (the platform) satisfying a set of constraints posed by the designers. The choice of the components to use and mapping are the essential steps in design implementation. Optimizing these steps is critical to the quality of the design and to design time. While this optimization can be carried out manually, the real benefit of a formal approach to design as the one offered by PBD is that the process can be automated. Since the platform components depend on the particular application domain, while the overall scheme is common across domains, optimization should leverage all information about the design space. PARADES in collaboration with UC Berkeley proposed a common design flow for solving the mapping problems and we customized the algorithms for a variety of domains including multimedia and automotive. The common design flow forms the core of the Metro II framework.

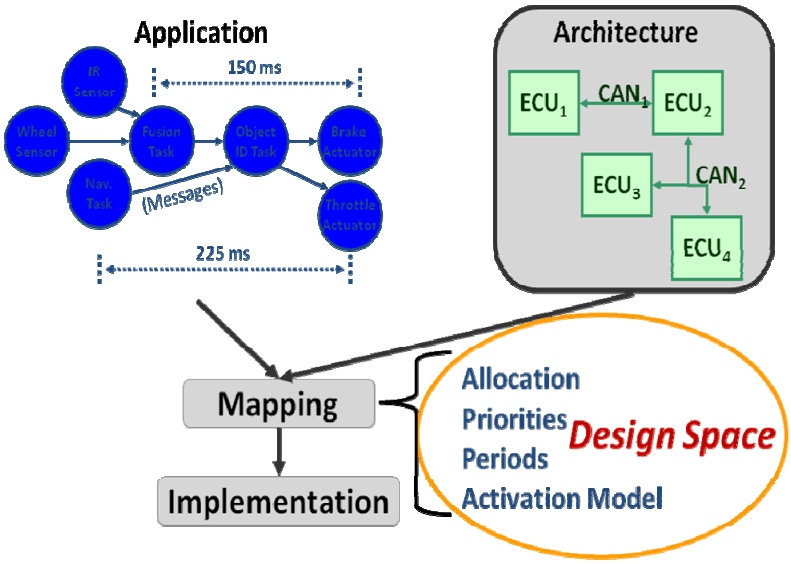


Figure 2.4-1 Design Flow for optimizing distributed systems with latency constraints

Mapping allocates functional blocks to tasks and tasks to ECUs. Correspondingly, signals are mapped into local communication or messages that are exchanged over the buses. The

priorities and periods of tasks and messages are also decided during mapping. Therefore, *period assignment, allocation of tasks, signal packing and allocation of messages, as well as priority assignment* are the design variables we can explore during mapping (see Figure 1). However, the entire formulation with all design variables is usually intractable for industrial-size problems. Therefore, as shown in Figure 2, we started by tackling several sub-problems that could then be integrated to provide a solution.

The first case study approached with this method was period optimization [DZD+] (this paper earned the Best Paper Award at DAC in the system category), in which the periods of tasks and messages were assigned based on geometric programming (GP) to satisfy end-to-end latency constraints. In the second case study [ZDP+, DZP+], we explored the allocation of tasks and messages, the packing of signals to messages, as well as the priorities of tasks and messages. In this case, we used a two-step mapping algorithm based on mixed integer linear programming (MILP). Also in these cases, the results warranted a best paper and a nomination for best paper award.

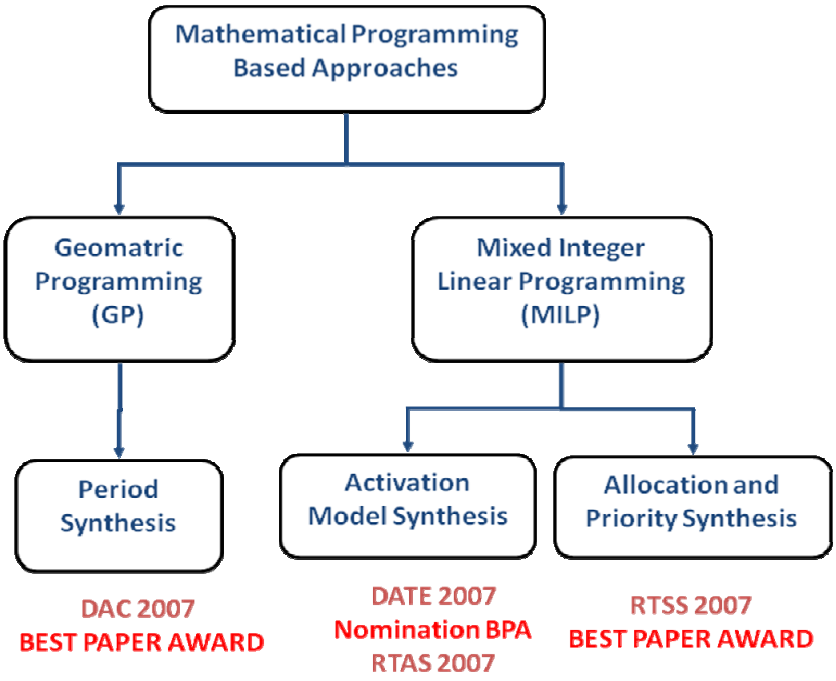


Figure 2.4-2 Approach and results

Topic 2: Platform for the analysis of safety critical embedded systems

The main effort this year concerns both, the connection between user level standards for the description of system architectures (AADL, MARTE, SysML), as well as the connection of back-end tool chains, starting from one of the envisaged semantic level formats (such as the HRC intermediate representation, or intermediate representation directly linked to back-end tools such as BIP) and integrating validation and code generation tools.

This platform has been conceived as a set of loosely connected sub-platforms which share at least some formats or tools. This year some additional connections have been added or at least planned. The subplatforms representing efforts to analyse or generate code from AADL specifications using the BIP or Lustre intermediate presentation have now already been partly made available through the OpenEmBeDD platform. The OpenEmBeDD and SPEEDS platform have previously been mainly linked through common back-end analysis tools, the choice of Eclipse as an integration framework, as well as the choice of SE-tools for model-transformations. In the future, we plan to use in SPEEDS some of the open source

developments developed in OpenEmBeDD, such as editors and model transformations. For the expression of non functional constracts in SPEEDS (going beyond the generic patterns defined in CSL), we envisage the use of macro notations from the MARTE standard. Also a link between this platform and the platform for performance critical systems has been established now through the adaptation of the Persiform tool chain for performance analysis of software systems running on a platform with an ARINC scheduler (see further down).

Notice that the work on the integration of front-end tools had started for MARTE and AADL towards the end of year 3, for and the translation SysML to HRC is still ongoing. The translation from SysML to and from HRC into formats of particular tools has been an objective of year 4, but couls not be completely terminated, especially for the frontend part.

The ***SPEEDS*** IP project (http://www.speeds.eu.com), with ARTIST partners INRIA, OFFIS, PARADES, and VERIMAG, started in 2006. It is a concerted effort to define the new generation of *end-to-end methodologies, processes and supporting tools for safety- and nonsafety-critical embedded system design.* The aim is to enable European systems industry to evolve from model-based design of hardware/software systems, towards integrated component based construction of complete virtual system models. We want to achieve this by means of a rich interface model allowing the specification of hierachical components by means of contracts associated with different view points. The interface model has a well-defined semantics and is rich enough to represent specifications from diverse commercial development tools allowing therefore the virtual integration of systems designed in different tools.

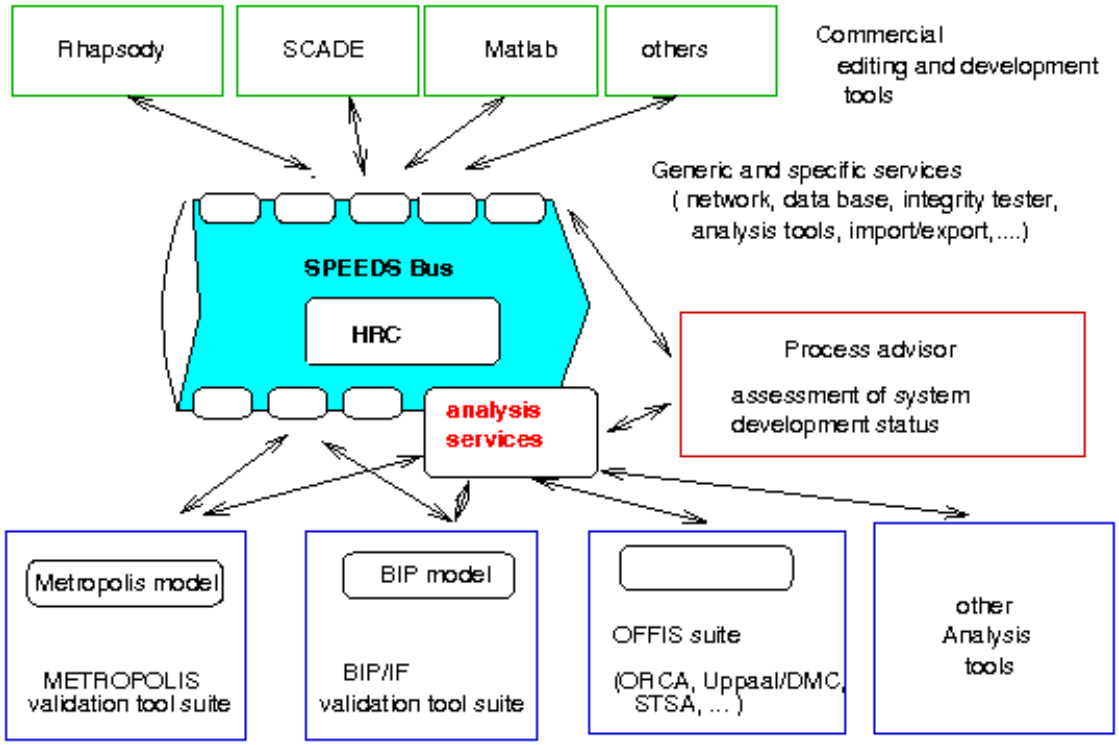


Figure 2.4-3 SPEEDS overall platform architecture

This year, an important work on tool integration has been started, and partly achieved, this year. Tool integration is done on one hand at model level through the common HRC exchange format and bi-directional translators between design tool formats (such as SysML) and HRC, and between analysis tool formats and HRC respectively. On the other hand, API's for the

integration of commercial industry standard modeling tools are defined to assemble system-level design models with rich interface specifications by combining models expressed in different authoring tools which have been made compliant to the integration standard, Tools which are presently being made SPEEDS compliant are Matlab-Simulink/Stateflow, Rhapsody, and Scade.

We have defined the concept of virtual integration by hosted simulation, as well as methods for contract-based validation in the context of HRC. Analysis results will be exploited by a process advisory tool that gives the system architect at any time an overview on the progress of the design and that helps pin-pointing potential hot spots.

Analysis will be achieved by exporting HRC interface models to different existing validation platforms, in particular BIP, Metropolis, Ariadne, ORCA, as well as some new tools. An effort is made to share generic transformations between tools, for example those transforming high-level analysis problems in more basic ones that can be directly handled by tools. Also a range of analysis methods supporting interface compliance testing and dominance analysis between contracts expressed in HRC are being developed and integrated as services into the SPEEDS platform.

The French National platform project *OpenEmbeDD* (http://openembedd.inria.fr), includes the ARTIST Partners CEA, France Telecom, INRIA, Thales, and VERIMAG. The objective of the project is to build an open platform allowing sharing of diverse analysis and simulation or code generation tools for different user level modelling and development frameworks by means of (customizable) open source transformation tools into formats of actual analysis or simulation engines. The platform provides also a set of generic tools supporting model-based system engineering in general (such as editors and frameworks for model transformation. Clearly, with respect to the SPEEDS platform, the OpenEmBeDD platform is much less focussed - in particular by not aiming at a strong integration of tools through a unique intermediate format - and could in future contain at least a considerable subset of the tools developed in SPEEDS as a subset.

A classification of the tools and formalisms considered in OpenEmBeDD can be seen in the figure below. They can be classified as follows:

- General support tools for model-based engineering: the model editors from Topcased and Papyrus and the model transformation environments Kermeta and ATL. These tools are mainly pre-existing or shared with other projects and only very partially developed within OpenEmBeDD. The Artist platform participants are involved in the development of the Papyrus editor as a support for the MARTE profile (CEA).
- User level modelling languages used for the design of embedded systems such as SDL, AADL, UML and in particular the MARTE profile.
- Intermediate formats shared between backend tool providers, in particular the formats for behaviour modelling Fiacre and SAM, each one generalising concepts of a subset of tools. These formats aim at sharing translation effort between tools, and hopefully allow decoupling the translation for individual tools from the evolution of standards. The HRC format developed in SPEEDS or the BIP format play a similar role but for system level design.
- Tools defining transformations between formats and thus enabling the definition of methodologies for the joint use of subsets of tools. The transformation chains developed by Artist platform partners (CEA, INRIA and Verimag and industrial partners FTRD and Thales) are described in more details below.

Related to the OpenEmBeDD platform are formats of individual tools and the tools that can be integrated into an OpenEmBeDD based methodology. None of these tools or formats is developed within OpenEmBeDD.

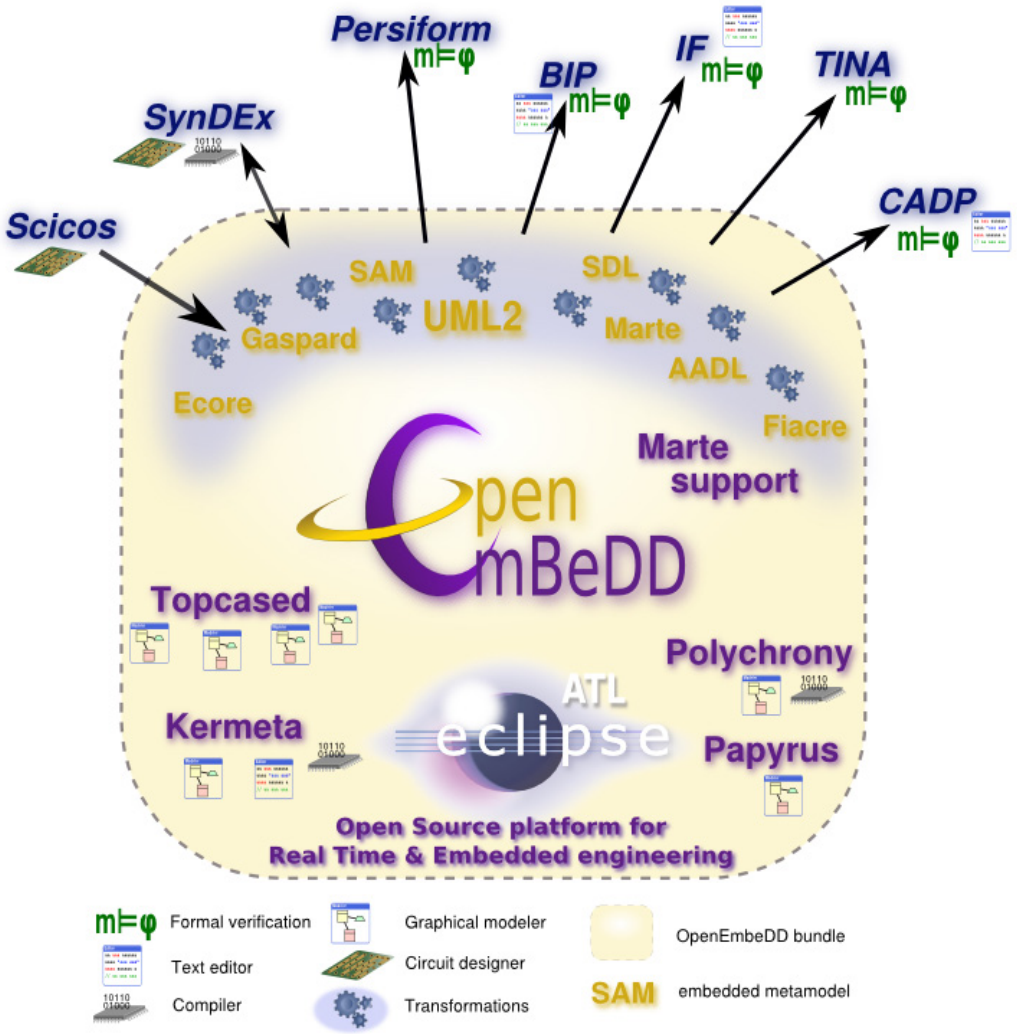


Figure 2.4-4 OpenEmBeDD platform (infrastructure)

Code generation from and analysis of AADL specifications has been addressed in several projects. This year, work has been carried out in the SPICES ITEA project (http://www.spices-itea.org/public/news.php) for *Support for Predictable Integration of mission Critical Embedded Systems* with Artist partners CEA, Leuven, Cantabria and VERIMAG and in the before mentioned OpenEmBeDD project which has many common partners with SPICES and TopCased. The objective is to 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 [CRBS08].

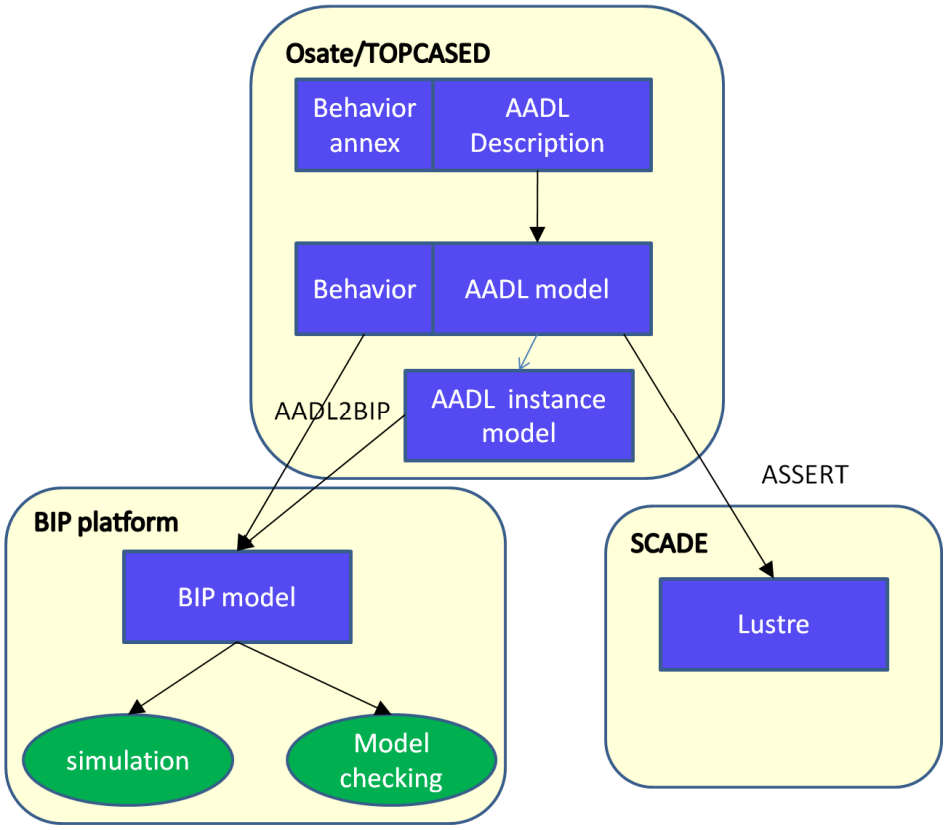


Figure 2.4-5 Validation of AADL specification in BIP and Lustre

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

The collaboration between VERIMAG and FTRD on the *compilation of BIP component systems to THINK* takes place within the Minalogic Regional competivity pole effort. The goal of this joint effort is to simultaneously derive the executable embedded code of an OS and its behavioural model for analysis and verification. Today a transformation exists from BIP (used for analysis) to THINK.

During the years 3 and 4 we have defined a new language for developing component-based embedded systems. This language, called Buzz, tries to combine two complementary component frameworks: BIP and THINK. Buzz can be seen as a THINK ADL (Architecture Description langage) front end as in Buzz, THINK components and bindings are decorated with tags defining (implicitly) their behavioural semantics. . Buzz contributes to offer a more familiar IDE to "ordinary" embedded system developers than direct BIP notation. It can be seen as a pivot langage that bridges the gap between regular OS oriented dynamic behavioural features (such as threads, events and so on…) and BIP primitives.

In Buzz, components can be either active or passive depending whether they embed a thread or not. An active component can be seen as the server of the methods in its provided interface. In Buzz, any active component services its provided method on a run-to-completion basis: only one method execution is running at a time. Bindings can be either *synchronous* (as regular method invocation) or *asynchronous* (caller does not wait for the invoked method to return). Multiple method invocation (*broadcast*) is also supported as well as joint method invocation.

Thus, Buzz has been defined in such a way that most popular parallel programming styles for embedded system can be easily mapped into Buzz: Multi-threading, event-orientation, compositions of automata, etc.

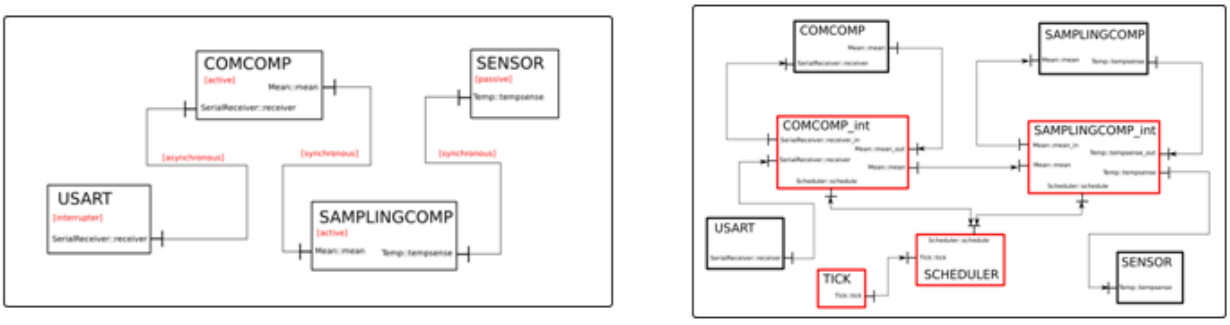


Figure 2.4-6: BUZZ Wireless sensor node software architecture with (red) tags that specify system behaviour; and the corresponding THINK software architecture

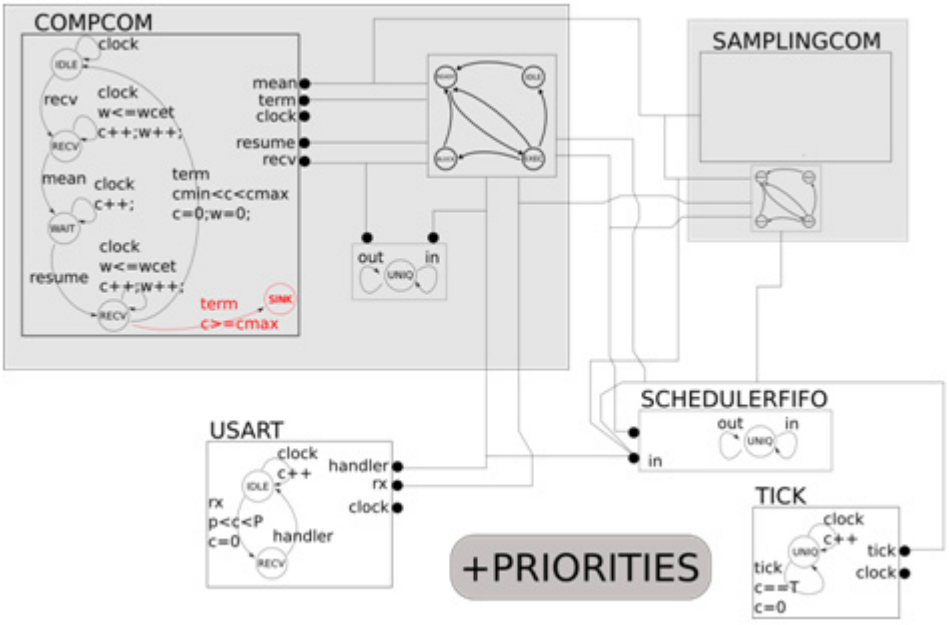


Figure 2.4-7: automatically produced BIP model corresponding to the original WSN node BUZZ architecture

Buzz comes with a compiler that allows both the generation of a Think architecture for the software execution on the embedded platform and the generation of a BIP model for verification and analysis of the running system. As BIP is component-based, it has been possible to associate a BIP component of the behavioural model with a Think component of the running code. Moreover the back-end of the *Nuptse ADL* compiler of the Think tool chain has been modified in order to generate directly the BIP model from the Think architecture (the original Nuptse Compiler generates C files from the System ADL source and Component functional codes). This feature guarantees the truthfulness of the resulting behavioural model with respect to the running code which is the key property for code validation.

We illustrate the method by running sensor node software on an 8 bits micro-controller AVR Atméga 2561 and automatically verifying timing constraints.

The Buzz project is to be pursued in the MIND project of the Minalogic Regional competivity pole. Other works carried out within Orange lab/FT R&D concerning distribution, protection and access control in component based archicture could also enrich Buzz notation, allowing Buzz

to take other aspects of embedded system design. A webpage will be available soon at http://think.objectweb.org.

In the previous years, the Inria team has developed a tool chain to support a complete software design process for real-time components, from service specifications down to executable software components in Java or C.

This tool chain named Thot includes tools from other Artist2 partners, e.g. the IF and Kronos tools from Verimag and the Giotto runtime from EPFL. The tool chain has been completed in February 2008. The principles, architecture and capabilities are documented in [SBDP07] and in Sebastien Saudrais' PhD thesis [Sau07].

In 2008 the main efforts on this tool have been assigned to dissemination within a larger community of researchers, mainly through talks and participation in other national or international projects.

The AMAES project (http://www-verimag.imag.fr/~krichen/AMAES/) aims at more dependable software architectures for autonomous robots. In this context, we use BIP for modelling software for autonomous robots. 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.

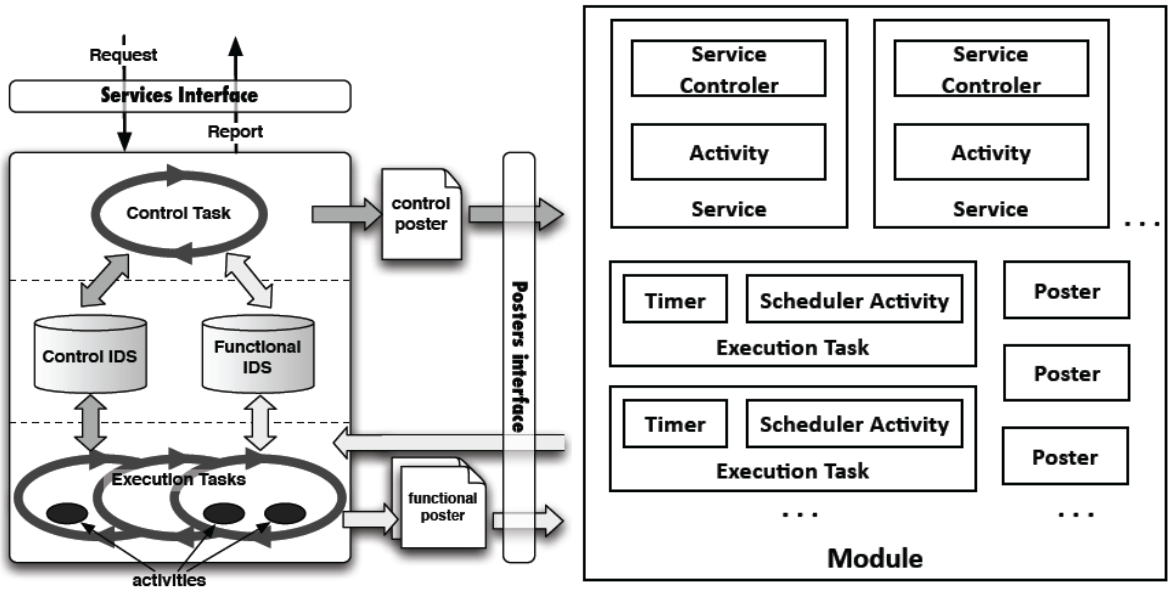


Figure 2.4-8: A module of the Genom architecture and its componentisation in BIP

We proposed a modelling paradigm based on BIP to enforce the separation between coordination and computation (execution of sequential code). This year, we have contributed to the evolution of the LAAS Architecture for Autonomous System and its tool GenoM using BIP. In a case study, we have shown how we are able to seamlessly integrate BIP into the preexisting methodology. We have componentized the functional level of a robot, synthesed an execution controller and validated essential safety properties using the DL-finder tool (see below). 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).

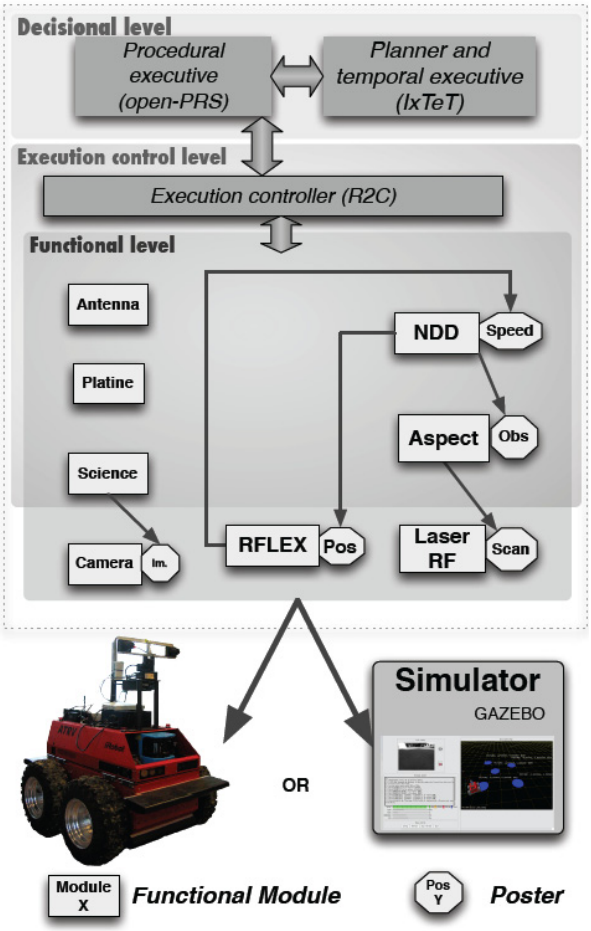


Figure 2.4-9: instance of the Genom architecture for the DALA robot

Within the context of the MemVaTEx French project, CEA-LIST has defined a MARTE extension to deal with requirements and traceability issues. This latter is compatible with MARTE, SysML and EAST-ADL2, and a plug-in has been implementyed within the open source tool for UML2 Papyrus in order to support these extensions.

Topic 3: Platform for the analysis of performance critical systems

This platform was recently developed in the context of the French *Persiform* (http://www-persiform.imag.fr) project (ARTIST partners are FTRD, INRIA and VERIMAG; additional partners were INT who provided expertise on performance models and Orpheus, an industrial user). The platform supports the integration of performance evaluation in the design activity by connecting a well-known UML modelling tool, Rational Software Modeler (RSM), to a commercial performance simulator, HyPerformix Workbench.

RSM has been extended for that purpose with an UML profile focusing on performance data in information systems. The connection between the tools consists in a sequence of model transformations involving an intermediate language with clear operational semantics. This rich intermediate language is based on coloured Petri Nets and Queueing Networks. It allows deriving performance models from complex UML designs with reasonable trust. In addition, a successful experiment has been carried out on the support for functional analysis, by transformation of intermediate models into Promela specifications. Almost all model transformations are implemented in ATL.

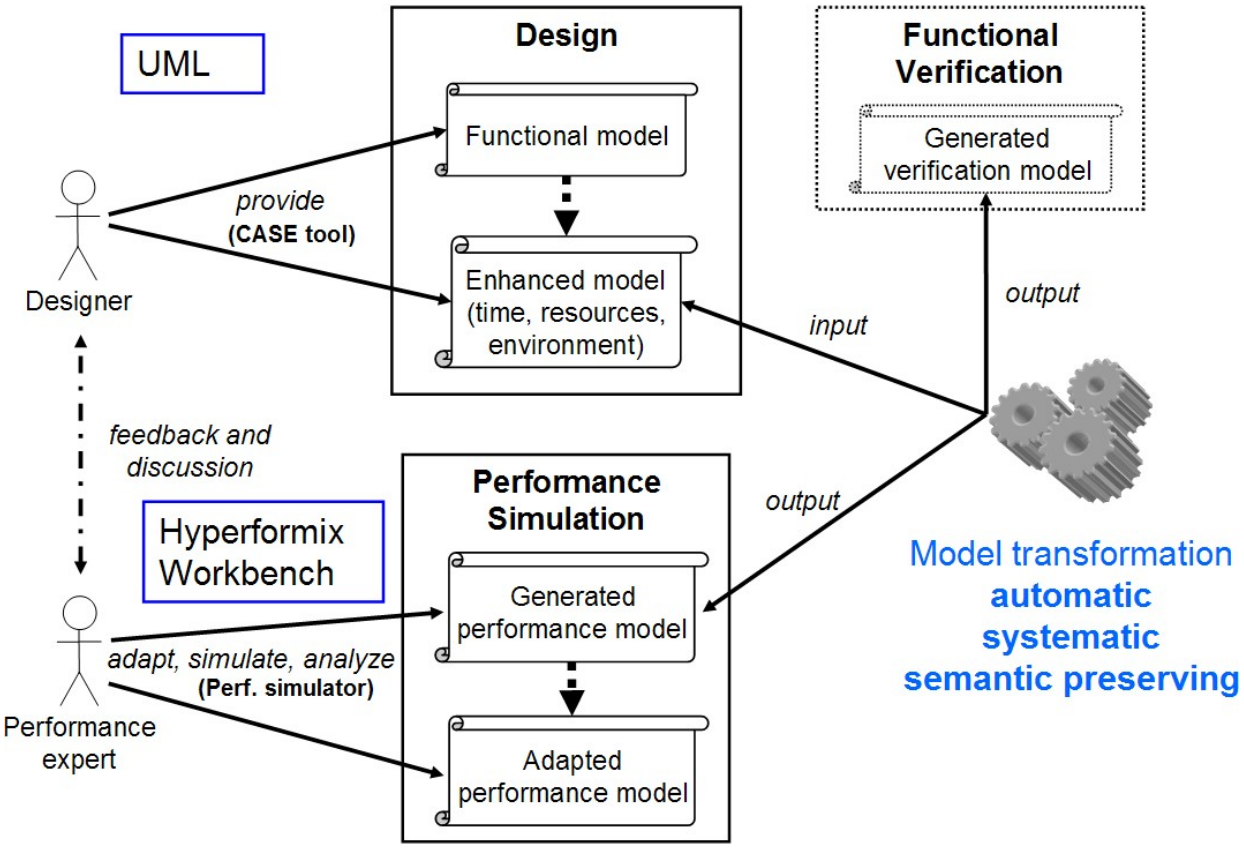


Figure 2.4-10: Persiform methodology: model transformations

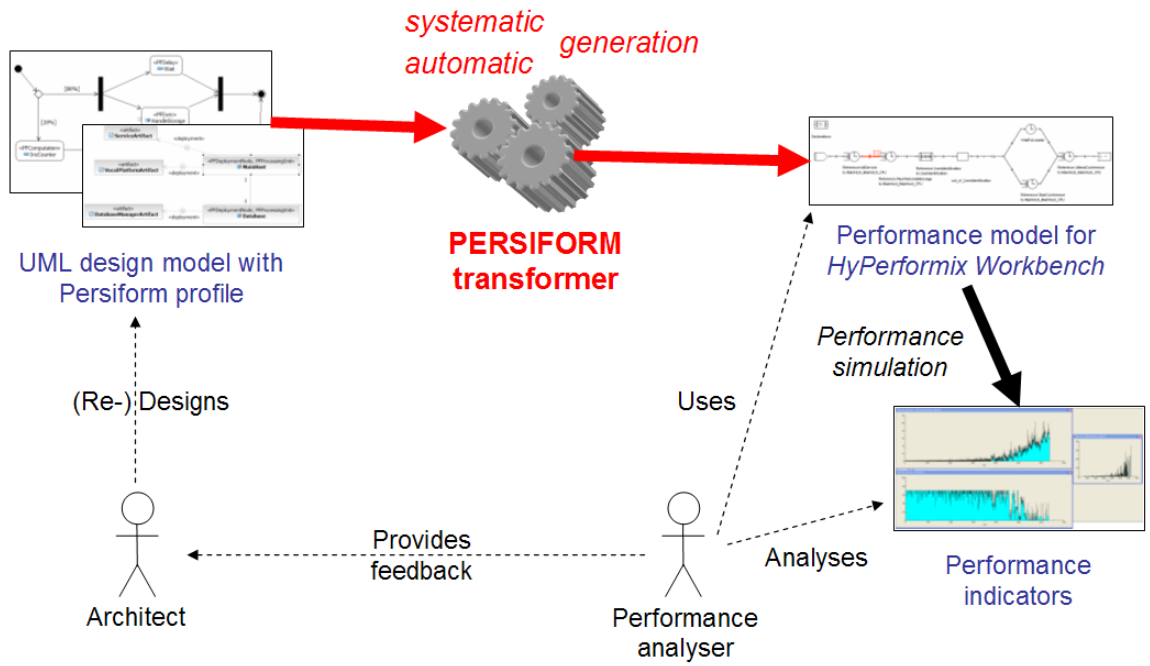


Figure 2.4-11 Persiform methodology: tool usage

The platform has been validated on several case studies from the industry partners. The results on the tool chain and the methodology are published in a technical report [CGM07] and they were also demonstrated at ICSE 2008 [CWG08].

The Persiform platform is being reused in the OpenEmbedd project. It is being extended to cover a different type of systems via the integration of an additional front-end modelling language. Concretely, avionic systems based on ARINC infrastructures are being modelled by Thalès in UML with the MARTE profile.

The collaboration between Thalès and VERIMAG has first focused on defining which Workbench models are expected as outputs from these MARTE models. This task involves two aspects. The first one consists in interpreting the ARINC-653 specification so as to propose an executable performance model of the ARINC infrastructure including its 3-layered scheduling system. The second aspect relates to the selection of the right level of abstraction in every part of the model to allow performance experts to obtain useful, understandable performance results. These results mainly concern processes meeting their deadlines. This task has made significant progress this year.

The next task consists in implementing a model transformation from the relevan MARTE subset to one of the intermediate languages of the Persiform platform. In this transformation, the general principles of ARINC systems will be encoded in a library or, equivalently, in a constant transformation module. The data specific to the system being modelled will be extracted from the MARTE model. Model transformations will be implemented in ATL.

We recently started to work on another performance related topic: ***simulation of wireless sensor networks*** for the purpose of estimating network lifetime [DB*07], [MSZ07]. Network lifetime is determined by the energy consumption due to commutations in individual nodes and communication activities. This work is done in the French ARESA project (http://www.citi.insa-lyon.fr/project/aresa/), with the aim to facilitate research, developments and commercialization of wireless sensor networks (WSNs). Artist partners are Verimag and FTRD. Large scale deployement of a WSN still faces a number of challenging problems. In particular, lowering energy consumption is a critical issue as long-term network lifetimes (more than 10 years) must be guaranteed. Hence, every layer of a WSN application (node hardware, communication protocols, auto-organization mechanisms) should be specifically designed to run in an utmost energy efficient manner.

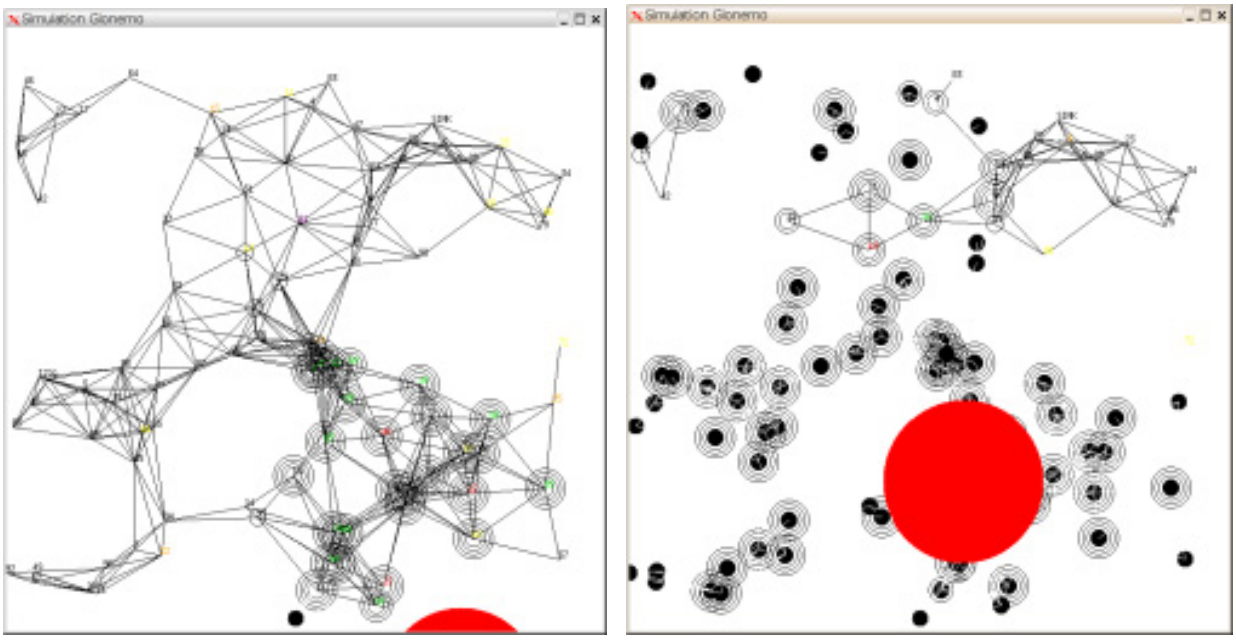


Figure 2.4-12 example of simulation with Glonemo

The color of the nodes indicates in which mode (sleep, idle,...) is their radio. A node is represented by a black disk when its battery ran out of energy. The number of circles corresponds to the number of collisions suffered by the sensor. The cloud (particular environment) is the red disk.

The aim of our work within ARESA is to address the problem of developing accurate prototypes of WSNs, that can be formaly analyzed, and that can be transformed by dedicated abstraction mechanisms, able to simplify the model complexity while preserving (or at least over-approximating) the energy consumption. Using the ARESA techniques, we will explore new event-driven and asynchronous software and hardware architectures, tailored to extremely low power consumptions; propose new communication and organization protocols, optimized in terms of energy consumption and robustness and study new network structures which facilitate auto-organization.

During the initial part of the project a simulator called Glonemo (for "global network modelling") has been developped within VERIMAG (http://www-verimag.imag.fr/~samper/Glonemo/). It allows simulating networks of up to several hundred thousands nodes, on typical monitoring application, running models of existing communication protcols (for the MAC and routing levels), while precisely evaluating the energy consumption of each node. In particular this simulator allows to take into account models of the external environment (providing the sensor inputs), which happen to be particularly important to correctly estimate energy consumptions (and hence network lifetime). These features outperform the ones proposed by most of the existing simulation tools.

During the past year, the ***Glonemo*** simulator has been enhanced to allow modelling and simulation of more complex protocols. In particular, we are currently working on a new protocol[1] combining the MAC and routing layers and which uses vitual sensor coordinates computations, without requiring a precise (and expensive) node location mechanism. The purpose of this work is twofold: first, to provide a detailed description of the protocol that would be suitable for implementation; second, to evaluate this protocol with respect to more classical static routing schemes from the energy comsumption point of view. Finally, we also proposed a theoretical framework to perform component-based abstractions of a WSN while preserving (over-)approximations of energy consumptions. This framework allows the verification of network lifetime lower bounds.

Two industrial partners are involved in the ARESA project (Orange Labs and Coronis), and a part of their activity is to develop new energy efficient solutions for wireless infrastructures (from the nodes architecture to the software communication stacks). A dedicated and global simulation tool like Glonemo will help them to early evaluate a given design, before any concrete deployment.

Topic 4: Platform for the certification of smart-card applications

The work on this platform continues to be supported by collaboration between CEA and VERIMAG on functional validation of critical applications on smart cards. This work is carried out in the context of a national project, *EDEN 2* (http://www.eden-rntl.org/), which pursues the work of EDEN, in order to reach a consolidated implementation for industrial exploitation.

We already had defined a methodology for the certification of smart-applications according to the International standard known as the *Comon Criteria* (CC) for security, and developed several tools which aim at helping developers of JavaCard applications to produce the evidences requested for such a certification. Some advances have also been made on the automatic generation of test objectives. CEA has worked on test case concretisation along the system specification refinement process and on unitary test derivation of components

[1] *On Using Virtual Coordinates for Routing in the Context of Wireless Sensor Networks, Thomas Watteyne, David Simplot-Ryl, Isabelle Augé-Blum, Mischa Dohler. 18th IEEE Int. Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07), Athens, September 2007*

according the respective concrete use of each component inside the system ([FGG07], [GGRT06]).

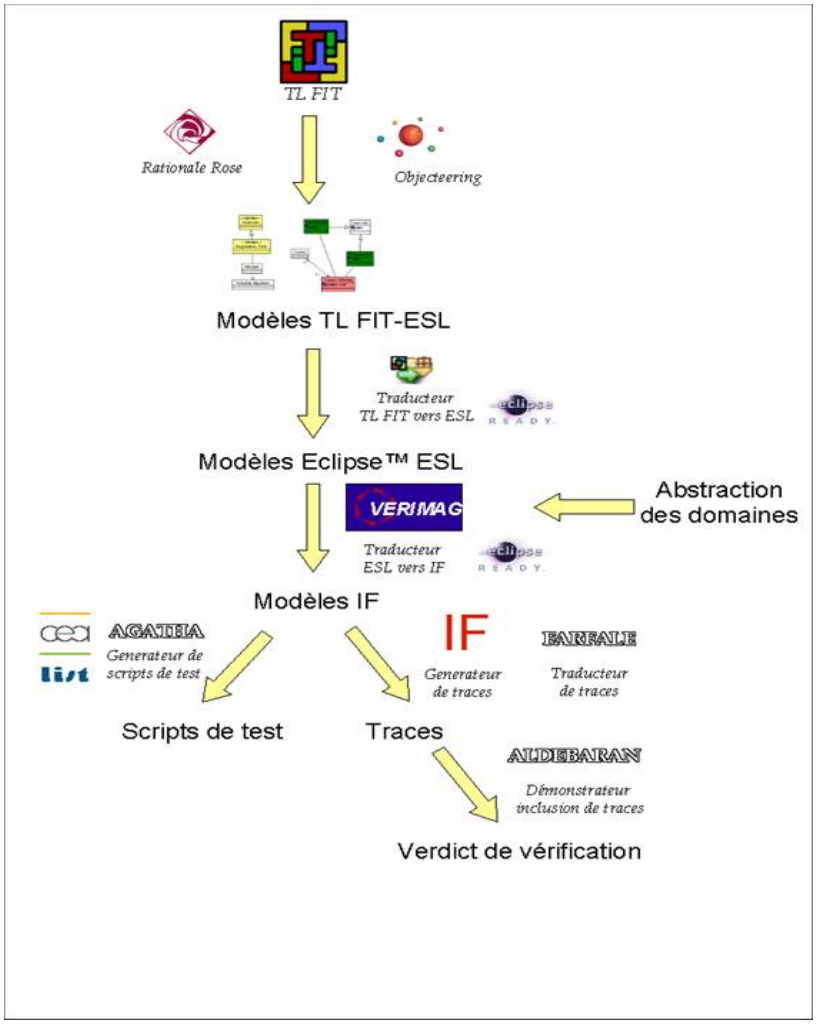


Figure 2.4-13: Functional flow of the Eden platform

The assets of the EDEN projet are a methology up to the CC requirement, a user-friendly language (a Java-like syntax) for describing security policies as monitors, and a large amount of automation of the certification and verification tasks. The ultimate goal is that the methodology doesn't require the developpers to be experts in formal methods.

During the last year, the project encountered difficulties in hiring development engineers and the two main developers quitted for better paid positions and after 6 months of delay. This led to a slight redefinition of the project objectives by focusing mainly on methodology for certification and reducing the development task.

The trend in certification -- initiated by works on proof-carrying code, is the generation of certificates in the form of a proof that can be submitted to trustable proof-checkers. On advices of the french CC committee (DCSSI), we oriented our researches on the definition of "Convincing proofs for program certification" that was presented in the 1st workshop on Certification of Safety-Critical Software Controlled Systems (SafeCert'08). We proposed an evaluation process that increases confidence in certificates by involving the evaluators in the design of a simple proof-checker that is finally used to validate the generated certificate [GP08]. As as continuation, experimentations are conducted on a concrete example: the generation of proofs of invariant properties for IF/BIP models (IF/BIP are used to represent the

security model and the semantic of Java Card programs); the certificate are produced in the format of the COQ proof-environment.

These results serve as building blocks for the proof of conformance (RCR) between the security policy model and the semantic model of the application (developped in Java Card). Establishing the correspondance between models is the backbone of the Common Criteria methodology of certification. At the highest level of assurance (EAL7+) evaluators expect a full formal argument proving that the implementation conforms to the security policy. Very few certifications were done at that level of formalization and each of them provided its own interpretation of the CC requirement. Up to day no conclusive framework as emerged for EAL7+ and the methodology is still lacking a well defined interpretation RCR [NP09], [NP09a].

Note that recent improvments in SMT solvers (eg., Yices, Z3) show that they can be used to prove symbolic properties of systems. EDEN then evolves towards the generation of formal proofs of the conformance of an application to a security policy. Instead of checking a simplified finite model, symbolic techniques can prove properties of the actual model without restricting assumptions. Symbolic verification requires more development but provide results that can serve as formal certificates.

The Eden2 project proposes a precise and formal definition of security conformance relation which is formulated in a general framework of inter-program properties. This theory has been presented at COCV'08, focusing on its ability to prove the transfer of properties through program translation [NV08]. A publication is in preparation that focuses on its application to certification of smart card applications.

Topic 5: Transversal validation technology for platforms

The development of new verification techniques is not the primary goal of the component platform (this topic is covered by the Verification cluster and platform activities). We report here on some new validation tool developments that are intended to be integrated into one or more of the platforms. Some of this work is also reported in the validation platform.

In Uppsala, the main effort has been on validation techniques for timed systems, in particular resource-related analysis to cover a broad range of resources such as processors, buffers and memory blocks etc.

To extend the TIMES tool to handle multi-processor scheduling and analysis, Uppsala has studied multiprocessor scheduling in different settings [KSY07, GYGY08]. In a recent work [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.

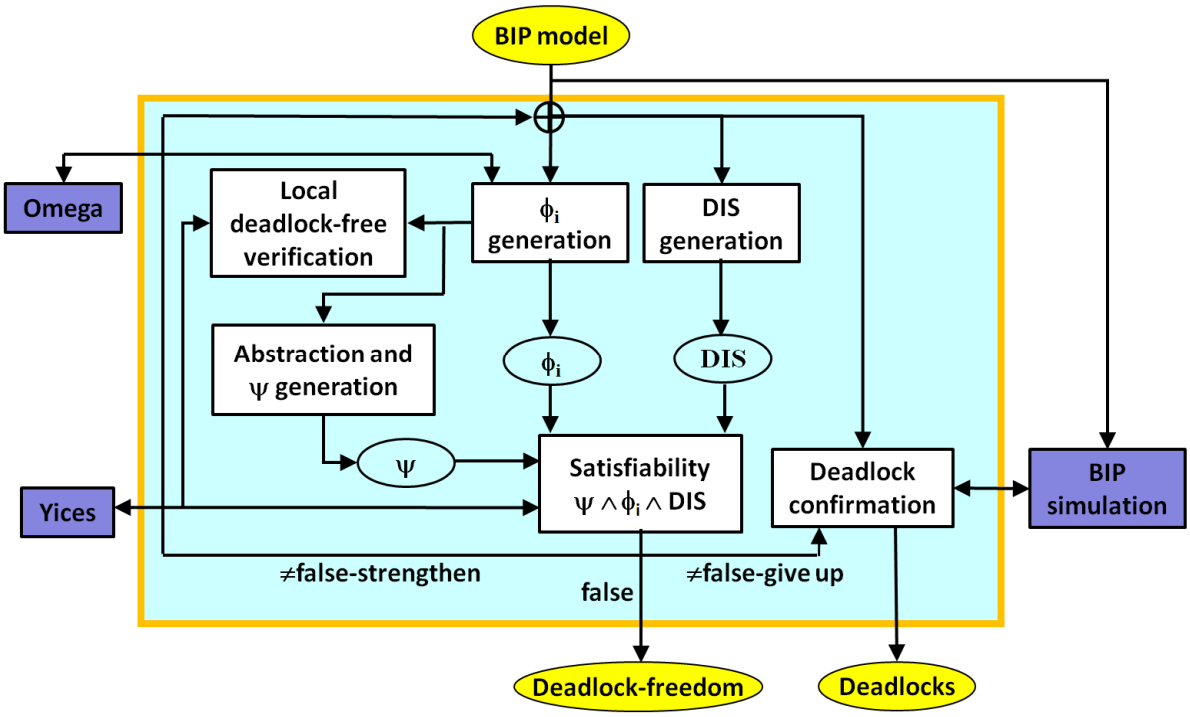
Cyclic dependencies in component-based real-time systems have not been well-understood in the context of modular performance analysis. In a joint work [JPTY08] with ETH, Zurich, Uppsala has developed a general operational semantics underlying the Real-Time Calculus, and use this to show that the behavior 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 [KMY07], 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 www.timestool.com/cats.

CEA has started to adapt *the symbolic exection kernel, Agatha,* to exploit modelling formalisms used in Automotive domain, this of Statmate Statecharts, VHDL/AMS, Matlab/Simulink (restricted to discrete part). This has been supported by three projects of Num@tec Automotive / System@tic Paris Région: HeCoSim – http://www.projet-hecosim.org; SysPEO; EDONA – http://www.edona.fr. This will be used as basis to provide a prototype for component-based test generation from heterogenous specifications of systems and its evaluation in automotive domain. (http://www-list.cea.fr/labos/fr/LLSP/agatha/AGATHA_publications.htm)

Correctness-by-construction: as planned, Verimag has worked on The *BIP verification engine* (http://www-verimag.imag.fr/~async/BIP/bip.html) which does a compositional deadlock detection/verification. The methods that we started to develop have been significantly improved and implemented in the DeadlockFinder tool by combining structural analysis for component behaviours with structural analysis of connectors.



2.4-14 Functional view of the D-finder tool

The D-Finder toolset allows deadlock verification using structural analysis. It takes as input a BIP model and computes component invariants CI. This step may require quantifier elimination using the tool Omega. Then, it checks for deadlock-freedom based on the set of computed component invariants: it computes an abstraction of the model derived from the invariants CI, and it then computes interaction invariants II for this abstraction.

Then, it checksthe satisfiability of the conjunction of II and CI and the predicate DIS (characterizing the set of the states in which no interaction is enabled) using the satisfiability checker Yices. If this conjunction is unsatisfiable, then there is no deadlock. Else, D-finder

either generates stronger component and interaction invariants, or tries to confirm the detected deadlocks by using reachability analysis techniques [BBSN08].

OFFIS has worked on the combination of analytical methods and computational requirement specification in the area of real-time analysis of distributed embedded systems. In the previous period we started to define a sufficient subset of timed automata templates, so-called Cyclic Timed Automata (CTA), that are used to simulated the temporal behaviour as it is observed by applying traditional scheduling analysis techniques. Meanwhile the equivalence of CTA classes and event stream based characterizations of temporal worst case behaviour (which in fact is the basis of traditional scheduling theory) was proven [SDM07]. This new technique allows us to efficiently verify temporal properties given as timed automata, e.g. derived from contracts used in the SPEEDS project, against implementations of distributed systems on a layer of abstraction which is similar to AUTOSAR. More complex properties beyond simple deadlines can be verified, for instance whether an implementation guarantees a given order of a set of signals, the so-called coordination layer of a systems behaviour. While properties of the coordination layer are frequently used, they usually are specified in terms of sequence diagrams. Within the project COMBEST we defined a translation of a specific class of sequence diagrams, Life Sequence Charts, to timed automata [DSW08].

The implementation of these work packages are done in the ORCA framework. Experiments on industrial use cases have shown that the CTA framework is a powerful verification engine, but at some point it suffers from being only temporal, e.g. often the current state of system modes directly influence which timing properties the implementation has to guarantee. Hence we started working on the combination of the temporal and the functional viewpoint, by adapting the CTAs towards functional aspects on the one hand and extending traditional scheduling analysis towards functional properties [M08] on the other hand.

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

Figure 2.4-15 How the COSI framework has been used to generate specific synthesis tools

In collaboration with UC Berkeley and Columbia University, PARADES helped delivering the first release of COSI (Communication Synthesis Infrastructure), a software framework to interconnect infrastructure synthesis that is publicly available.

The framework allows developing specialized flows and tools for communication synthesis as exemplified by the internal release of COSI-NOC (Communication Synthesis Infrastructure for Network-on-Chips) [PCSV1], a software toolkit for the automatic synthesis of synchronous networks-on-chip based on the platform-based design paradigm, and by COSI-BAD, for building automation design [PCSV2].

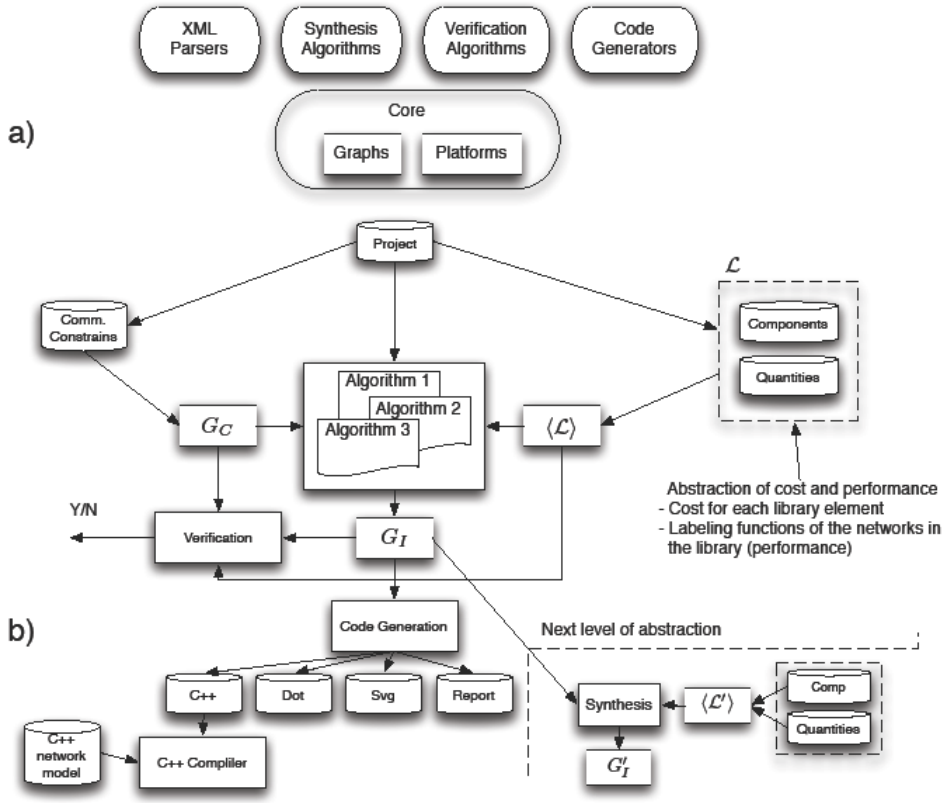


Figure 2.4-16 The COSI Platform-Based Design-like structure

2.4.2 Individual Publications Resulting from these Achievements

This section contains only individual publications; joint publications are listed in Section 2.3.4.

Publications by **CEA**

Year 3

[CMTG07a] A. Cuccuru, C. Mraidha, F. Terrier, S. Gérard. Métamodèles et points de variation sémantique. Sémo'07 (workshop IDM), 2007

[CMTG07b] A. Cuccuru, C. Mraidha, F. Terrier, S. Gérard. Enhancing UML Extensions with Operational Semantics - - Behaviored Profiles with Templates. *MoDELS 07*, 2007.

[CMTG07c] A. Cuccuru, C. Mraidha, F. Terrier, S. Gérard. Templatable Metamodels for Semantic Variation Points. *European Conference on Model Driven Architecture - Foundations and Applications (ECMDA-FA)*, 2007

[FGG07] Alain Faivre, Christophe Gaston and Pascale Le Gall, Symbolic Model based Testing for Component oriented Systems, 19th International Conference TestCom (TestCom 2007), Springer Verlag. June 2007, Estonia

[GGRT06] Christophe Gaston, Pascale Le Gall, Nicolas rapin and Assia Touil, Symbolic Execution Techniques for test Purpose Definition , 18th International Conference TestCom (TestCom 2006), Springer Verlag. May 2006, USA.

[LETG07] *François Lagarde, Huáscar Espinoza, François Terrier and Sébastien Gérard.* Improving UML Profile Design Practices by Leveraging Conceptual Domain Models. International Conference on Automated Software Engineering (ASE)*, november 2007 (*short paper*)*

[LTAG07] *Lagarde François, Terrier François, André Charles, Gérard Sébastien*, "Constraints modeling for ²(profiled) UML models.", 3rd European Conference on Model Driven Architecture - Foundations and Applications (ECMDA-FA - 2007), Haifa, Israël, June 2007

[LTG07] *Lagarde François, Terrier François, Gérard Sébastien*, "Extending OCL to ensure model transformations", ER 2007 Workshop Proceedings, 3rd International Workshop on Foundations and Practices of UML (FP-UML - 2007), Auckland, Nouvelle-Zélande, 2007

[TGDT07] *Frédéric Thomas, Sébastien Gérard, Jérôme Delatour and Francois Terrier.* Software Real-Time Resource Modeling*. In Forum on Specification and Design Languages (FDL) 2007, Barcelona, Spain. ECSI, September 2007.*

[TETG07] *Frédéric Thomas, Huascar Espinoza, Safouan Taha and Sébastien Gérard.* MARTE : le futur standard OMG pour le dévéloppement dirigée par les modèles des systèmes embarqués temps réel*. In Génie Logiciel, pages 27-31, Mars 2007.*

[TG06] François Terrier, Sébastien Gérard . Model-driven engineering and prototyping of real time embedded applications. in From Model-Driven Design to Ressource Management for Distributed Embedded Systems. Kleinjobann, Lisa Kleinjobann, Ricardo J. Machado, Carlos Pereira, P.S. Tbiagarajan, October 2006.

Year 4

[CMTG07c] *A . Cuccuru, C . Mraidha, F . Terrier, S . Gérard*. Enhancing UML Extensions with Operational Semantics - - Behaviored Profiles with Templates. *MoDELS 07*, Oct. 2007.

[E07] *H. Espinoza*, "An Integrated Model-Driven Framework for Specifying and Analyzing Non-Functional Properties of Real-Time Systems", PhD Thesis (English), University of Evry, France. September 2007

[ESG08] *H. Espinoza, D. Servat, and S. Gérard*, “Leveraging Analysis-Aided Design Decision Knowledge in UML-Based Development of Embedded Systems”, SHARK Workshop at ICSE’08, Leipzig, May 2008.

[FGGT08] *Alain Faivre, Christophe Gaston, Pascale Le Gall, Assia Touil*, "Test Purpose Concretization through Symbolic Action Refinement" - TestCom/FATES 2008, Tokyo, Japan – LNCS, 2008

[HLRG08] *B. Hamid, A. Lanusse, A.Radermacher, S. Gérard*, "Designing Reconfigurable Component Systems with a Model Based Approach", Workshop on Adaptive and Reconfigurable Embedded Systems, APRES'08, 2008

[HRVLG08] *B. Hamid, A. Radermacher, P. Vanuxeem, A. Lanusse, S. Gerard*, "A fault-tolerance framework for distributed component systems", Proceedings of the 34th Euromicro SEAA conference, IEEE CS, 84-91, 2008

[HRLJGT08] *B. Hamid, A. Radermacher, A. Lanusse, C. Jouvray, S. Gerard and F. Terrier*, "Designing fault-tolerant component based applications with a model driven approach", IFIP Workshop on Software Technologies for Future Embedded and Ubiquitous Systems (SEUS 2008)}, Springer, Lecture Notes in Computer Science 5287, 9-20, 2008

[LETG07] *François Lagarde, Huáscar Espinoza, François Terrier and Sébastien Gérard.* Improving UML Profile Design Practices by Leveraging Conceptual Domain Models. International Conference on Automated Software Engineering (ASE)*, november 2007.*

[MGC08] *Stephane Maag, Cyril Grepet, Ana Cavalli*, "A formal validation methodology for MANET routing protocols based on nodes' self similarity", Computer Communications Journal, Vol.31:4, pp. 827-841, 2008

[MTJTG08] *Chokri Mraidha, Yann Tanguy, Christophe Jouvray, François Terrier, Sébastien Gérard*, "An execution framework for MARTE-based models", Joint 13th IEEE ICECCS & 15th IEEE ECBS (UML&AADL - 2008), Belfast, Irlande, 2008

[TRGD07] *Taha S., Radermacher A., Gerard.S, Dekeyser J-L*, "An Open Framework for Detailed Hardware Modeling", SIES'2007, IEEE 2nd International Symposium on Industrial Embedded Systems, Lisbonne, Portugal, 2007

[TSG08] *Tessier P., Servat D., Gerard S.*, "Variability Management on Behavioral Models", 2nd International Workshop on Variability Modelling of Software-intensive Systems (VaMoS - 2008), Essen, Allemagne, 22, pp. 121-131, 2008

[TDGBT07] *Thomas Frédéric, Delatour Jérôme, Gérard Sébastien, Brun Matthias, Terrier François*, "Contribution à la modélisation explicite des plates-formes d'exécution pour l'IDM", TSI - L'Objet, 0291-7335, 2007

[TGDT07] *Thomas Frédéric, Gérard Sébastien, Delatour Jérôme, Terrier François*, "Software Real-time Resource Modeling", FORUM on Specification & Design Languages with Industrial Workshops, Forum on Specification and Design Languages (FDL - 2007), Barcelone, Espagne, ECSI, pp. 231-236, 2007

Publications by **FTRD**

[SLJ*07] Anshuman Saxena, Marc Lacoste, Tahar Jarboui, Ulf Lücking, and Bernd Steinke. A Software Framework for Autonomic Security in Pervasive Environments. Information Systems Security, LNCS 4812. 2007

Publications by **INRIA**

Year 3

[SBP06] Sébastien Saudrais, Olivier Barais, and Noël Plouzeau. -- Composants avec propriétés temporelles. -- In Proceedings of the CAL 2006, Nantes, France, 2006.

[SBD06] Sébastien Saudrais, Olivier Barais, and Laurence Duchien. -- Using model-driven engineering to generate qos monitors from a formal specification. -- In Proceedings of the Aquserm 2006, Hong Kong, China, October 2006.

[SPB07] Integration of Time Issues into Component-Based Applications , Sébastien Saudrais, Noel Plouzeau and Olivier Barais, Proceedings of the Component Based Software Engineering Conference (CBSE'07), July 2007, p. 169-184.

Year 4

[SBDP07] Sébastien Saudrais, Olivier Barais, Laurence Duchien, Noël Plouzeau: "From formal specifications to QoS monitors", in Journal of Object Technology, vol. 6, no. 11, Special Issue on Advances in Quality of Service Management, December 2007, pages 1-20, http://www.jot.fm/issues/issue 2007_12/article1/

[Sau07] Sebastien Saudrais, "Qualite de service temporelle pour composants logiciels", PhD thesis Université de Rennes 1, December 5th 2007, in French.

Publications by **OFFIS**

Year 3

[DM07] W. Damm and A. Metzner. A Design Methodology for Distributed Real-Time Automotive Applications. In Next Generation Design and Verification Methodologies for Distributed Embedded Control Systems, pp. 157-174. Springer LNCS. ISBN 978-1-4020-6253-7, 2007

[DD*07] W. Damm, S. Disch, H. Hungar, J. Pang, F. Pigorsch, C. Scholl, U. Waldmann, B. Wirtz. Automatic verification of hybrid systems with large discrete state space. In: Proceedings of the 4th International Symposium on Automated Technology for Verification and Analysis, Lecture Notes in Computer Science 4218, 2006

[HRW07] H. Hungar, O. Robbe, B. Wirtz. Safe-UML - Restricting UML}for the development of safety-critical systems. In: Proc. FORMS/FORMAT 2007

[KD*07] S. Kupferschmid, K. Dräger, J. Hoffmann, B. Finkbeiner, H. Dierks, A. Podelski, G. Behrmann; Uppaal/DMC -- Abstraction-based Heuristics for Directed Model Checking; Tools and Algorithms for the Construction and Analysis of Systems (TACAS) 2007;679--682; LNCS 4424; Springer

[KD*07b] S. Kupferschmid, K. Dräger, J. Hoffmann, B. Finkbeiner, H. Dierks, A. Podelski, G. Behrmann; Uppaal/DMC -- Abstraction-based Heuristics for Directed Model Checking; Tools and Algorithms for the Construction and Analysis of Systems (TACAS) 2007;679--682; LNCS 4424; Springer

[Seg07] M. Segelken. Abstraction and Counterexample-Guided Construction of ω-Automata for Model Checking of Step-Discrete Linear Hybrid Models. In: Proceedings CAV 2007, LNCS 4590, pages 433-448, 2007.

[SDM07] I. Stierand, H. Dierks, and A. Metzner. Combining timed automata based formal specifications and real-time scheduling analysis. AVACS Technical Report No. 18, SFB/TR 14 AVACS, June 2007. ISSN: 1860-9821

Year 4

[DKL07] H. Dierks, S. Kupferschmid, K.G. Larsen. *Automatic Abstraction Refinement for Timed Automata*. In J.-F. Raskin, P. S. Thiagarajan (Edts.) Proceedings Formal Modeling and Analysis of Timed Systems on the 5th International Conference, FORMATS 2007, Lecture Notes in Computer Science 4763, Springer-Verlag, S. 114-129, 2007

[DSW08] H. Dierks, I. Stierand, B. Westphal. The Power of Uppaal – Model Checking Live Sequence Charts. Technical Report (to appear) 2008

[M08] Alexander Metzner. Analysis of Distributed Real-Time Systems under Functional Constraints. In: Proceedings of the 13th IEEE International Conference on Emerging Technologies and Factory Automation, 2008.

Publications by **PARADES**

Year 3

[DDM+] Abhijit Davare, Douglas Densmore, Trevor Meyerowitz, Alessandro Pinto, Alberto Sangiovanni-Vincentelli, Guang Yang, Haibo Zeng and Qi Zhu, A Next-Generation Framework for Platform-Based Design, in Proceedings of Design and Verification Conference (DVCon'07), San Jose, CA, February, 2007.

[DZD+] Abhijit Davare, Qi Zhu, Marco Di Natale, Claudio Pinello, Sri Kanajan, and Alberto L. Sangiovanni-Vincentelli. Period optimization for hard real-time distributed automotive systems. In DAC, pages 278–283. IEEE, 2007.

[DZP+] Marco Di Natale, Wei Zheng, C. Pinello, P. Giusto, and A. Sangiovanni-Vincentelli. Optimizing end-to-end latencies by adaptation of the activation events in distributed automotive systems. In RTAS 2007, Washington, USA, April 2007.

[SV] A. Sangiovanni-Vincentelli, Quo Vadis, SLD? Reasoning About the Trends and Challenges of System Level Design, Proceedings of the IEEE, Vol. 95, N. 3, pp. 467-506, March 2007.

[YHC+] G. Yang, H. Hsieh, X. Chen, F. Balarin and A. L. Sangiovanni-Vincentelli, Constraints Assisted Modeling and Validation in Metropolis Framework, in Proceedings of The 40th Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, California, November, 2006.

[ZDP+] Wei Zheng, M. Di Natale, C. Pinello, P. Giusto, and A. Sangiovanni-Vincentelli. Synthesis of task and message activation models in real-time distributed automotive systems. In 2007 IEEE/ACM Design Automation and Test in Europe Conference and Exposition, DATE07, Nice, France, April 2007.

Year 4

[PCSV1] A. Pinto, L.P. Carloni, and A. Sangiovanni-Vincentelli . COSI: A Framework for the Design of Interconnection Networks, IEEE Design & Test of Computers. Vol. 25, No. 5, September/October 2008.

[PCS] C. Pinello, L.P. Carloni, and A.L. Sangiovanni-Vincentelli , Fault-Tolerant Distributed Deployment of Embedded Control Software IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. Vol. 27, No. 5, May 2008.

[PCSV2] A. Pinto, L.P. Carloni, and A.L. Sangiovanni-Vincentelli , A Communication Synthesis Infrastructure for Heterogeneous Networked Control Systems and its Application to Building Automation and Control , Proceedings of the Seventh International Conference on Embedded Software (EMSOFT), 2007.

Publications by **Uppsala**

Year 3

[FKPY07] Elena Fersman, Pavel Krcal, Paul Pettersson and Wang Yi. Task Automata: Schedulability, Decidability and Undecidability. In Journal: Information and Computation, 205(8), 2007. pages: 1149-1172..

[FMPY06] Schedulability analysis of fixed-priority systems using timed automata. Elena Fersman, Leonid Mokrushin, Paul Pettersson, Wang Yi Theor. Comput. Sci. 354(2): 301-317 (2006)

[HP07] Partial Order Reduction for Verification of Real-Time Components. John Hakansson and Paul Pettersson. In Proceedings of the 5th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'07), LNCS 4763. 2007

[KSY07] Pavel Krcal, Martin Stigge, Wang Yi. Multi-processor Schedulability Analysis of Preemptive Real-Time Tasks with Variable Execution Times. In the proc. of 5th International Conference on Formal Modeling and Analysis of Timed Systems, Salzburg, Austria, October 3-5, 2007. Lecture Notes in Computer Science, Volume 4763, pages: 274-289.

Year 4

[KMY07] Pavl Krcal, Leonid Mokrushine and Wang Yi. CATS: A tool for compositional analysis of timed systems by abstraction (extended abstract). In Einar Broch Johnsen, Olaf Owe, and Gerardo Schneider, editors, Proc. of NWPT07, the 19th Nordic Workshop on Programming Theory, Oslo, Oct. 10-12, 2007.

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

[TXY08] Simon Tschirner, Liang Xuedong and Wang Yi. Model-Based Validation of QoS Properties of Biomedical Sensor Networks. M Accepted at the 8th International Conference on Embedded Software, Atlanta, USA, 2008.

Publications by **VERIMAG**

Year 3

[BK*07] S. Bensalem, M. Krichen, L. Majdoub, R. Robbana and S. Tripakis. Test Generation for Duration Systems. In VECoS 2007, Alger.

[BS07a] Simon Bliudze and Joseph Sifakis. The algebra of connectors structuring interaction in BIP. In EMSOFT'07, Salzburg, 2007.

[BS07c] Simon Bliudze and Joseph Sifakis. Causal semantics for the algebra of connectors. Formal Methods in System Design. Submitted, 2008.

[GQ07] Susanne Graf and Sophie Quinton. Contracts for BIP: hierarchical interaction models for compositional verification. In Int. Conf on Formal Technics, FORTE 2007, Talinn, volume 4574 of Lect. Notes in Comp. Sci., 2007.

[GP07] Susanne Graf, Andreas Prinz. Time in Abstract State Machines. Fundamentae Informatice, February 2007

[MSZ07] L. Mounier, L. Samper, W. Zneidi. Worst-Case Lifetime Computation Of A Wireless Sensor Network By Model-Checking. PE-WASUN 2007, Oct. 2007, Chania, Greece.

[MS*07] F. Maraninchi, L. Samper, K. Baradon, A. Vasseur. Lustre as a System Modeling Language: Lussensor, a Case-Study with Sensor Networks. SLA++P'07, ETAPS'07 Satellite Workshop on Model-driven High-level Programming of Embedded Systems, March 31, 2007, Braga, Portugal

Year 4

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

[BGL*08] Ananda Basu, Matthieu Gallien, Charles Lesire, Thanh-Hung Nguyen, Saddek Bensalem, Felix Ingrand and Joseph Sifakis. Incremental Component-Based Construction and Verification of a Robotic System. *International Workshop on Current Software frameworks in Cognitive Robotics integrating different computational paradigms, Sept. 22nd 2008, Nice, France.*

[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.*

[BBG*08] Saddek. Bensalem, Marius. Bozga, Matthieu. Gallien, Felix. Ingrand, Moez. Krichen and Stavros Tripakis. Automatic Generation of Observers for the Dala Robot with TTG. *In the International Conference CISA 2008, Annaba, Algeria*.

[BBSN08] Saddek Bensalem, Marius Bozga, Joseph Sifakis, Thanh-Hung Nguyen. Compositional Verification for Component-based Systems and Application. *6th International Symposium on Automated Technology for Verification and Analysis, October 20-23, 2008, Seoul, South Korea*

[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.*

[BS08] S. Bliudze, J. Sifakis. The Algeba of Connectors—Structuring Interaction in BIP. *IEEE Transactions on Computers*, vol. 57, no. 10, pp. 1315–1330, October, 2008.

[BGMO08] Marius Bozga, Susanne Graf, Laurent Mounier, Iulian Ober. Real Time Systems 1: Modeling and verification techniques. Hermes, Lavoisier 2008

[CG08] Olivier Constant, Susanne Graf. CSL semantics and compiler. SPEEDS project deliverable D2.3 x, September 2008.

[CRBS08] 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

[Aresa07] M. Dohler, D. Barthel, F. Maraninchi, L. Mounier, S. Aubert, C. Dugas, A. Buhrig, F. Paugnat, M. Renaudin, A. Duda, M. Heusse and F. Valois. The ARESA Project: Facilitating Research, Development and Commercialization of WSNs. IEEE SECON'07 (Fourth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2007.

[GP08] Manuel Garnacho and Michaël Périn, Convincing proofs for program certification, in Certification of Safety-Critical Software Controlled Systems (SafeCert'08), electronically published in Electronic Notes in Theoretical Computer Science.

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

[NP09] Iman NARASAMDYA, Michael PERIN, Certification of Smart-Card Applications in Common Criteria, accepted at ACM Symposium on Applied Computing 2009

[NP09a] Iman NARASAMDYA, Michael PERIN. Certification of Smart Card Applications in Common Criteria: Proving Representation Correspondences, submitted to FASE 2009

[NV08] Iman Narasamdya and Andrei Voronkov, Proving Inter-Program Properties in Translation Validation, in the 7th International Workshop on Compiler Optimization Meets Compiler Verification (COCV'08), electronically published in Electronic Notes in Theoretical Computer Science.

[OGYO08] Iulian Ober, Susanne Graf, Yuri Yushtein, Ileana Ober. Timing analysis and validation with UML: the case of the embedded MARS bus manager. In *Innovations in Systems and Software Engineering* vol. () 2008

[QG08] Sophie Quinton, Susanne Graf. Contract-Based Verification of Hierarchical Systems of Components. In 6th IEEE Int. Conferences on Software Engineering and Formal Methods, SEFM08, Cape Town, South Africa, november 2008 vol. IEEE Computer Society Press 2008

2.4.3 Interaction and Building Excellence between Partners

We consider the collaboration between the partners of the platform activity to be very intense. Most of the core partners collaborate with several other core partners in different projects on the topics directly related to the platform activity (as can be seen from the list of projects in Section 3.4), and in the course of the last year new projects have been built up establishing collaborations between partners that so far had no or only marginal collaborations. All affiliated partners have either strong connections to at least one of the core partners (such as U. of Cantabria) or collaborate as case study providers (such as EADS). In addition to formalised projects, several more informal collaborations exist.

- Uppsala has been collaborating since year 3 with Lothar Thiehle's group at ETH Zurich 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 has also initiated collaboration with North Eastern University in China, on multiprocessor scheduling.
- Collaboration on MARTE has lead to:
    - Cooperation between CEA LIST and INRIA on AADL integration and profile management;
    - Cooperation between CEA LIST and U. Cantabria on real time platform modeling and design;
    - for CEA, U. Cantabria and Thales to the set up of action support within the FP7, the ADAMS project. This latter is action for the dissemination and Adoption of the MARTE and related Standards for component based middleware.
- Collaboration between CEA and KTH in the ATESST IST project with partners in automotive domain with, namely, Volvo, Siemens VDO, ETAS, Carmeq, KTH and CEA has been a strong driver to elaborate, reinforce and disseminate the open source modeller of the platform: Papyrus and to promote its plug-in for EAST-ADL2 which has been delivered in an open-source form on the Papyrus web site (http://www.papyrus-uml.org). Moreover, all these partners will continue to contribute on this subject within the follow-up of Atesst, the Atesst 2 project which is an FP7 project.
- Collaboration between CEA and STMicroelectronics (associated partner) on Software and Hardware design flow integration
- There are a number of collaborations around AADL and related languages for which ARTIST is a common forum. There is the already mentioned collaboration between CEA LIST and INRIA. The ASSERT project was a promoter of AADL and has lead to several translations from AADL to analysis tools and enhancements of these tools, in particular Lustre and the IFx UML tool developed in the Omega project. Also in the SPICES and OpenEMBeDD projects, AADL plays a central role and involves also partners who are not formally in ARTIST but who are now part of the "Artist community"

and (co-)organise Artist workshops, such as the **UML&AADL** or the **EAST-ADL, AADL, MARTE, Autosar harmonization** workshop.

- The collaboration that started in the Persiform project between INRIA, FTRD and VERIMAG and the tool chain for the analysis of performance oriented models, has expanded to a collaboration in the OpenEmBeDD project which arose from collaboration in ARTIST.
- The SPEEDS project lead to an important collaboration between INRIA, OFFIS, PARADES and VERIMAG on the definition of the SPEEDS metamodel HRC [BCSM07] which is the basis of an important analysis platform (platform 1). This collaboration continues for the definition of a verification methodology. From the collaboration in SPEEDS has started a broader collaboration on a general framework for the semantics of communication in distributed systems with INRIA, PARADES and VERIMAG with external collaboration of University of Columbia and Cadence Design Systems [BCC+].
- Collaborations between INRIA, EPFL and VERIMAG resulted in a Kermeta-IF-Giotto tool chain for deriving both monitors and embedded code from models
- ARTIST has initiated a convergence between several, initially quite independent, collaborations between FTRD and VERIMAG. In particular, (1) the collaboration on the integration of design and performance oriented modelling in Persiform and OpenEmBeDD which is rooted in earlier collaborations on SDL and on UML – in OMEGA – (2) the collaboration porting THINK to BIP/IF which is presently continued in the form of a common PhD work [BMP+07], (3) the collaboration on Sensor networks in the ARESA project, and (4) the collaboration on test in projects like Politess or OTest which are follow-ups on earlier collaborations around test (e.g. in the AGEDIS IST project).
- ARTIST has initiated a strengthening of the collaboration between Verimag and CEA. Before Artist, there was only a relatively small collaboration on test around the tools Agatha and IF and a starting collaboration around certification (Eden 1). Since then, many more collaborations exist and are presently being built up, such as the (informal) collaboration on MARTE, the OpenEmBeDD and SPICES projects, the common organisation of workshops (such as the MARTES workshop [GGH+06] and the forthcoming ACES^{MB} workshop). New collaborations are presently on the way of being built up on general models for describing and validating architecture.
-
- Together with the University of Oldenburg, OFFIS is collaborating with Saarland University and ETH Zurich within the Transregional Collaborative Research Center AVACS, addressing the rigorous mathematical verification and analysis of models and realizations of complex safety critical computerized systems. Within one of its subprojects they are working together on the implementation of embedded real-time systems on distributed architectures. The objective of this subproject is to establish a continuous work flow from task specification to task deployment. [ED*07]

Notice that the projects on which this platform is based, in particular SPEEDS, OpenEmBeDD, EDEN, ATESST, involve important tool builders, such as Trusted Logics, Esterel Tech., Telelogic, GenSys, ETAS, Mentor Graphics and Extessy which will hopefully allow us to increase the impact.

Generally, the platform activity had a very positive effect on the collaboration amongst ARTIST partners which would have been impossible to achieve without the existence of ARTIST, in particular, the collaboration between EPFL, INRIA, OFFIS, PARADES and VERIMAG on

modelling of heterogeneous systems addressing a crucial problem for the platform aiming at the integration of synchronous and asynchronous approaches.

Several IST projects on topics related to the component platform arose directly from collaborations initiated by ARTIST and ARTIST2 – and from some previous collaborations on the model-driven approach, such as SafeAir and OMEGA - in particular the projects OpenEmBeDD, SPEEDS, ATESST-2, ADAMS and COMBEST. The most recent one is COMBEST which has started this year. The Artist partners involved in that project are Verimag (coordinator), EPFL, ETHZ, INRIA, OFFIS, Parades, Braunschweig U. and Artist associated partners EADS and IAI. The aim of COMBEST is provide a formal framework for component based design of complex embedded systems that allows formal integration of heterogeneous components and that provides complete encapsulation of components also for extra-functional properties, thus providing the key for prediction of performance and robustness. For doing so, the project will develop a design theory for complex embedded systems covering heterogeneity, interface specifications, composability, compositionality, and refinement for functional and extra-functional properties. We expect that these results will enable us at a longer term to make the presently separate platforms cooperate in a meaningful way. COMBEST will have a strong interaction with SPEEDS which is one year before its termination.

The organization of a large number of workshops as a collaboration of several ARTIST partners, also from different platforms (see section 2.3.5) is another indicator of collaboration between the different communities which have lived a quite independent life before the beginning of ARTIST.

2.4.4 Joint Publications Resulting from these Achievements

Year 3

[BMP+07] A. Basu, L. Mounier, M. Poulhiès, J. Pulou and J. Sifakis Using BIP for Modeling and Verification of Networked Systems - A Case Study on TinyOS-based Networks 6th IEEE Int. Symp. on Network Computing and Applications (NCA 2007), July 2007, Cambridge, MA, USA.

[BCC+] A. Benveniste, B. Caillaud, L.P. Carloni, P. Caspi, A.L. Sangiovanni-Vincentelli and S. Tripakis, Communication by Sampling in Time-Sensitive Distributed Systems , in Proceedings of the Sixth International Conference on Embedded Software (EMSOFT), Seoul, Korea, October, 2006.

[BCSM07] M. Bozga, O. Constant, M. Skipper, and Q. Ma. SPEEDS meta-model syntax and static semantics. SPEEDS deliverable D2.1d, July 2007.

[CCG+07a] *Philippe Cuenot, DeJiu Chen, Sébastien Gérard, Henrik Lönn, Mark-Oliver Reiser, David Servat, Carl-Johan Sjöstedt, Ramin Tavakoli Kolagari, Martin Törngren and Matthias Weber* Managing Complexity of Automotive Electronics Using the EAST-ADL. In Proc. of the 2nd Int. UML&AADL Workshop (UML&AADL'2007) at the 12th Int. Conf. On Engineering of Complex Computer Systems, Auckland, New Zealand, July 11 - 14, 2007

[CCG+07b] Philippe Cuenot, DeJiu Chen, Sébastien Gérard, Henrik Lönn, Mark-Oliver Reiser, David Servat, Ramin Tavakoli Kolagari, Martin Törngren, Matthias Weber. “Towards Improving Dependability of Automotive Systems by Using the EAST-ADL Architecture Description Language", In Book Architecting Dependable Systems IV, August 2007.

[CGM07] O. Constant, W. Monin, S. Graf “From Complex UML Models to Systematic Performance Simulation with Persiform”. Verimag Research Report no TR-2007-10, submitted for publication

[DB*07] M. Dohler, D. Barthel, F. Maraninchi, L. Mounier, S. Aubert, C. Dugas, A. Buhrig, F. Paugnat, M. Renaudin, A. Duda, M. Heusse and F. Valois. The ARESA Project: Facilitating Research, Development and Commercialization of WSNs' IEEE SECON'07 (4th IEEE Com. Soc. Conf. on Sensor, Mesh and Ad Hoc Communications and Networks), June 18-21, 2007, San Diego, CA, USA

[DKL07] H. Dierks, S. Kupferschmid, K.G.Larsen; Automatic Abstraction Refinement for Timed Automata; In J.-F. Raskin, P. S. Thiagarajan (Edts.) Proceedings Formal Modeling and Analysis of Timed Systems on the 5th International Conference, FORMATS 2007, Lecture Notes in Computer Science 4763, Springer-Verlag, S. 114-129, 2007

[ED*07] F. Eisenbrand, W. Damm, A. Metzner, G. Shmonin, R. Wilhelm, and S. Winkel. Mapping Task-Graphs on Distributed ECU Networks: Efficient Algorithms for Feasibility and Optimality. In Proceedings of the 12th IEEE Conference on Embedded and Real-Time Computing Systems and Applications. IEEE Computer Society, 2006.

[FTSG07] *Faugère Madeleine, Tourbeau Thimothée, De Simone Robert, Gérard Sébastien*, "MARTE: Also an UML Profile for Modeling AADL Applications", In ICECCS'2007, 1st IEEE-SEE International Workshop UML and AADL - 2007, Auckland, Nouvelle-zélande, July 2007

[EDG+07] *Huascar Espinoza, Hubert Dubois, Sébastien Gérard, Julio Medina, Dorina C. Petriu, Murray Woodside.* Annotating UML Models with Non-Functional Properties for Quantitative Analysis*. In Satellite Events at the MoDELS 2005 International Workshop, Montego Bay, Jamaica, Revised Selected Papers, pages pp. 79 - 90. Springer, 2006. (*ISBN: 3-540-31780-5*).*

[FBSG07] Madeleine Faugère, Thimothée Bourbeau, Robert de Simone and Sébastien Gérard. MARTE: Also an UML Profile for Modeling AADL Applications*. ICECS, 2007.*

[GGM+07a] Gregor Gössler, Susanne Graf, Mila Majster-Cederbaum, M. Martens, and Joseph Sifakis. An approach to modeling and verification of component based systems. In Current Trends in Theory and Practice of Computer Science, SOFSEM'07, number 4362 in LNCS, 2007.

[GGM+07] Gregor Gössler, Susanne Graf, Mila Majster-Cederbaum, M. Martens, Joseph Sifakis, Ensuring Properties of Interaction Systems by Construction. In Program Analysis and Compilation, Theory and Practice, number 4444 in LNCS, 2007.

[GGH+06] Susanne Graf, Sébastien Gérard, Oystein Haugen, Iulian Ober, Bran Selic. MARTES - Modelling and Analysis of Real Time and Embedded Systems Using UML. In *MoDELS 2006 International Workshops, Doctoral Symposium, Educators Symposium; Genoa, October 2006, Revised Selected Papers* LNCS 4364, 2006

[LMD07] *Lopez P.; Medina J.; Drake J.M., Real-Time Modelling of Distributed Component-based Applications. 32nd EUROMICRO Conference on Software Engineering and Advanced Applications (EUROMICRO-SEAA - 2006) ; 29/08/2006 - 01/09/2006 ; Cavtat/Dubrovnik ; Croatia*

[LTAG07b] Constraints modeling for (profiled) UML models.*. François Lagarde, François Terrier, Charles André and Sébastien Gérard. In European Conference on Model-Driven Architecture: Foundations and Applications 2007 (ECMDA 07), Haïfa, Israel, Juin 2007.*

[MFF+07] *Pierre-Alain Muller, Franck Fleurey, Frédéric Fondement, Michel Hassenforder, Rémi Schneckenburger, Sébastien Gérard and Jean-Marc Jézéquel.* Model-Driven Analysis and Synthesis of Concrete Syntax.*. In MoDELS, pages 98-110, 2006.*

[MAP+07] *Marau R; L. Almeida; P. Pedreiras; M. González Harbour; Sangorrín D.; Medina J., Integration of a flexible network in a resource contracting framework, 13th IEEE Real-*

Time and Embedded Technology and Applications Symposium (RTAS - 2007) ; 03-06/04/2007 ; Seattle ; US.

[MLD+07] *Julio Medina, Patricia Lopez, Jose Maria Drake, Francois Terrier, Sebastien Gerard.* A Modeling Approach for the Timing Verification of COTS Components-based Distributed Hard Real-Time Systems*. In Proccedings of the Workshop on Models and Analysis for Automotive Systems, held in conjunction with the 2006 RTSS, 2006.*

[MLD07] *Medina J.; Lopez P.; Drake J.M., Towards a UML Profile for Real-Time Modelling of Component-Based Distributed Embedded Systems. Forum on Specification and Design Languages (FDL - 2006) ; 19-22/09/2006 ; Darmstadt ; Germany*

[SCC+07] Carl-Johan Sjöstedt, De-Jiu Chen, Phillipe Cuenot, Patrick Frey, Rolf Johansson, Henrik Lönn, David Servat, Martin Törngren. Developing Dependable Automotive Embedded Systems using the EAST-ADL; representing continuous time systems in SysML. In Proc. of EOOLT'2007. 1st Int. Workshop on Equation-Based Object-Oriented Languages and Tools.

[TRGD07] An Open Framework for Hardware Detailed Modeling. S. Taha, A. Radermacher, S. Gerard & J-L Dekeyser. In IEEE proceedings SIES'2007, pages 118-125, Lisboa, July 2007.

Year 4

[BCCCS] A. Benveniste, B. Caillaud, L.P. Carloni, P. Caspi, and A.L. Sangiovanni-Vincentelli. Composing Heterogeneous Reactive Systems, ACM Transactions on Embedded Computing Systems, Vol. 7, No. 4, July 2008.

[CSST08] P. Caspi, N. Scaife, Ch. Sofronis, S. Tripakis. Semantics-preserving multitask implementation of synchronous programs. *ACM Transactions on Embedded Computing Systems*, 7(2), February 2008

[CWG08] Olivier Constant, Wei Monin, Susanne Graf. A model transformation tool for performance simulation of complex UML models. ICSE Companion 2008.

[CFJLRSTKC08] *Cuenot Ph, Frey P, Johansson R., Lönn H, Reiser O, Servat D, Tavakoli Kolagari R, Chen DJ, "*Developing Automotive Products Using the EAST-ADL2, an AUTOSAR Compliant Architecture Description Language", 4th European Congress on Embedded Real Time Software (ERTS - 2008), Toulouse, France, 2008

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

[DABBCLLPSV08] *Dubois H., Albinet A., Begoc S., Boulanger J.-L., Casse O., Dal I., Lakhal F., Louar D., Peraldi-Frati M.-A., Sorel Y., Van Q.-D*. "The MeMVaTEx methodology: from requirements to models in automotive application design", Proceedings of the 4th European Congress ERTS 2008, 4th European Congress on Embedded Real Time Software (ERTS - 2008), Toulouse, France, 2008

[ERG08] *H. Espinoza, K. Richter, S. Gérard*, "Evaluating MARTE in an Industry-Driven Environment: TIMMO's Challenges for AUTOSAR Timing Modeling", Design, Automation, and Test in Europe (DATE - 2008), Munich, Allemagne, 2008

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

[HJR+07] N. Halbwachs, E. Jahier, P. Raymond, X. Nicollin, D. Lesens Virtual execution of AADL models via a translation into synchronous programs *Seventh International Conference on Embedded Software (EMSOFT 2007)*, Salzburg, Austria

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

[LETAG08] *F. Lagarde, H. Espinoza, F. Terrier, C. André, S. Gérard.* "Leveraging Patterns on Domain Models to Improve UML Profile Definition". FASE 2008: pp. 116-130, Budapest, Apr 2008

[LTAG07a] Extending OCL to ensure model transformations. *François Lagarde, François Terrier, Charles André and Sébastien Gérard.* Foundations and Practices of UML, *November 2007. (*workshop of ER 2007*).*

[MAPGSM07] *Marau R., Almeida L., Pedreiras P., González Harbour M., Sangorrín D., Medina J.*, "Integration of a flexible time triggered network in the FRESCOR resource contracting framework", Proceedings of the 12th IEEE Conference on Emerging Technologies and Factory Automation (ETFA - 2007), Patras, Grèce, 1481-1488, Oct. 2007

[MFFHSGJ08] *Muller P-A., Fondement F., Fleurey F., Hassenforder M., Schnekenburger R., Gerard S., Jezequel J-M*, "Model-Driven Analysis and Synthesis of Textual Concrete Syntax", Software and Systems Modeling, 1619-1366, 2008

[Metal08] C. Mrugalla, Olivier Constant, Julen de Antoni, Eldad Palachi: SPEEDS Meta-model – Profile Definition. SPEEDS deliverable D2.1.4, May 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

[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

[STS+07] Jianlin Shi, Martin Törngren, David Servat, Carl-Johan Sjöstedt, DeJiu Chen, Henrik Lönn. Combined usage of UML and Simulink in the Design of Embedded Systems: Investigating Scenarios and Structural and Behavioral Mapping. To appear in OMER 4 workshop on Object-oriented modelling of embedded real-time systems, Oct. 30-31, 2007.

[STS+08a] 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

2.4.5 Keynotes, Workshops, Tutorials

ARTIST Summer School on embedded systems design
Su Zhou, China. Jul. 12-18, 2008,

is the third edition of the ARTIST summer school on embedded systems design organized jointly by ARTIST and China. The school is to promote collaboration between European and Chinese research community on embedded systems, and related areas.

http://www.artist-embedded.org/artist/Artist2-Summer-School-in-China.html

ARTIST Summer School on embedded systems design
Autrans, France Sep. 8-12, 2008
This is the fourth such summer school organised by Artist in Europe, and it is meant to be exceptional in terms of both breadth of coverage and invited speakers. The topics covered include Modeling and Validation, Compilers and Timing Analysis, Adaptive Real Time Systems, Control for Embedded Systems, Execution Platforms and MPSoC. A balance is seeked between foundational aspects and applications. Speakers include recognized leading researchers and engineers.

http://www.artist-embedded.org/artist/ ARTIST2-Summer-School-2008.html

under preparation:

Spring School on MDD for Distributed Real-Time and Embedded Systems
Autrans, France, March, 2009

Workshop: EAST-ADL, AADL, MARTE, Autosar harmonization workshop

Paris -- Oct. 25, 2007

The workshop provided useful information exchange between the standardization initiatives and ***ATESST***. Approximately 25 participants from the automotive industry (apart from ATESST partners, VW, Audi and Continental attended), CMU/SEI and research universities/institutes were represented. Also invited were representatives from the recently started TIMMO project. It was agreed to maintain contacts, and to organize follow up meetings. Identified topics of common interest include Timing, Error modeling and Methodology. A common email list will be set up.

Workshop: FMCO 2007, 6th Int. Symposium on Formal methods for Components and Objects

Amsterdam – November 7-10, 2007

The objective of this symposium is to bring together researchers and practioners in the areas of software engineering and formal methods to discuss the concepts of reusability and modifiability in component-based and object-oriented software systems. VERIMAG is a co-organiser of this event. For 2007, we organised a special issue of this symposium bringing together groups of a set of related EU projects and NoEs; Artist is one of those groups.
http://fmco.liacs.nl/fmco07.html

In 2008, the idea experimented in 2007 has been taken up for a different selection of IST projects and by a fresh set of organisers. FMCO 2008 will take place in November in Nice.

Workshop: Model based development of automotive embedded systems - The EAST-ADL approach

Brussels -- March 3rd, 2008

At the workshop, the results from the ***ATESST*** research project were presented for the attending representatives (approx. 30 persons) from industry, research, the European commission and interest organizations (EUCAR). The results, challenges and future prospects for the project results were discussed.

Workshop : SafeCert 2008 International Workshop on the Certification of Safety-Critical Software Controlled Systems

ETAPS 2008

Budapest, Hungary – 29 March, 2008

In many domains like transportation, power generation, medical technology, manufacturing and space exploration, statutory obligations traditionally require a formalized certification for the development of high assurance products. Formal methods are part of the standard recommendations, in particular for the higher safety integrity levels. However, experience shows that certifiable development of high-assurance software needs a lot more than pure application of formal techniques and tools that are founded on a formal semantics and support in parts automated code generation, formal analysis, verification or error detection. The major question to be addressed in the workshop is how to embed formal methods and tools in a seamless design process which covers several development phases and which includes an efficient construction of a safety case for the product.
http://safecert08.offis.de/

Workshop: UML&AADL

Belfast -- April 2nd, 2008

This ARTIST workshop is held in conjunction with the 13th IEEE International Conference on Engineering Complex Computer Systems, ICECCS 2008. It gathered 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/-UML-AADL-2008-.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

Workshop: 1st IEEE International workshop UML and Formal Methods

Kitakyushu-City, Japan -- October 27th, 2008

Hold in conjunction with the 10th International Conference on Formal Engineering Methods, ICFEM 2008. For more than a decade now, the two communities of UML and formal methods have been working together to produce a simultaneously practical (via UML) and rigorous (via formal methods) approach to software engineering. The fact that the UML semantics is too informal has led many researchers to formalize it with different existing formal languages. The main objective of this workshop is to encourage new initiatives of building bridges between informal, semi-formal and formal notations.

http://www.artist-embedded.org/artist/UML-FM-08.html

Workshop: **RTSS08 track on Design and Verification of Embedded Real-Time Systems** with 29th IEEE **Real-Time Systems Symposium**.

Barcelona --- November 30 - December 3, 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

Tutorial: UML Tutorial: MARTE
Forum on specification & Design Languages (FDL'07)
Barcelona, Spain - September 20, 2007

http://www.ecsi-association.org/ecsi/fdl/fdl07/programme.htm

Tutorial: MARTE: A New Standard for Modeling and Analysis of Real-Time and Embedded Systems UML Tutorial: MARTE
19th Euromicro Conference on Real-Time Systems (ECRTS 07)
Pisa, Italy - July 3, 2007

http://feanor.sssup.it/ecrts07/tutorial.shtml

Lecture: UML for the design of Real-Time Embedded Systems
ARTIST2 Winter School 2007 – MOTIVES (MOdelling, TestIng, and Verification for Embedded Systems)
Pisa, Italy - July 3, 2007
http://feanor.sssup.it/ecrts07/tutorial.shtml

Lecture: Towards Automated Test Generation for Timed Systems
TAROT Summer School 2008
Pisa, Italy - July 3, 2007

http://feanor.sssup.it/ecrts07/tutorial.shtml

3. Milestones and Future Evolution Beyond the NoE

3.1 Milestones

Milestones from the descriptions of Work

- Year 1: Initial definitions of modules to assemble in the platform

  This milestone had been achieved at the end of year 1

- Year 2: Initial connections within a common framework of existing UML-based analysis and validation tools.

  This milestone has been achieved at the end of year 2: there exist new tool connections in the platform picture that can be demonstrated, including complete chains from modelling to validation, in particular

  - *the Persiform tool chain from an Activity Diagram oriented UML profile for functional service specifications or annotated MSC to the SES workbench performance analysis tool.*
  - *the Kermeta – IF tool chain manages software development support starting from the specification of components and their composition, their verification down to the generation of Java or C based executable units for the execution of a specific platform,*
  - *the BIP/THINK tool chain represents the backend of a tool chain of a tool chain with the same motivations as the previous one.*
  - *The start of the OpenEmbeDD, System@tic/Usine Logicielle, and SPEEDS project represent an important milestone, as their aims are fully in line with those of the platform and they provide the funding for deep technical work and the modelling languages they build upon, focus on different, complementary aspects.*

- Year 3: Strengthen and extend the existing tool chains so we are capable to connect some of the analysis and validation tools developed by the partners or outside Artist to UML tools by means of mappings to a few semantic frameworks, in turn mapped to the input languages of the tools. This will allow relising tool chains from high level languages down to code.

  This work will include in particular, mappings from the HRC model defined in SPEEDS into semantics level formalisms for the connection to validation and and analysis tools as well as tools for model-based code generation.

  > *We have not yet finalized the mappings from the HRC model defined in SPEEDS into semantics level formalisms, but this will be achieved within the 4th year. We consider that the milestone of the second year has been achieved. The existing tool chains have been strengthened and new connecting elements added to the global picture, in particular. Most individual objectives have been fulfilled or are closed of being fulfilled.*

  Updated milestone of year 3: **Strengthen and extend the existing tool chains so as being able to connect some of the analysis and validation tools developed by the partners or outside Artist to UML tools by means of mappings to a few semantic frameworks, in turn mapped to the input languages of the tools.**

- Year 4: Final integration of the results of the related Joint Research Activities.

This milestone appears to be over optimistic. We will achieve a higher degree of collaboration between tools than at the beginning of Artist but full integration can not be achieved in such a short time.

Updated Milestone for year 4: At the end of the project, the possible degree of collaboration between tools will be much increased with respect to the beginning of Artist.

3.2 Indicators for Integration

The main indicators for integration for the platform activity are the following ones:

- ***Joint publications on platform related issues***

  As can be seen in section 2.3.4, we have over 40 joint publications in the last two years of the project, half of it i for each year, where most of them imply more than 2 platform partners. This number has been strongly increasing since the beginning of the project (in year 2 there were 5, and in year 3 there were 20 joint publications).

- ***Joint workshop organisations***

  From the start of ARTIST, workshops, schools and other events have been organised jointly by several partners of the platform, and their number has been steadily increasing. This year, several workshop concern component-based architecture modelling and validation, as well as corresponding industrial standards (AADL, EAST-ADL). Most workshops are organised jointly between Artist partners and partners outside Artist which leads to a de facto broadening of the “Artist community”.

- ***Joint project proposals***

  Since the existence of the ARTIST NoE, a number of new projects around tool development or concerning a formal basis for tool developments have been set up jointly by ARTIST partners. Some of the partners had already collaborated in the past, but there arose also new collaborations, in particular between partners from the domain of formal methods and those from model-based design.

  In particular the following projects have started during the duration of the NoE: the SPEEDS IP with four academic Artist partners and several associated industrial partners and the SPICES ITEA project with four Artist partners and numerous French projects involving several French Artist partners started in 2006. . The ADAMS dissemination action (http://www.adams-project.org) is an FP7 project started in Mai 2008. This project is aiming at promoting MARTE in embedded domain, especially in both automotive and aeronautics domains. Two academics Artist partners are involed (CEA LIST and the university of Cantabria), but also two affiliated industrial partners, Thales and Volvo Technology. CEA and Volvo Tech. are also involved in the followup of an eutopean project ATESST (www.atesst.org).

  The FP7 Combest project, which aims at developing and promoting modelling paradigms appropriate for heterogeneous systems, as well as several smaller projects have started this year; they all involve several platform partners.

- ***Joint tool developments and integration of toolsets***

  Within the set of tool development activities under the umbrella of the modelling platform of the cluster are several platform projects and tool chain developments representing joint

efforts between several partners. In fact, almost all the activities grouped in the 3 platforms are development involving at least 2 Artist partners.

Presently, the platform presented in this deliverable is a set of platforms for particular purposes rather than an integrated platform. At a long term, some convergence may be desirable, and in some cases feasible. For example, the developments in the OpenEmBeDD and the SPEEDS project could converge to some extent. However, since this approach needs a significant amount of dedicated resources, it is outside the scope of ARTIST. Some connections between the different parts have been achieved:

- Back-end analysis tools are largely shared amongst the different platforms – modulo project specific adaptations. And this tendency will certainly increase through the increased sharing of intermediate representations
- The standalone tool-chain for performance simulation developed in Persiform is being integrated into the platform developed in the OpenEmBeDD project through a lightweight connection to the MARTE profile. Integration into the SPEEDS platform was envisaged but not retained as a priority.
- There are several developments around AADL ongoing in several projects which all use OSATE as an input tool. These efforts should reach some converge soon.

3.3 Main Funding

The funding for the coordination and planning work reported above as well as the meeting and deliverable preparations have been funded by ARTIST (with the exception of a few travels paid with other resources). The funding for the development of the platform components, reported in Section 2 come from the following sources where we distinguish projects which have terminated during ARTIST2 and those which are still ongoing, or have just started, today:

Successfully terminated projects

- ASSERT – IP project (http://www.assert-project.net/, Verimag, ETH, Esterel Technologies, EADS) addressing the problem of by construction correct system architectures for SPACE systems (started in 2004 and terminated early 2008)
- ATESST – IST project (http://www.atesst.org/, CEA, KTH, Volvo Tech., Daimler Chrysler, etc.) addressing system modelling techniques for automotive software development under alignment constraints with Autosar, UML and SysML standards
- EDEN (http://www.eden-rntl.org/ for CEA, Verimag), French national RNTL project on UML based development and verification of security critical system;
- Families (for CEA, INRIA, Thales), ITEA European project on component based modeling of product lines
- HeCoSim French project (http://www.projet-hecosim.org, Artist partners CEA and INRIA) centered on co-simulation of a whole system using heterogeneous formalisms used in automotive domain. Simulation scenarios are computed and generated via symbolic execution of heterogeneous models.
- PERSIFORM (http://www-persiform.imag.fr/, for FTRD, INRIA and Verimag), a French National RNRT project on functional and performance analysis of service oriented specifications (terminated in August 2007)

- SAVE++ (http://www.mrtc.mdh.se/SAVE/, for Uppsala) supported by Swedish strategic research. Component Based Design of Safety Critical Vehicular Systems
- STACS (for CEA, Thales), French national RNRT project on validation and testing of heterogeneous component based models
- SysPEO Eureka project (ARTIST partners CEA and Leuven) was centered on verifying Matlab and Simulink model in the automotive model through formal techniques using the Agatha symbolic execution kernel.

Ongoing projects

- ADAMS (www.adams-project.org, for CEA), FP7 project, Action for the Dissemination and Adoption of the MARTE and related Standards for component based middleware. The ADAMS project aims at promoting the usage of the MARTE standard for the development of real-time and embedded systems using both model and component design paradigms.
- AMAES (http://www-verimag.imag.fr/~krichen/AMAES/, for Verimag), A French National project on the development and validation of Advanced Methods for Autonomous Embedded Systems.
- ARESA (http://www-verimag.imag.fr/SYNCHRONE/index.php?page=fiche-aresa, for Verimag and FTRD), French National ANR project on modelling energie consumption of Sensor networks
- ATESST 2 (http://www.atesst.org), FP7 project, it aims at improving development practice through model-based techniques: The Architecture Description Language EAST-ADL2 is being refined and related methodology, analysis, and synthesis techniques are being explored.
- AVACS (http://www.avacs.org/, for OFFIS, Saarbruecken) on Automatic Verification and Analysis of Complex Systems, Transregional Collaborative Research Center.
- The CARROLL initiative, a common research program between Thales, CEA and INRIA, it has been, in particular, the core support for the construction, submission and adoption of the new UML standard for real time embedded systems (MARTE)
- CREDO (http://www.cwi.nl/projects/credo/, for Uppsala), supported by EU, Modeling and analysis of evolutionary structures for distributed services started in 2007 taking up on results of the OMEGA project
- EDEN 2 (http://www.eden-rntl.org/, for CEA, VERIMAG), French national RNTL project on UML based development and verification of security critical system
- FAROS (www.lifl.fr/faros/, for INRIA and FTRD), French National RNTL project on composition of service-oriented systems based on software contracts and components
- MemVaTEx – French RNTL project (www.memvatex.org/, CEA, INRIA, Siemens VDO, etc.), a modelling methodology that supports the development continuity, model refinement and interoperability between heterogeneous modelling formalisms.
- “Modeling and verification of timed systems” (for Uppsala) financed by the Swedish research council. This project supports the activities of Uppsala on Times and Uppaal.
- OpenEmBeDD (http://openembedd.inria.fr/, for CEA, FTRD, INRIA, and VERIMAG), French national RNTS project aiming at the development of an open source platform for providing model based engineering technologies for the development of real-time embedded applications.

- SPEEDS IP project (http://www.speeds.eu.com/), with the ARTIST partners INRIA, OFFIS, PARADES and VERIMAG and affiliated industrial partners EADS and IAI.
- The SPICES ITEA project on *Support for Predictable Integration of mission Critical Embedded Systems*. (http://www.spices-itea.org/public/news.php) with Artist partners CEA, Leuven, Cantabria and VERIMAG and several industrial partners started end of 2006 and will terminate end of 2009.
- Usine Logicielle (Software Factory, www.usine-logicielle.org/, http://www.events-systematic-paris-region.org/forum06/press/Usine%20Logicielle.pdf), French project of the System@tic pole of competivity (Thales, CEA, INRIA, EADS, etc.), aiming at the development of an open platform for model driven engineering of complex systems.

Projects started in 2008

- COMBEST FP7 project on component based design of complex embedded systems with Artist partners Verimag (coordinator), EPFL, ETHZ, INRIA, OFFIS, Parades, Braunschweig U. and Artist associated partners EADS and IAI. This project has started in January 2008. http://www.combest.eu/home/
- Genesys FP7 project on Genesys whose objective is to define a cross-domain reference architecture for embedded systems that can be instantiated for different application domains to meet the requirements and constraints defined in the Artemis strategic research agenda. The Artist partners are CEA, TU Vienna (coordinator), Twente, Verimag and several affiliated industrial partners
- Industrial funding (Pirelli, Ferrari, United Technology Corporation, Cadence, ST) for the Metropolis II and its application were provided to PARADES.

3.4 Future Evolution Beyond the Artist2 NoE

The platform will not continue as such in NoE ArtistDesign. But the work on most topics will continue in the Artist Design cluster “Modeling and Validation” or in still ongoing or new projects. We expect the collaborations that have been initiated through Artist to continue.

The activities on modelling framework (topic 1) will continue in Artist Design -- whose objective is to establish a coherent body of modelling formalisms that support the component-based design and automatic analysis of embedded systems -- and focus on composition of heterogeneous components based on interfaces, and modelling of resource related and quantitative aspects. In particular,

- The SPEEDS partners OFFIS, INRIA, Parades Verimag will continue to enhance and make evolve the HRC meta-model defined in the project. HRC enhances components with contracts but does not introduce any application or concern specific concepts. Such concepts might be added and the adopted concepts might be taken over from existing formats (AADL, MARTE, Decos meta-model, ...).
- CEA does intend to continue its effort with regards to platform-based design
- PARADES will continue to work on platform-based design and related tools both in new European projects such as COMBEST and Artist-Design an in collaboration with its industrial partners. In addition, it will explore with greater emphasis the application of methodology and tools to the fault tolerant domain.
- Uppsala will continue to work on resource modelling

- Verimag will continue the work on the BIP component model, and develop general and application dependent methodologies for resource constraint context. In particular, we will continue developing modelling paradigms for the evaluation of energy consumption in WSN with support from the ARESA project, development of resource models for embedded platforms for performance evaluation, modelling paradigms for robotic applications and for service oriented architectures. New application domains will be considered as well.

Also the activities on analysis and validation engines (topic 5) will continue in Artist Design and focus on compositional validation, quantitative validation (tools for stochastic, real-time, and hybrid systems), cross-layer validation and synthesis; in addition, we may consider safety and security aspects, as well as validation for certification (topic . The partners of the still ongoing projects SPEEDS, OpenEmBeDD, ATESST, Combest, … will continue to work on the planned analysis and validation tools. In particular the following efforts will continue

- CEA will continue to improve and adapt the Agatha tool to different validation problems
- Together with the University of Oldenburg, OFFIS is collaborating with Saarland University and ETH Zurich within the Transregional Collaborative Research Center AVACS, addressing the rigorous mathematical verification and analysis of models and realizations of complex safety critical computerized systems. Within one of its subprojects they are working together on the implementation of embedded real-time systems on distributed architectures. The objective of this subproject is to establish a continuous work flow from task specification to task deployment. [ED*07]
- The Desyre tool will be enhanced as we enlarge its applicability to other domains of system level design such as energy efficient building design.
- Uppsala will in particular work on timing analysis for embedded software on multicore platforms
- Verimag will develop new compositional analysis methods. We will continue to improve the existing tool D-finder which implements structural deadlock analysis for general models. We will develop stronger methods for models which adhere to domain specific structure constraints, in particular for timing analysis. We will push further contract-based compositional analysis and synthesis. We will also continue to work on efficient simulation of WSN and adapt these methods to other applications.

The platforms of the present JPRA (topics 3 – 4) will not exist as such in Artist Design. It's constituents will continue to be developed in the projects by which they are supported and some of them will be part of Artist Design. For several platforms there exist already precise exploitation plans, some will probably remain "proofs of concept". In particular,

- It is planned to continue the development and the exploitation of the OpenEmBeDD and SPICES platforms in future projects. However these projects are still under construction
- The SPEEDS project has still more than 1 year to go and the way in which the future development and exploitation is ensured is presently actively discussed within the project.
- The tool chain developed in the Persiform project is presently being integrated in the OpenEmBeDD platform. It could be adapted as performance simulation tool into any design platform in which this type of performance analysis is relevant. Due to the separation between the functional and performance aspects, it could also be adapted to different performance analysis methods.

- Important parts of the platform in the Eden and Eden-2 projects have already been transferred to tool providers in the domain of certification. If the results on the generation of certificates are up to the expectation, they will certainly been taken up by certification authorities and tool builders.
- The tool chain developed in the ARESA project is already used by an SME specialized in Sensor networks. The project will certainly have some continuation.
- The BIP and IF modelling and validation platforms will continue to be developed and enriched by Verimag. Several projects have recently started which provide support for this work.
- Within the JU ARTEMIS framework some of the ARTIST2 partners (ibcluding CEA, INRIA, OFFIS, PARADES) are involved in a proposal called CESAR (Cost-efficient methods and processes for safety relevant embedded systems). Provided that CESAR will be selected for funding a modelling and analysis platform based on existing approaches (including SPEEDS and ATESST and others) will be established and enhanced.

4. Internal Reviewers for this Deliverable

Alberto Sangiovanni Vincentelli (Parades, cluster internal)

Arne Skou (Aalborg, external to cluster)