IST-004527 ARTIST2
Network of Excellence
on Embedded Systems Design

Activity Progress Report for Year 3

JPIA-Platform

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 Contents

1. Overview of the Activity

1.1 ARTIST Participants and Roles

Platform Leader: 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

Team Leader: Saddek Bensalem (Verimag)

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

Team Leader: Michael Perin (Verimag)

Contributions of his team: security of smartcard applications

Team Leader: Laurent Mounier (Verimag)

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

Team Leader: Sébastien Gérard (CEA)

Contributions of his team: UML Profile for Modelling and Analysis of Real-Time and Embedded Systems: MARTE profile, modelling for RT/E Systems, code generation, RT/E analysis such as WCET and schedulability analysis.

Team Leader: Francois Terrier (CEA)

Team Leader: Jacques Pulou (France Telecom R&D)

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

Team Leader: 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

Team Leader: Noël Plouzou (INRIA)

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

Team Leader: Martin Torngren (KTH)

Contributions of his team: collaboration on the “safety critical” platform, in particular in the context of the ATESST project

Team Leader: Bernhard Josko (OFFIS,)

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

Team leader: Alberto Sangiovanni-Vincentelli (PARADES)

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

Team Leader: Wang Yi (Uppsala)

Contributions of his team: Connection between modelling and verification tools, Times tool

1.2 Affiliated Participants and Roles

Team Leader: 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).

Team Leader: 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]

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, recently started and 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 3

In the first two years, we started collaborating on three platforms, each one providing 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):

- 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 first platform is mainly about generic techniques whereas the two other platforms target more specific application domains. A long term goal would be reaching a state where they are indeed instances of a common “meta”platform. However, since this approach needs a significant amount of dedicated resources, it is outside the scope of Artist. Nevertheless some actions along this line have been carried out within our cluster, namely:

- 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; the representation as a SysML profile making it accessible to typical users is being carried out..
  - The BIP framework providing a rich framework for incremental component composition based on a three layered structure developed by VERIMAG has been enriched [BS07a], [BS07c], [GQ07]; this structure is now part of the HRC metamodel. The execution and simulation platform has been significantly improved
  - 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 first year of the French National project OpenEmbeDD (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.
  - In the first year of the SPEEDS IP project (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 working on specific verification technology (see also results on validation technology).
  - The tool chain Kermeta-IF-Giotto has been extended to include timed BIP components as inputs for validation and monitor generation [SBD06], [SBD07].
  - BIP/Think collaboration 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 complemented by a translation in the other direction and some further development of Think (called Buzz) [BMP+07] needed to capture better concepts of standard ADLs. In parallel, work has started on the direct translation of AADL to BIP and Lustre [HJR+07].

- 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

- 3. Platform for the analysis of performance-critical systems
  - The main body of the work in this area was carried out previously in the context of the French Persiform project (http://www-persiform.imag.fr). This project has now successfully terminated; it yielded a platform for performance evaluation of functional specifications of services to be integrated into existing service platforms. The platform has now been demonstrated on case studies, and will be exploited in other projects [CGM07]
  - Recently, we started to work on simulation and validation of energy related properties of sensor networks. In the ARESA project (http://www.citi.insa-lyon.fr/project/aresa/), we study both algorithms for improving energy-related performance and modelling formalisms, and frameworks for efficient analysis of these properties [DB*07], [MSZ07],. We plan using BIP in this context.
- 4. Platform for the certification of smart-card applications. The work on this platform is supported in the Eden project (http://www.eden-rntl.org/) by collaboration between CEA and VERIMAG on functional validation of critical applications on smart cards. This year, we have defined a methodology for the certification of smart-applications and developed tools for its support [FGG07], [GGRT06].
- 5. Validation technology for platforms. We have developed a number of verification tools that could be used in more than one platform, either directly or modulo some adaptation. We expect that the development of intermediate representations will help making adaptation easier.
  - Results for the verification of systems with asynchronous communication channels have been implemented in CATS, a tool that combines timing and performance analysis [HP07].
  - The symbolic execution kernel Agatha has been integrated in the Usine Logicielle Eclipse platform in order to generate test cases for UML specifications
  - We have designed and implemented new algorithms for checking deadlock freedom for BIP models compositionally by exploiting the composition structure.
  - 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.

We have also continued the dissemination work by organising workshops and summer schools. According to the plan of action of the cluster, we have held no plenary internal platform meeting, but many meetings of subgroups and workshops in collaboration with the validation and embedded control platform (see also the sections 2.3.2 – 2.3.5 on publications and dissemination).

1.6 Comments from Year 2 Review

1.6.1 Reviewers' Comments

4.4.1 D4-RTC-Y2 Component Modelling and Verification (Platform)

ACCEPTED

This task consists of defining modelling languages around three platforms for the analysis of safety critical embedded systems, performance critical systems and for the certification of smart card applications. The work around the last platform has been delayed due to a reschedule of priorities in project EDEN-2.

The document explains in detail the progresses made and shows the various work of integration of languages and tools. However with the number of modelling languages and tools, the document is a bit difficult to read. It would have benefited of additional figures representing the interactions of the various components.

Figures have been presented during the review presentation. The document is accepted, however one should add one (or several) figure(s) showing the tools chains/languages and interaction between components.

The timetable needs to be updated.

1.6.2 How These Have Been Addressed

The final version of this year's deliverable contains the relevant diagrams to show the architecture of the platforms, the interaction of the different parts, and the relationships between platforms where possible. We used for the year 3 report the same structure as in the year 2 report, which hopefully allows recognising easily the continuation of the work, as well as some (rare) terminations.

2. Summary of Activity Progress

2.1 Reminder: Work in Year 1 (exact copy of Y1 deliverable)

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.

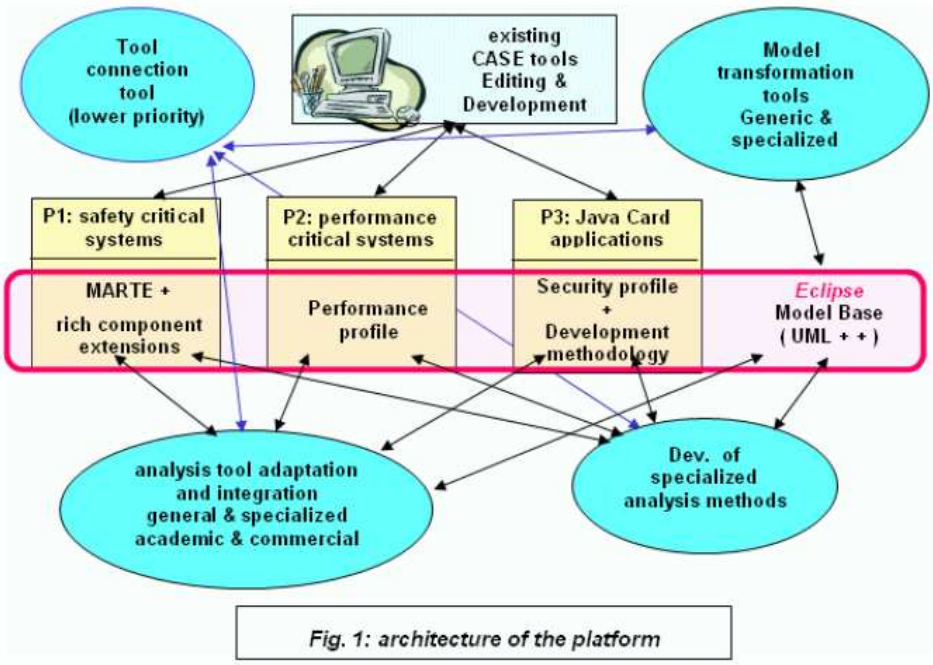

Fig. 1: architecture of the platform

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*. 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*. 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*. 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 (significantly shortened)

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. We have worked on both user and semantic formalisms where the separation is sometimes narrow, as concepts useful for validation are often somehow 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. 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 capitalize 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 Current Results

2.3.1 Technical Achievements

The problems tackled in the third year can be classified in 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 carry out case studies on worklines that had already started, and (3) to start the work inprojects OpenEmbedd and SPEEDS. In addition, we have initiated 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 results on validation technology.

1. Modelling languages and 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.

The ***MARTE profile*** has been submitted and adopted at the end of June 2007 (www.omgmarte.org). It covers modelling for designing real time embedded systems and for analysing real time behaviour and performance of the systems [TRGD07], [TGDT07], [TETG07], [TG06]. Its first implementation has been made public through its integration as a plug-in in the open source UML modelling tool: Papyrus (www.papyrus-uml.org, (see also the ARTIST 2 notice on the web site). Complementing the MARTE profile, a dedicated profile to model fault tolerance and safety requirements and architectures is been developed in the Usine Logicielle project of the Systema@tic Paris-Région pole of competitivity (www.usine-logicielle.org). Alignement with MARTE is underway. It will be made public through intregation in the Papyrus tool as a complementary plug in. These profiles will be further tooled in the platform developed in the OpenEmbedd project.

The ***Executable UML profile*** was built in the context of the Usine Logicielle project of the Systema@tic Paris-Région pole of competitivity (www.usine-logicielle.org). Its purpose is to provide a user friendly support to describe any computation and communication model in association with a formal semantics (mathematically founded) allowing to exploit it with automatic and formal techniques for model analysis or model transformations [LETG07], [CMTG07c], [CMTG07b], [CMTG07a]. This work is performed in cooperation with SupElec High School (www.THeSys.eu.org). It will be integrated to the Usine Logicielle platform, and again made public as a new Papyrus plug-in.

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. During the past period, an important part of the profile was defined [BCSM07] and the meta-model implemented as an Eclipse plug-in. HRC has been developed so far as a standalone meta-model, but it will be defined as a SysML profile.

The ***BIP framework*** (http://www-verimag.imag.fr/~async/index.php?view=components) for the composition of heterogeneous components has been extended as planned by a notion of hierarchical connectors and connector algebras that allow to transform a system architecture specification according to any required (hierarchical) grouping of components [BS07a], [BS07c]. The concept of rich hierarchical connectors has been been integrated to HRC.

We have also started to work on a semantics for distributed execution. In the context of SPEEDS, some work has been done to make easier encapsulation with BIP [GQ07]. BIP is used extensively in a number of projects, either as a system development paradigm or for validation.

The semantics of **Metropolis II** [DDM+] is centered on the connection and coordination of components [SV]. Unlike Metropolis the components are specified using external languages and the framework serves to integrate these languages and their supporting tools. 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. Metropolis II is also intended to support mixed operational-denotational specifications. Constraints are expressed in the system using first order temporal logic and regular expressions [YHC+]. The execution semantics in Metropolis is provided by intersection of behaviors and constraints. A simulator is intended to operate based on the operational description “filtered” by the constraints. Metropolis II supports non deterministic systems. Metropolis can then support rich components and provides verification and synthesis services. In the future, the role of the various tools listed above in a loosely integrated platform will be carefully considered.

2. Platform for the analysis of safety critical embedded systems

The main efforts this year concern back-end tool chains, starting from one of the envisaged semantic level formats (in particular UML profiles and HRC) and integrating validation and code generation tools. The work on the front-end tools, that provide mappings from user level profiles to semantic level formalisms has just started for MARTE and will start within the next year for HRC.

The French National platform project ***OpenEmbeDD*** (http://openembedd.inria.fr), includes the ARTIST Partners CEA, France Telecom, INRIA, Thales, and VERIMAG. In the first year, the architecture of the platform to be built was shaped by focussing on generic methods and tools, such as editors (e.g. Papyrus) and model transformation methods (such as ATL and Kermeta). Even before the release of the MARTE profile, the partners have begun defining mappings from user level formalisms, the MARTE UML profile and SDL to semantic frameworks. The case studies yet to be identified, will determine which tools or toolchains will be connected.

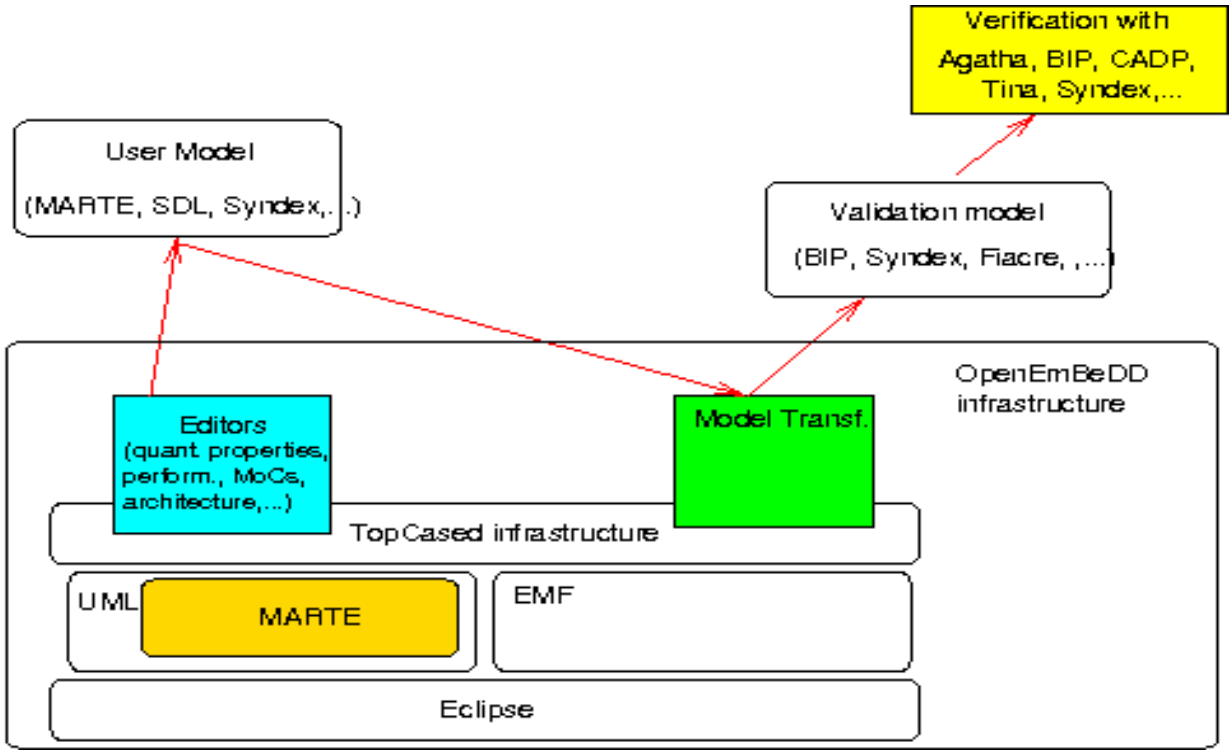

Figure 2.3-1: OpenEmBeDD platform (infrastructure)

The ***SPEEDS*** IP project (http://www.speeds.eu.com), with ARTIST partners INRIA, OFFIS, PARADES, and VERIMAG, started last year. 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.

As already stated, in the first year we defined the rich component interface model, HRC, a SysML compliant metamodel. 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.

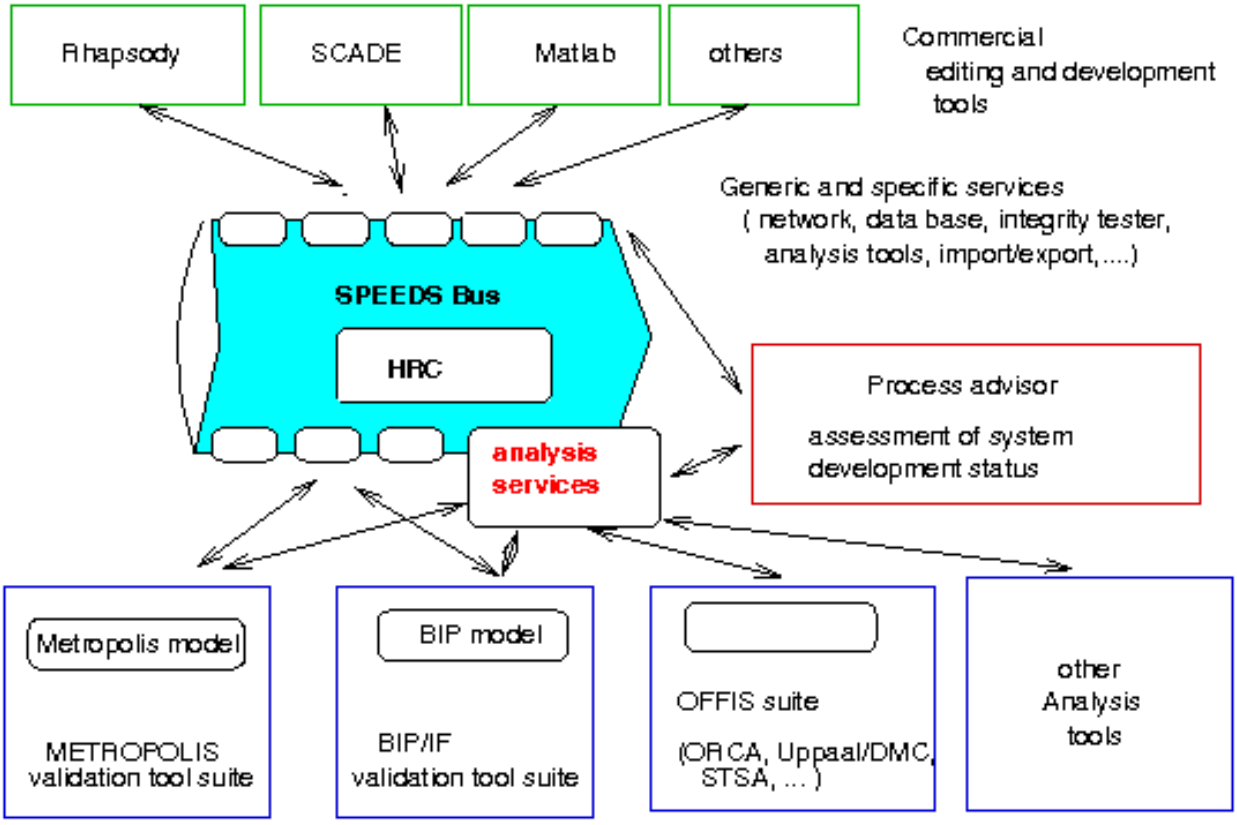

Figure 2.3-2: SPEEDS overall platform architecture

The INRIA team has extended the ***IF, Kronos, Giotto, Kermeta chain*** to include support for BIP components. The chain relies on tools from several ARTIST teams. 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 can be generated by model transformations using tools from *INRIA Triskell team*. The target architecture is the Giotto platform from *EPFL*. This year, as a follow-up of a cooperation between Inria and Verimag, the tool chain has been extended to include timed BIP components as inputs for validation and monitor generation [SBD06], [SBD07]. Hence, any timed BIP structure can be checked at runtime against execution time specification.

The collaboration between VERIMAG and FTRD on the ***compilation of BIP component systems to THINK*** takes place in a project of the Minalogic Regional competivity pole. 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. The project has concentrated this year on the extension of FRACTAL/THINK to include behaviour programming style to target execution environments and operating systems. FRACTAL/THINK components are C or assembly language components that comply with the FRACTAL component model (http://fractal.objectweb.org). They can be assembled to a software architecture using the FRACTAL Architecture Description Language (FRACTAL ADL).

BUZZ is such an extension. BUZZ [BMP+07] interconnects passive and active components in a synchronous, asynchronous, delayed, … fashion, possibly with multiple fan in or fan out (fork and join features). Many popular behaviour programming styles (multithreading, event

driven…) can be easily translated into BUZZ and on the other hand, it is easy to define a BIP model that captures finely the behaviour of any BUZZ architecture. These two features were in fact taken as inputs for the definition of BUZZ. BUZZ defines a precise behaviour for a THINK architecture by means of FRACTAL/THINK ADL tags. Tags are mainly used to

- dispatch ADL components between the sets of active and passive components
- specify the semantics of binding between components (this semantics will be formally defined using the BIP notation).

Another BUZZ extension is devoted to scheduler specification which can be viewed as an additional controller type that is added to the standard FRACTAL controller list.

BUZZ descriptions can be compiled to a concrete hardware target as the Nuptse THINK/ADL compiler takes into account BUZZ tags all along the translation process. Presently, a fully operational prototype has been developed and partially tested on a hardware board based on an Atmega 2561 8 bits microcontroller.

The next period will be devoted to validate BUZZ approach on a lightweight concrete operating system such as TinyOS. Beside this concrete target we also plan to improve the existing link between BUZZ and the analysis and verification tool set provided with BIP. We also expect to link BUZZ to existing developments in FT involving security enforcement architecture (mainly access control and authentication). This work will result in an IDE able to support the development of secure embedded operating systems offering a fully characterized and predictable run time behaviour.

Code generation from and analysis of AADL specifications is addressed in several projects. In the ASSERT project (http://www.mayeticvillage.com/assert).as, we propose using an encoding of AADL in Lustre for efficiently validating AADL descriptions as they are taken into account by the SCADE tool [HJR+07]. In the context of the related 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. 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. The overall tool chain is integrated under Eclipse in the TopCased environment. AADL is being extended with concepts for expressing specific real-time constraints (MARTE) and translations to intermediate representation for analysis are envisaged. There exists an initial systematic and structure preserving translation to BIP.

The AMAES project (http://www-verimag.imag.fr/~krichen/AMAES/) uses BIP for ***modelling software for autonomous robots***. Autonomous robots are complex systems involving numerous cooperating heterogeneous software components. They are critical systems as they must meet safety properties including ordering and hard real-time constraints. In this domain the problem arising form the use of dispersed coordination mechanisms such as semaphores, monitors, message passing, remote call, protocols, … and the lack of a unified paradigm for describing and analyzing the information flow between components is particularly tangible.

We proposed a modelling paradigm based on BIP to enforce the separation between coordination and computation (execution of sequential code). A main improvement that we expect through this better modularity is to be able to better control and analyse timing properties. We have exemplified a methodology for incremental componentization on an existing robot software system [Ngy]. The 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. Our main contribution includes:

- A methodology for componentizing and architecting autonomous robot systems.
- Composition techniques for organizing and enforcing complex event-based interaction using the BIP framework.

- Validation by using the structural deadlock detection algorithms developed for BIP and explained in sub topic 5, and which are applied in a compositional manner [BK*07].

3. Platform for the analysis of performance critical systems

This platform has been developed for the last 3 years 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 a Orpheus, an industrial user). The aim of this project is the integration of performance evaluation and formal verification in the design activity.

The first goal is to connect commercial performance analysis tools (event-based simulation mainly) to functional UML modelling tools for high-level performance analysis, in particular service specifications expressed in terms of activity diagrams has been reported last year. A UML profile has been defined and a formal semantics has been also defined through a mapping to a restricted class of coloured Petri nets extended by uninterpreted annotations with probabilities and distributions indicating timing and resource usage. Alternatively, Message Sequence Charts (MSCs) can be transformed into the same class of annotated Petri nets. Annotated Petri nets are then transformed into the input format of the performance evaluation platform HyPerformix Workbench (http://www.hyperformix.com/products/workbench/). These transformations are based on the construction of meta-models for the different languages and transformation rules.

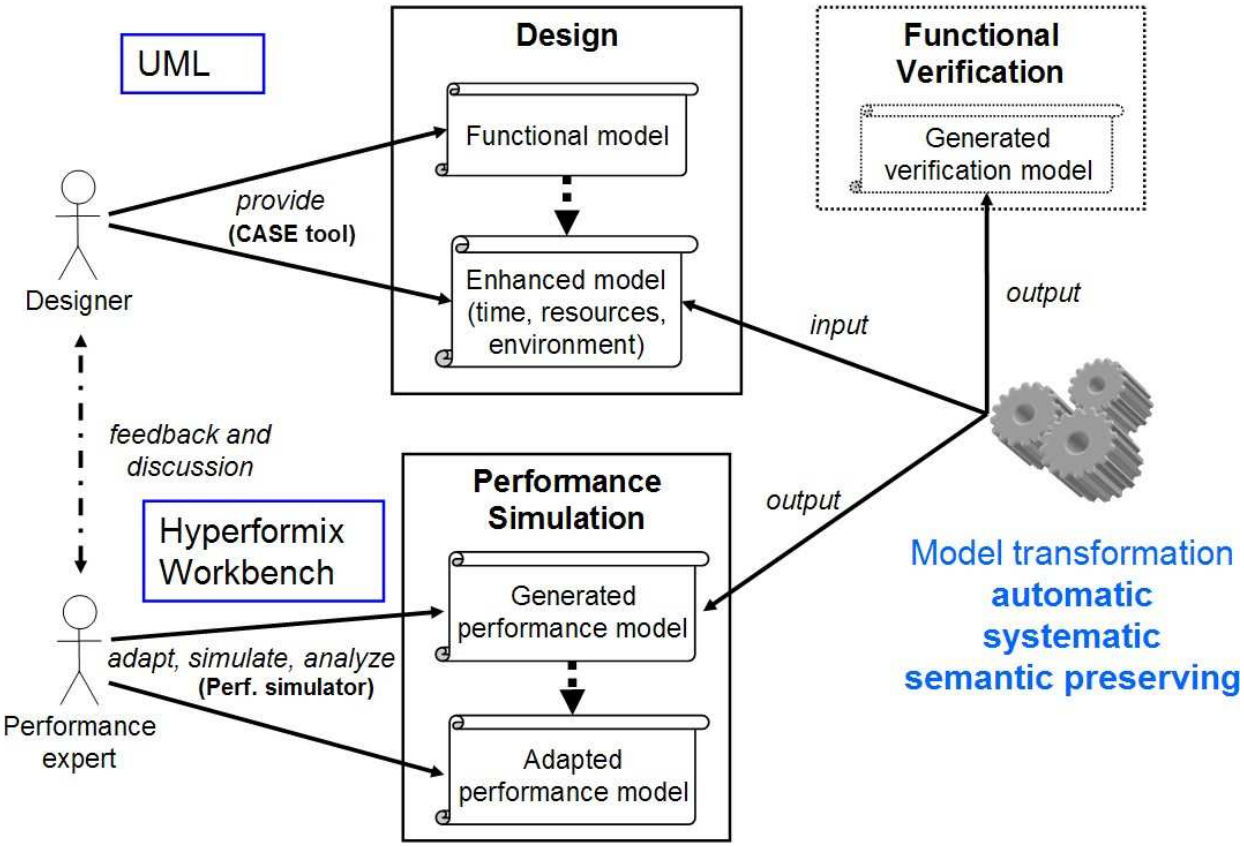

Figure 2.3-3: Persifrom methodology

During this year, we have improved the transformation tool chain by extending it to all the concepts of the user language. In addition, a successful experiment has been carried out on the support for functional analysis, by transformation of intermediate annotated Petri nets into Promela specifications. We have also significantly improved the layout generation tool which is needed in order make the resulting Hyperformix model exploitable. We have not foreseen

automatic feedback to the functional model as this would restrict too much the class of models that we can expect to be able to handle. This tool provides a first step towards the a fully integrated functional/performance analysis tool chain. The tool chain has been modularly designed so as to be extendible to other user-level design languages, as shown by the addition of MSCs as input language for the tool, which could be done very easily. This shows also the pertinence of the intermediate semantic format. The tool chain has been demonstrated on two small industrial case studies. One of them allowed to compare and validate the tool chain against the traditional "from scratch" approach to the construction of performance models.

The project is now successfully terminated. The results on the tool chain, the methodology are published in a technical report [CGM07] submitted for publication, and more results, in particular on the semantics and on the case studies, will be published in a near future.

After the termination of the Persiform project, we plan to reuse and extend the Persiform tool chain in other research projects. In particular, it will be used in the OpenEmbedd project, in two ways: it will be used as an exemplary show case for the use of the ATL model transformation tool, and it will be integrated also into the platform by connecting it to one of the OpenEmbedd modelling languages and applied in a case study provided by Airbus who has important needs for the kind of performance analysis targeted by our tool.

More recently, we 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.

The aim of 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 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).

In the next period it is planned to develop a framework for defining and validating component-based abstractions of a WSN that would allow performing more exhaustive verifications of energy-related properties.

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/), that pursues the work of EDEN, in order to reach a consolidated implementation for industrial exploitation.

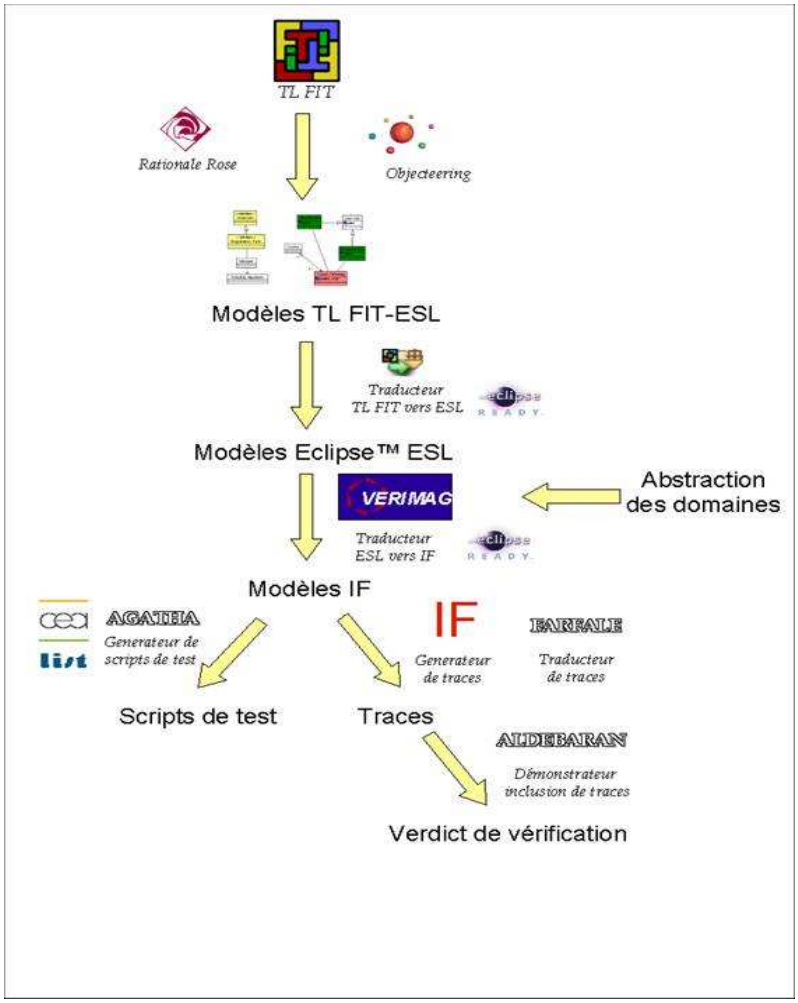

Figure 2.3-4: Architecture of the Eden platform

We have defined a methodology for the certification of smart-applications according to the International standard known as the *Comon Criteria* (CC) for security. 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. The TLFIT environment is based on the UML framework and produces both documentation and inputs for the verification tools.

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]).

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.

The projet has reached its mid term. During the next year, the work will mainly consist in finalising the tool set, applying it to an industrial case study provided by Gemalto and presenting the results to the French CC committee (DCSSI).

5. Transversal validation technology

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.

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. A series of theoretical results have been achieved. [FKPY07, KSY07] shows that the schedulability problem in the multiprocessor setting is already undecidable for systems with two processors.

To overcome these obstacles, we have been developing approximation and abstraction methods. As an abstraction for timed automata, we have adopted arrival curves of the network calculus as communication and resource consumption interfaces for compositional modeling and validation. A prototype tool (named ***CATS***) for compositional timing and performance analysis has been developed for systems modeled using timed automata and the real time calculus developed at EPFL. It is based on an over-approximation technique in which a component of a system, modeled as a timed automaton is abstracted as a transducer of event streams described by arrival curves from the real-time calculus. This allows us to characterize the semantics of a system as a set of equations over streams. Many interesting properties such as schedulability and buffer boundedness can be checked in solving the equations. The CATS tool is implemented in the Eclips tool platform. As the main feature of the current version, it 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. To scale up the verification technique based on timed automata, a recent work has also applied the partial order method developed in our group to component-based real-time systems, with promising experimental results [HP07].

The symbolic exection 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. In parallel the same technical architecture based on the EMF Eclipse repository and model transformations using ATL has been extended for exploitation of Matlab/simulink and Statemate models (this last work is supported by two projects of the System@tic Paris-Région pole of competitivity: the Eureka SysPEO project and the French project HeCoSim – www.projet-hecosim.org).

The ***BIP verification engine*** (http://www-verimag.imag.fr/~async/BIP/bip.html). In the previous periods, we started to develop sufficient criteria for guaranteeing properties of ***BIP*** component systems by exploiting the fact that BIP separates the description of component behaviours and of the way components interact and execute. In previous year, we did mainly theoretical studies [GGM+07a], [GGM+07]; this year, we started to implement these methods, to experiment them and finally propose quite substantial improvements. The initial idea was to use a dependency graph with a number of nodes linear in the number of components and connectors such that deadlock freedom can be guaranteed by absence of cycles satisfying a

certain constraint. It turned out that in practice the number of potential cycles that have to be eliminated by checking the constraint is very high.

We improved the algorithm by avoiding the explicit construction of the graph on one hand, and by conjoining the cycle condition with invariants on the other hand. We have started to generate both local and global “synchronisation invariants” for this purpose.

Uppaal/DMC. In cooperation between OFFIS and Aalborg the model-checker Uppaal has been extended with directed model-checking techniques [KD*07, KD*07b] within the AVACS (http://www.avacs.org) project. This improves the ability to find error states because less memory and less computation time is needed in comparison with the standard search methods. This improvement was an prerequisite for a counter-example guided abstraction refinement (CEGAR) approach for timed automata. Using this method, instead of the full model, a sequence of step-wise refined abstractions is analysed and due to the directed model-checking techniques the latter approach is faster in most cases.

Algorithms for the ***Analysis of Hybrid Systems with Large Discrete State Spaces*.** [DD*07], [Seg07] While the tools KRONOS and UPPAAL excel in the analysis of hybrid systems with complex continuous dynamics, many applications, for instance in embedded control, also exhibit a high degree of discrete complexity. The analysis of such systems calls for extensions of the techniques employed. The IF-toolset combines symbolic analysis for the timing part with highly efficient state space exploration for the discrete part.

In cooperation with the CvO University Oldenbrug, MPI Saarbrücken and the U. Freiburg, OFFIS has pursued approaches which combine other techniques which have proven successful in the discrete world (binary decision diagrams, and-inverter graphs) with first-order reasoning for the continuous part, resulting in deeply integrated analysis algorithms for such hybrid systems. They have been successfully applied to systems with very large discrete state spaces taken from industrial case studies.

***Pattern based real-time analysis for implementations*.** In contract based development, e.g. provided by the usage of Rich Component Models within the SPEEDS environment, requirements are specified in terms of computational denotation, i.e. automata, due to their expressiveness and flexibility. Verifying that design specifications fulfill requirements spaning by its contracts can be efficiently achieved by using state of the art COTS tools, like UPPAAL. While the quality downto the implementation level for the functional behaviour can be sustained using code generation, for extra-functional behaviour this typically is not the case. In particular this holds for the temporal behaviour which at the implementation level is defined by the usage of dedicated operating systems. However, there exist powerful analytical methods which provide the capability of assessing the timing behaviour of implementations on the operating system level. In order to achieve a seamless, quality preserving development, the gap between analytical methods with their strength on detailed assessment of behaviour at the implementation level and computational methods with their strength on expressiveness at the specification level has to be closed. Here we introduced the so-called Cyclic Timed Automata (CTA) to build a semantically sound bridge between both worlds. CTAs are templates of timed automata representing the temporal behaviour of components at the implementation level which is caused by the application of dedicated scheduling. We have shown that the CTA classes we derived are sematically equivalent to a trace based semantic interpretation of the analytical methods for assessing temporal behaviour. This paves the way for a seamless development, preserving design quality shown at the specification level downto the implementation. Furthermore, CTA characterizations are compositional, which allows their application in component based design, and at the same time provides efficient verification methods for checking the compatibilty of composition.

2.3.2 Individual Publications Resulting from these Achievements

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

Publications by **CEA**

[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.

[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.*

[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*).*

[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.

[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.

Publications by **INRIA**

[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.

Publications by **OFFIS**

[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

[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

[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.

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

Publications by **PARADES**

[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.

[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.

Publications by **Uppsala**

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

[KSY07] Multi-Processor Schedulability Analysis of Preemptive Real-Time Tasks with Variable Execution Times. Pavel Krcal, Martin Stigge and Wang Yi. In Proceedings of the 5th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'07), LNCS 4763. 2007

[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

[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)

Publications by **VERIMAG**

[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. Technical report, Verimag, 2007. submitted for publication.

[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. To appear in Fundamentae Informatice, 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

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

[Ngy] Thanh-Hung NGUYEN. Modélisation et validation d'un système robotique autonome en BIP. Master 2R Informatique, UJF Grenoble

2.3.3 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:

- Collaboration on MARTE has lead for CEA and INRIA ([FBSG07]) to the set up of a major industrial French project of the System@tic pole of competitivity, Usine Logicielle, in which implementation of the profile as Eclipse plug-ins is performed for RSA and Papyrus Open Source tool (www.papyrus-uml.org)
- Collaboration on MARTE has lead for CEA and U. Cantabria on research invitation to Julio Medina to contribute as post-doc at the CEA on the field of performance analysis. This has started at the end of this period and will continue during the next one ([EDG+07], [MLD+07], [MLD07], [MAP+07], [LMD07]).
- Collaboration between CEA and INRIA on has lead to a mapping between abstract and concrete syntax for action languages (with INRIA/Triskel) and to a second on meta-model and profile management (with INRIA/Aoste & Univ. Nice: [LTAG07a&b], [MFF+07]).
- Elaboration of a common semantic model for activity diagrams between INRIA, FTRD and VERIMAG and the implementation of a tool chain for the analysis of performance oriented models has lead to a complete tool chain and successful project termination in this period [CGM07].
- 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 [CCG+07]

- Collaboration between Verimag, CEA and externals on the organisation of the MARTES workshop [GGH+06]
- Collaboration between EADS and VERIMAG on the translation of AADL to synchronous languages in ASSERT
- Collaboration between INRIA, OFFIS and PARADES and VERIMAG on the definition of the SPEEDS metamodel HRC [BCSM07]. Collaboration on the definition of the verification methodology.
- Collaboration on 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
- Collaboration between FTRD and VERIMAG on porting THINK to BIP/IF has continued and lead to a common PhD work [BMP+07]
- Collaborations between VERIMAG and FTRD on performance analysis [CGM07], on use of BIP for validation of Think architectures [BMP+07] and in the ARESA project [DB*07]
- Collaboration between OFFIS and Allborg on the extension of Uppaal [DKL07]
- Collaboration between OFFIS and Saarbruecken in AVACS [ED*07]
- Collaborations on a model-driven approach integrating validation started in projects like SafeAir, OMEGA, and ARTIST have lead to new collaboration in projects such as SPEEDS, OpenEmbEDD and COMBEST.

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., I-Logic, TNI, ETAS, Carmeq, 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.

A new IST project that arose from the collaborations in ARTIST will start within the next year. Involved Artist partners 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.

The organization of different workshops in collaboration by several partners, also from other ARTIST platforms (see section 2.3.5) is another indicator of collaboration between these communities.

2.3.4 Joint Publications Resulting from these Achievements

[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.

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

[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

[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

[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

[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*).*

[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.*

[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*...*

[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.

[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.

[CCG+07b] Philippe Cuenot, DeJiu Chen, Sébastien Gérard, Henrik Lönn, Mark-Oliver Reiser, David Servat, Ramin Tavakoli Kolagari, Martin Törngren, Matthias Weber. Improving Dependability by Using an Architecture Description Language. Accepted book chapter contribution for the forthcoming book Architecting Dependable Systems IV. Editors: Rogerio de Lemos, Cristina Gacek, Alexander Romanovsky. LNCS, Vol .4615, 2007.

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

[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*).*

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

[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.*

[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) ; 03/04/2007 - 06/04/2007 ; Seattle ; US.*

[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) ; 19/09/2006 - 22/09/2006 ; Darmstadt ; Germany*

[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*

[DKL07] H. Dierks, S. Kupferschmid, K.G.Larsen; Automatic Abstraction Refinement for Timed Automata; FORMATS 2007; LNCS; Springer

[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.

[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.

2.3.5 Keynotes, Workshops, Tutorials

Summer school: ARTIST2 MOTIVES Winter School on Component & Modelling, Testing & Verification, and Statical Analysis of Embedded Systems
Trento, Italy, on Feb. 19-23, 2007

This summer school was jointly organized by the RTC, Verification, and Compilers clusters, with over 50 students and included contributions relevant to the platform activities
http://www.artist-embedded.org/artist/Overview,577.html

Workshop: MARTES 2006, Modelling and Analysis of Real Time and Embedded Systems; a satellite event of MoDELS/UML 20065, Int. Conf. on Model Driven Engineering Languages and Systems
Genova, Italy- October 2, 2006

VERIMAG and CEA have been the initiators of this workshop on model-driven development and real-time and embedded systems as a follow-up event on the successful workshop series on Real time embedded systems SIVOES and SVERTS. MARTES has been hold in October 2006 as a satellite event of the MODELS conference. The workshop attracted a number of interesting submissions and participants. The results of the workshop, as well as 2 best papers have been published in an LNCS volume. http://www.martes.org/

Workshop : FMCO 2006, 5th Int. Symposium on Formal methods for Components and Objects
Amsterdam – November 7-10, 2006

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. This symposium is a four days event organized to provide an atmosphere that fosters collaborative work, discussions and interaction. The program consists of keynote and tutorial presentations which are published in an LNCS Tutorial proceedings. VERIMAG is a co-organiser of this event
http://fmco.liacs.nl/fmco06.html

For 2007, we are preparing a special issue of this symposium bringing together groups of a set of related EU projects and NoEs; Artist is one of those groups.

Workshop : Towards a Systematic Approach to Embedded Design, a satellite event of
DATE 2007
Nice, France – April 20th, 2007

This workshop has been coorganised by KTH and VERIMAG as an interplatform meeting. The aim of this workshop was to increase awareness for potential industrial users about existing leading-edge academic embedded systems design tools. Results from several Artist platform activities and related external tools and challenges where presented..
http://www.artist-embedded.org/artist/Organisers.html

Workshop : Artist Workshop: Tool platforms for Embedded Systems Modelling, Analysis and Validation, a satellite workshop of
CAV 2007, Conference on Automated Verification
Berlin, Germany – July 1-2, 2007

This workshop has been coorganised by CEA, Aalborg University, KTH and VERIMAG as a follow-up of the interplatform meeting with DATE. The motivation for the workshop was the discussion of the specific problems raised in the context of embedded systems and the presentation of solutions from the perspective of design and development. The main aim was

to intensify the cross fertilisation between the formal methods and the embedded systems communities. Results from several Artist platform activities and related external tools and challenges where presented. http://www.artist-embedded.org/artist/Organisers.html

Workshop: Perspectives on integrating MDA and V&V (MoDeV2a'06)
MoDELS'2006
Pisa, Italy – October dates, 2006
The workshop has been organised by CEA, INRIA and University of Queensland (Australia) in conjunction with the MoDELS conference. V&V is an established area of research, and a transfer of ideas between V&V and MDA might help to improve quality and reliability of MDA and induce a new conceptual way of thinking in established V&V. So it is crucial to go beyond model-based testing and take a truly model-driven-development approach to V&V to reap even greater benefits.

http://modeva.itee.uq.edu.au

CAV 2007-19th International Conference on Computer Aided Verification
Berlin, Germany, July, 3-7, 2007

The 19th International Conference on Computer Aided Verification, CAV 2007, was held in Berlin from July 3-7, 2007, sponsored by – amongst others – the ARTIST2 NoE.

The CAV conference series is dedicated to the advancement of the theory and practice of computer-aided formal analysis methods for hardware and software systems. It covers the spectrum from theoretical results to concrete applications, with an emphasis on practical verification tools and the algorithms and techniques that are needed for their implementation. The proceedings of the conference are published in the Springer-Verlag Lecture Notes in Computer Science series.

On its tutorial day, CAV 2007 hosted 4 invited tutorials, by Tom Henzinger, EPFL (Switzerland), on *Modeling, Verification, and Synthesis of Component Interfaces,* Natarajan Shankar, SRI (USA), on *Satisfiability Modulo Theories,* Gary T. Leavnes, Iowa State University (USA), on the *Java Modelling Language*, and Martin Fränzle, CvO University Oldenburg (Germany), on *Verification of Hybrid Systems.* The main program of the conference featured 3 invited talks, by Byron Cook, Microsoft Research (UK), David Russinoff, AMD (USA) and Thomas Kropf, Robert Bosch AG (Germany), as well as talks about 33 regular papers and 14 tool presentations, carefully selected from a record number of 173 submissions.

CAV 2007 was accompanied by seven satelite events, several of them related to Artist or organized by or with the participation of Artist partners

http://cav2007.org/

Workshop Modeling and Safety Standards - How to Get it Right
SafeTronic 2006:
Munich, Germany, November 14, 2006.

Speakers: Hardi Hungar (OFFIS), Oliver Plan (Berner&Mattner Systemtechnik), Almuth-Ines Spiess (TÜV Süd Rail)**.** A one-day tutorial has been held at the SafeTronic 2006 explaining how to use UML in the development of safety-critical (rail) systems by employing the language Safe-UML. There were about 25 participants, mostly from industry. It was demonstrated how the requirements layed down in domain-specific standards (here: the CENELEC standards EN 50126 and 50128, which have been derived from the more general IEC 61508) can be met in a development using UML. Adhering to the restriction of Safe-UML was shown as a key ingredient in this process.

Seminar on "Tools for the model-based development of certifiable, dependable systems"
Dagstuhl, Germany, 10.06.-15.06.2007

Transportation is an important application field of embedded systems. In this domain, the design of systems faces the challenge of not only producing a system which performs its function correctly, timely and reliably, but also of documenting to authorities that this is the case, if the system's is of safety-critical nature. This requirement has strong impact on the design process, as there are domain-specific standards which need to be followed.

Though the current practice largely seems to achieve its goal - as can be seen in the low percentage of accidents being attributable to design flaws - there are strong arguments to look for improvements. On the one hand, the effort to achieve sufficient confidence is rather high. And on the other hand, formal methods seem to have matured to a state that even a mathematically rigorous proof might become achievable.

To do this constitutes a challenge for the formal methods community with many facets: Not only several sorts of formal arguments (concerning e.g. timing, function and fault probabilities, different design levels, software and hardware and so on) are called for, but also evidence for the trustworthiness will be required. If e.g. a model checker verifies a property, it either must itself be verified or produce a proof for its verdict which can be validated by other means. To this end, existing approaches will have to be extended and combined into coherent, comprehensive methodologies.

To discuss these questions, Hardi Hungar (OFFIS) together with Michaela Huhn (TU Braunschweig) and Doron Peled (Bar-Ilan Univ.) organised an international seminar in Dagstuhl (Seminar 07421, 10.06.-15.06.2007). Using a realistic case study (a level crossing) techniques, tools and approaches were discussed by the participants. Differences in approach and background – as both the scientific as well as the industrial world was represented – showed up, resulting in mutual learning and common conclusions to be documented in the forthcoming workshop proceedings.

Keynote : Reasoning about the Trends and Challenges of Engineering Design Automation
20th Int Conf on VLSI Design and 6th Int Conf on Embedded System Design
Bangalore, January 6-10, Bangalore, India

Alberto Sangiovanni Vincentelli gave a keynote talk.
http://vlsiconference.com/vlsi2008/sitemap.htm

Keynote :
FORTE 2007
Talinn, Estonia – June 26-29, 2007

Susanne Graf presented an extension of the BIP framework to hierarchical components allowing encapsulation. This extension will be applied in the context of modular verification of system designs.
http://cs.ttu.ee/FORTE07/

3. Future Work and Evolution

3.1 Problem to be Tackled over the next 12 months (Sept 2007 – Aug 2008)

Globally, the work will continue according to the last 18 month plan, the tool chains which started to be developed will be further extended and/or connected. New activitiess will be integrated and new projects defined. The initially planned tool integration through jETI is left as an interesting future perspective. The work on the platform for the certification of smart-card applications on which there was less progress in the second year has caught up and will achieve its goal.

Ou research work will concentrate on enlarging the existing tool chain kernels by means of new model transformations, and by bringing the modelling standards closer together.

Modelling languages and semantic frameworks and their implementations

There will be less work on the modelling formalisms themselves which are more or less defined. There will be some work on consolidation and some extensions, in particular for HRC which has not yet be assessed sofar. 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.
- Evaluate the capability of the Executable UML profil to support description of heterogeneous MoCs and demonstrate consistency.
- Full implementation of HRC and model transformations to analysis tools formats. It is also planned to enhance tool vendors code generation to make HRC components usable for model simulation, but this may not be achieved in one year
- An important plan for BIP is an execution engine for semantic preserving distributed execution as well as the integration of new analysis techniques. This will be used for defining specific frameworks dedicated to application domains or for handling specifications defined in particular languages.
- An extension of Metropolis II to deal with the design of distributed systems so as to be able to considering applications such as intelligent buildings. We will study an extensible mathematical programming approach to deal with latency requirements. The mathematical programming approach offers another unified framework to the synthesis of architectures. The design space we consider is the allocation of tasks to processing units, the choice of priorities, the periods and the activation models of the tasks. This work will be carried out in collaboration with the Gigascale System Research Center in the US and with PARADES and INRIA.

Platform for the analysis of safety critical embedded systems

The main future work on this platform will be carried out within the IP project SPEEDS and the System@tic/Usine Logicielle projects OpenEmBeDD and ATTEST. They will concern the missing connections between the modelling languages used and the back-end tools via semantic level intermediate formats.

Existing analysis tools will be extended to support the HRC (heterogeneous rich component) models developed in SPEEDS. In order to achieve scalable analysis, this requires more than just the adaption of existing analysis tools to HRC. We will define specific transformations for transforming various analysis problems (consistency, compatibility, contract dominance, contract satisfaction,…) to analysis problems as they can be solved by tools. In addition a process advisor tool will use analysis results to monitor system progress. This activity may start to show significant results only in the third year (after the end of Artist).

The work on the BIP/THINK/Buzz tool chain will focus on the validation of the BUZZ approach on a lightweight concrete operating system such as TinyOS. Beside this concrete target we also plan to improve the existing link between BUZZ and the analysis and verification tool set provided with BIP. We also expect to link BUZZ to existing developments in FT involving security enforcement architecture (mainly access control and authentication). This work will result in an IDE able to support the development of secure embedded operating systems offering a fully characterized and predictable run time behaviour.

The work on validation and compilation from other architecture description languages, in particular AADL, will continue to be studied in ASSERT and in SPICES

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.

Integration between the MARTE standard and the automotive domain, and in particular with Autosar standard will be continued in ATESST project. The EAST-ADL profile will be extended during next year in order to ease the modelling of product families (or product lines) by adding elements of variability description, in particular for variation of component behaviour.

Another line of work on the MARTE profile will be on its integration along the whole system development process through defining traceability support for UML based development in embedded system. Based the three UML profiles SysML, MARTE and EAST-ADL 2, an Eclipse component will be developed within the MemVaTEx French project.

Platform for the 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, it is planned to develop a framework for defining and validating component-based abstractions of a WSN that would allow performing more exhaustive verifications of energy-related properties.

Platform for the certification of smart-card applications

The work on this platform continues to be carried out in the EDEN-2 project and will mainly port on functional validation of critical applications on smart cards. During the next year, the work will mainly consist in finalising the tool set, applying it to an industrial case study provided by Gemalto and presenting the results to the French CC committee (DCSSI).

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:

The evaluation of the capabilities of the symbolic execution kernel Agatha to deal efficiently with hybrid and heterogenous formalisms as used in automotive industry. Finalise component based test generation from whole system requierement specifications for security application Models.

We will continue to work on the improvement of the BIP analysis engine by improving the automatic abstraction mechanisms provided by a system structure. Partly, these algorithms will rely on specific methodologies satisfying particular constraints.

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) will continue 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.

Compositional Safety analysis: within the next year we will investigate failure models suitable for compositional safety analysis. Derived from compositional safety analysis (underway) we will enrich existing failure models to improve the compositionality of the safety analysis (i.e. producing less pessimistic results). Also the question of how to "link" these failure models to physical failures will be addressed. The "link" needs to guarantee that the completeness of a safety statement (wrt. the high-level failures) is preserved when looking at the physical level. In particular this requires elaborating on an adequate notion of failure subsumption.

Collaboration and Dissemination

Like already in previous years, we will privilege open meetings and organisations of workshops over cluster meetings in a closed format. Some workshops are already planned, others will be defined in a close future: In particular, we reorganized the MARTES and MoDeV2a workshops with MoDELS in Toulouse.

The organization of a platform workshop as a satellite workshop of an appropriate major conference. Like this year, we will organise an interplatform workshop associated by some convenient conference. The workshop SafeCert08 is organised by OFFIS and Braunschweig as a satellite event of ETAPS. A Dagstuhl seminar is planned on verification methods for concurrent systems.

3.2 Current and Future Milestones

3.2.1 Plans and Milestones as stated in the Y2 deliverable

- 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.

3.3 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 20 joint publications, where most of them imply more than 2 platform partners. This number has been strongly increasing since the beginning of the project (for example, in the year-2 deliverable contains only about 5 joint publications.

- Joint workshop organisations

  There are several workshops organised by several partners of the platform, and their number is increasing. In this year, there are in particular two workshops that were organised jointly by partners of several ARTIST platforms, the first one as an satellite event of DATE, the second as a satellite event of CAV.

- 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 4 Artist partners and several associated industrial partners, the SPICES ITEA project with four Artist partners and numerous French projects involving several French Artist partners. Next year will start another EU project involving 7 Artist partners and 2 associated industrial 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, all the activities grouped in the 3 platforms are development involving at least 2 Artist partners.

3.4 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 4 come from the following sources:

- 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)
- EDEN 2 (http://www.eden-rntl.org/, for CEA, VERIMAG), French national RNTL project on UML based development and verification of security critical system
- STACS (for CEA, Thales -- terminated), French national RNRT project on validation and testing of heterogeneous component based models
- PERSIFORM (http://www-persiform.imag.fr/, for FTRD, INRIA and VERIMAG -- terminated), a French National RNRT project on functional and performance analysis of service oriented specifications (terminated in August 2007).
- CREDO (http://www.cwi.nl/projects/credo/, for Uppsala), supported by EU, Modeling and analysis of evolutionary structures for distributed services
- SAVE++ (http://www.mrtc.mdh.se/SAVE/, for Uppsala) supported by Swedish strategic research. Component Based Design of Safety Critical Vehicular Systems
- Modeling and verification of timed systems (for Uppsala) financed by the Swedish research council
- 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.
- 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.
- 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.

- 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
- OpenEmBeDD (http://openembedd.inria.fr/home_html, 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.
- Industrial funding (Pirelli, Ferrari, United Technology Corporation, Cadence, ST) for the Metropolis II and its application were provided to PARADES.
- SysPEO Eureka project (ARTIST partners CEA and Leuven) is centered on verifying Matlab and Simulink model in the automotive model through formal techniques using the Agatha symbolic execution kernel.
- HeCoSim French project (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.
- 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.
- ARESA (http://www-verimag.imag.fr/SYNCHRONE/index.php?page=fiche-aresa, for Verimag and FTRD), French National project on modelling energie consumption of Sensor networks
- AVACS (http://www.avacs.org/, for OFFIS) on Automatic Verification and Analysis of Complex Systems, Transregional Collaborative Research Center.
- 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.
- COMBEST 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 will start within the next year.

4. Internal Reviewers for this Deliverable

Alberto Sangiovanni Vincentelli (Parades, cluster internal)
Martin Torngren (KTH, external to cluster)