ARTIST 2

Network of Excellence

IST-004527 ARTIST2:
Embedded Systems Design

Activity Progress Report for Year 2

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 3
1.1 ARTIST2 Participants: Expertise and Roles 3
1.2 Affiliated Participants: Expertise and Roles 3
1.3 Starting Date, and Expected Ending Date 4
1.4 Baseline 4
1.5 Problems Tackled in Year2 4
1.6 Comments from the Previous Review 7
1.6.1 Reviewers' Comments 7
1.6.2 How These Have Been Addressed 7

2. Summary of Activity Progress 8
2.1 Previous Work 8
2.2 Current Results 10
2.2.1 Technical Achievements / Outcomes / Difficulties encountered 10
2.2.2 Publications Related to these Achievements 16
2.2.3 Keynotes, Workshops, Summerschools, Tutorials 17

3. Future Work and Evolution 20
3.1 Problems to be tackled over the next 18 months (Sep 2006 – Feb 2008) 20
3.2 Current and Future Milestones 22
3.3 Indicators for Integration 23
3.4 Main Funding 24
3.5 Internal Reviewers for this Deliverable 25

1. Overview of the Activity

1.1 ARTIST2 Participants: Expertise 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: Sebastien 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: 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: Jean-Marc Jézéquel (INRIA)
Contributions of his team: UML-based model transformation technology.

Team Leader: Noël Plouzou (INRIA)
Contributions of his team: Model transformations and aspect orientation, tools

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

1.2 Affiliated Participants: Expertise 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: Martin Torngren (KTH)
Contribution of his team: liaison with the control cluster, participation in the IST project ATTEST contributing to the platform

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.

Team Leader: Bernhard Steffen (University Dortmund)

Contributions of his team: tool integration platform jETI.

1.3 Starting Date, and Expected Ending Date

Started: September 1st, 2004

Expected Ending date: end of the project

Developing modelling and validation platforms for modelling standards is a long term effort. Several important projects have just started or will start their developments with scheduled activities close to the end of ARTIST 2. In particular two complementary projects will provide an important contribution to the platform: The SPEEDS IP project that has just started will provide an important contribution to the platform and will end after the end of ARTIST2. A large French project of the System@tic pole of competitiveness called Usine Logicielle (Software Factory) started at the end of 2005 with activities scheduled on a 3 to 5 years vision. We expect indeed the activities of this platform to go on after the prospective end of ARTIST2.

The work plan of this platform is a living document so that it can take into account developments outside ARTIST, such as the emergence of new standards or new technical trends. An important objective of the platform is to provide a discussion forum allowing exchange and sharing of ideas between projects working on methods and tools related to the platform.

1.4 Baseline

Before the beginning of ARTIST, UML began to be accepted as 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, TAU) and there exist also 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 Problems Tackled in Year2

In the first year of the project, we planned to aim at a platform with three tool chains, dedicated to slightly different types of applications (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

The problem tackled in the second year, was to actually start the tool integration work. As a result, some tool chains building an initial subset of the overall planned picture have been built by now, and according to the plans, new collaborative projects, initiated by the cluster participants have started and will contribute to the construction of more complete platforms.

For some of the now existing tool chains, demonstrations on case studies are available. We give here a short overview on the integration work, more detailed descriptions including all lines of work are provided in section 2.

- The work on the platform includes and strongly interacts with work on modelling standards and semantic level modelling formalisms, in particular
  - The MARTE UML profile for modelling real-time systems and their non functional properties, developed mainly with the support of the CARROLL research program (between CEA, INRIA and Thales) with the contribution of Cantabria and *Carleton University*
  - The "EAST-ADL 2" UML profile for **automotive architecture and component modelling**, is developed within the IST ATESST project with ARTIST partners CEA and KTH. Based on the ***Autosar***^{TM} meta-model it aims to provide a higher level of system modelling and to better support behavioural modelling aspects.
  - Converting the concept of **rich component models** into a mature framework for system design, in the form of of a SysML compatible profile, is pursued within IP-SPEEDS by the platform partners INRIA, OFFIS, PARADES, and VERIMAG.
  - The BIP framework providing a rich framework for incremental component composition (http://www-verimag.imag.fr/~async/index.php?view=components) based on a three layered structure developed by VERIMAG has been further developed and a platform for the efficient execution of such models has been implemented in this second year [BBS06].
  - Within the context of the SAVE Swedish national project, the Uppsala and Mälardalen teams are developing *SaveCCM* (the SaveComp component model) [ÅCF+06].
- In the context of platform 1, several lines of integration work have been carried out
  - BIP/THINK collaboration has started this year. The goal of this BIP/THINK joint effort is to get 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.
  - The tool chain Kermeta-IF-Giotto providing software development support starting from the formal specification of components and composition verification down to the generation of Java or C based executable units.
  - In the context of the French National project OpenEmbeDD (http://openembedd.inria.fr), which includes the ARTIST Partners CEA, France Telecom, INRIA, Thales, and VERIMAG, work will start on mappings from the user level formalisms SDL and the MARTE UML profile to the semantic framework of BIP, developed at VERIMAG and to INRIA's Kermeta model for further connection with validation tools.
  - In the SPEEDS project IP SPEEDS, with partners INRIA, OFFIS, PARADES, and VERIMAG, has started this year. The work involves the development of a system level UML/SysML compliant framework for heterogeneous components,

which will benefit from MARTE; it will be connected via semantic level formats like BIP to the validation platforms IF, Metropolis and RUVE.

- The work on the platform 2 that had already started within the French national Persiform project (http://www-persiform.imag.fr) with ARTIST partners FTRD, INRIA and VERIMAG, aiming at performance evaluation for both functional and design specifications of component-based services to be integrated into service platforms has well progressed [BCGMM-06]. An initial end-to-end tool chain is available and can be demonstrated on small case studies.
- The work on the platform 3 is supported by a collaboration among CEA and VERIMAG on functional validation of critical applications on smart cards. This work is carried out in a national project, EDEN 2, that continuous the work started in EDEN, in order to reach a consolidated implementation for industrial exploitation.
- Within the platform activities, we have carried out also some work on validation techniques, in particular methods intended to handle specific features or structure of the modelling languages used in the platform:
    - Some results for the verification of systems with asynchronous communication channels have been obtained [KY06] and are being implemented in UPPAAL.
    - Some verification methods exploiting the layered structure of BIP models, in particular for verifying absence of deadlock or interlock have been developed [GGMSM06] and are being implemented.
    - The **symbolic execution kernel**, Agatha, has been extended to support analysis of heterogeneous model using **heterogeneous models of computing**. Developed by CEA through two national projects (STACS and Usine Logicielle).

The work on the integration of tools at the user interface level and on the web-based execution of tools that was planned to be done with the help of the jETI environment developed by the team of Dortmund, has not been further pursued for now. It is still considered important, but given the degree of maturity of the existing chains, it has been considered premature to attack this kind of considerations immediately.

We have also actively continued the dissemination work by means of publications and by organising workshops and summer schools, in particular the MARTES workshop in October 2005 and the workshop on “MDD for Distributed Real Time Embedded Systems” held in September 2006. Contrary to the plans, we have held no formal plenary platform meeting, but many small meetings of subgroups, in particular jointly with the Autosar workshop in Innsbruck and with the MARTES workshop, and also within the associated collaborative research projects. (see also special section on dissemination in section 2.2.3).

1.6 Comments from the Previous Review

1.6.1 Reviewers' Comments

D2.1: Components Platform for Component Modelling and Verification: ACCEPTED

Report PDF file created 15/12/2005, updated version 18/01/2006

This task aimed to define a common kernel language for modelling real-time systems and translation from UML notation to this language. Analysis tools should be integrated with each others around three platforms and adapted according to the common language. The objective has been partly redefined replacing the common language by a semantic level approach.

page 8 of 27 This deliverable has been previously rejected for the following reasons: no global picture existed in term of state of the art, convergence of work between partners and the interaction between partners was not mentioned. The steps to reach the announced goal: "defining a common kernel language for modelling real-time systems and translation from UML notation to this language" did not appear.

The changes compared to the initial plans are now explained: merging of clusters component and modelling with real-time that should increase the importance of one of the three platforms, revision of the objective of a common language for modelling real-time systems that is now replaced by a semantic approach and reduction of objective on standardisation.

The state of the art now shows partners contributions as requested in the first review report.

The activity of integration among partners appear more clearly and should concentrate in the next months around the three component platforms, the integration of tools and the definition of semantic profile for analysis and simulation tools.

The deliverable is accepted, and ***it is expected that the technologies commons to this activity together with the integration tasks will be stressed in the Year 2 report****.*

1.6.2 How These Have Been Addressed

The main requirement from the last review report concerns integration of the work done by the different partners institution and explaining the commons between the different lines of work.

We believe that we have well taken into account these recommendations in the following way:

- We have actually started to build tool chains from modelling languages to validation tools, based on the connection to semantic level formats shared between several chains and using model transformation technology.
- We increased the focus of the platform by concentrating in this second year on two of the three planned platforms and by focussing on the interconnection between modelling languages and semantic level formalisms by means of model transformation techniques. We postponed to a later point of time the integration of the tools at user level by means of the facilities provided by the jETI platform. Such a stronger tool integration is however still considered relevant, once tool chains based on common exchange formats and model transformations have been achieved.

2. Summary of Activity Progress

2.1 Previous Work

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 held in Grenoble in October 2004, in Paris in January 2005 and in Rennes, at the end of June 2005. The June 2005 meeting has been hold in common with the hard real time and the adaptive real time clusters.

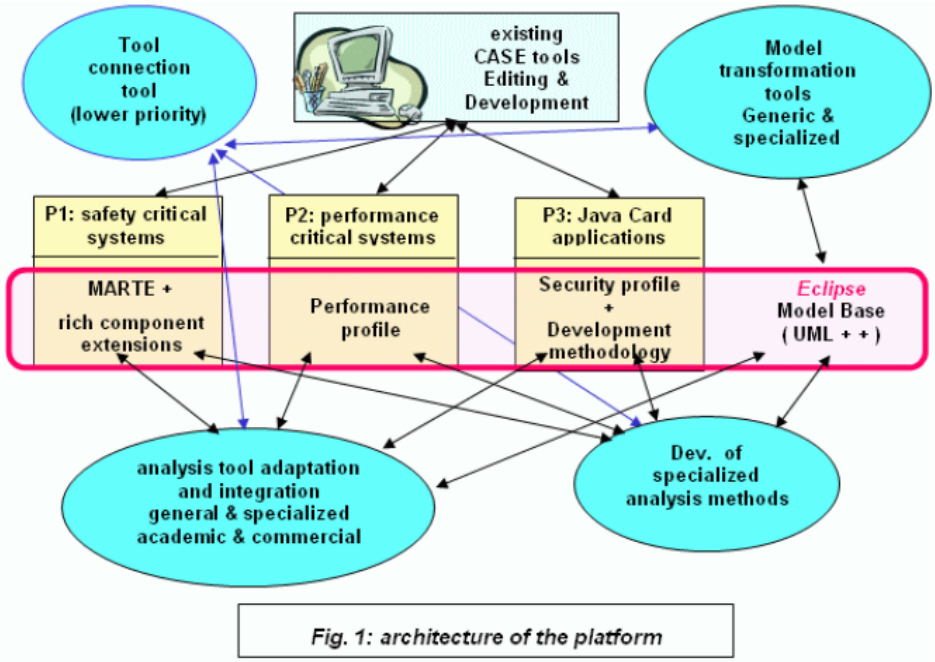

Fig. 1: architecture of the platform

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 or will be made UML compatible. 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 (started 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 mainly 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 projects.

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 Current Results

2.2.1 Technical Achievements / Outcomes / Difficulties encountered

The outcomes and achievements of this second year are structured into 5 sections,

1. Modelling languages and frameworks for providing semantic foundations,
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 interaction with standards

The work on the platform interacts with and depends on several activities related to the development of UML-based modelling languages and the development of formalisms for a semantic level representation of models. An important goal is achieving tool chains for related profiles by mapping them to a small set of semantic level formalisms used in validation and code generation tool chains. This should finally allow handle models more than one profile simultaneously. This section presents both user-level and semantic-level formalisms. In fact, the separation between these levels is sometimes narrow, as user-level profile will lift some of the concepts useful for validation at the user level and in some cases may be used for both purposes. We start with those clearly meant as user level language and pass then to semantic level formalisms.

The **MARTE UML profile** [EDG+05] for modelling real-time systems and their non functional properties, plays a central role as a user level format. The effort involves *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 [EMDG06] and for schedulability related issues [LMD06, MLD06]. It is now close to an acceptance as an OMG standard (see report on the standardization issues) and has started to be implemented. It will be a base for an open source modelling and validation platform developed in the OpenEmBeDD project. The development of this profile, its implementation as an Eclipse component and its integration to the RSA IBM tool requires a huge amount of work and feedback from a large panel of end users. For that, it benefits from the support of two large French projects:

- The Usine Logicielle (Software Factory) project of the System@tic pole of competitivity (involving as end users in addition to the previous partners: EADS, Dassault Aviation, Hispano Suiza, EdF, MBDA, CS… see www.usine-logicielle.org). In this project, MARTE standard is also implemented as an Eclipse component
- The OpenEmbeDD platform (involving as end users in addition to the previous partners: France Telecom, CS, Airbus)

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™* meta-model, it aims to provide a higher level of software component modelling and to better support behavioural modelling aspects. It complements for the automotive domain the MARTE profile, in particular, through specialisation of the UML component concept by a tight mapping on the Autosar™ paradigms. This Autosar™ mapping

limits its capabilities of managing dynamic interaction among components and will benefit from on going works done in the cluster on “rich component models”. It will provide an Eclipse component within the IST ATESST project developed by CEA, KTH and TUB together with their industrial partners (Volvo Tech., Daimler Chrysler, Siemens VDO, etc., see www.atesst.org).

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 and when deployed in a particular domain of application, has to be instantiated for a concrete, tool-supported environment; in addition, different restrictions and specializations apply to different development stages. The profile focuses on structural diagrams (class diagrams) and behavioural diagrams (state charts). The main general restrictions concern event handling (no unbounded message queues) and control of non determinism (in concrete implementation specs). Part of the specifications concern UML on a general level and define Safe-UML (S), where (S) stands for seamless development. On a more concrete level, the UML tool Rhapsody in C++ is considered, yielding Safe-UML (R), (R) for Rhapsody. Finally, Safe-UML (V) treats formal verification with the model checker RUVE. The aim of the Safe-UML definition is twofold. On the one hand models following this profile shall be compliance to standards (for example code compliance with the German railway guidelines MÜ8004 for the generated code) and on the other hand it is expected that verification tools based on Safe-UML can significantly be improved from a performance point of view in relation to a general UML verifier.

The work to develop 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. They are currently developing a meta-model for rich components, called **HRC**. This includes defining a notion of component for which different *viewpoints* (functional, times, safety, etc) can be synchronized, and different viewpoints for different components can be formally composed. It will comply with existing or de-facto standards, including the Autosar real-time component model, UML 2.0 (in particular SysML profile) [DVMJ05, Da06]. The work in SPEEDS also involves a new theory of *interfaces* is being developed, allowing for cross-viewpoint assume-guarantee reasoning. This piece of work undertaken within the SPEEDS project is a clear by-product of previous and current work developed in the ARTIST community (for more background, see RTC cluster report).

The **BIP framework** (Behaviour, Interaction, Priority) developed at VERIMAG over the last 5 years [GS05, BBS06] will play an important role 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. A key abstraction in system design is the one relating application software to its implementation on a given platform. Application software is often largely untimed, whereas the application code running on a given platform, however, is a dynamic system that can be modelled by a set of timed or hybrid automata. The run-time state includes not only the variables of the application software, but also all variables that are needed to characterize its dynamic behaviour, such as time variables and other quantities used to model resources.

The aim of the BIP framework is to provide a semantic framework for such systems of heterogeneous components.

- It supports a component construction methodology based on the thesis that components are obtained as the superposition of three layers. The lower layer describes *behaviour*. The

intermediate layer includes a set of *connectors* describing the *interactions* between transitions of the behaviour. The upper layer is a set of *priority rules* describing scheduling policies for interactions. Layering implies a clear separation between *behaviour* and *structure* (connectors and priority rules).

- It uses a parameterized *composition* operator on components. The product of two components consists in composing their corresponding layers separately. Parameters are used to define new interactions as well as new priority rules between the composed components. It allows *incremental* construction, that is, any compound component can be obtained by successive composition of its constituents. This is a generalization of the associativity/commutativity property for composition operators.
- It provides a powerful mechanism for structuring interactions involving both strong synchronization (rendez-vous) or weak synchronization (broadcast). Synchronous execution is characterized as a combination of properties of the three layers. Finally, timed components can be obtained from untimed components by applying a structure preserving transformation of the three layers.
- It allows considering the *system construction process* as a sequence of transformations in a three-dimensional space: *Behaviour* X *Interaction* X *Priority*. A transformation is the result of the superposition of elementary transformations for each dimension. This provides a basis for the study of property preserving transformations or transformations between subclasses of systems such as untimed/timed, asynchronous/synchronous and event-triggered/data-triggered.

The CEA, INRIA and Thales teams are contributing to the elaboration of a new standard: ***Executable UML foundation*** [MFJ05] that aims at providing a formal framework for defining an execution semantics of UML profiles in order to help harmonizing other standards. Its objective is to enable a chain of tools that support the construction, verification, translation, and execution of computationally complete executable models.

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. PARADES' industrial nature was essential in this step. 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 essential characteristics to be retained were:

- languages or conform to different models of computation.
- The capability of taking different parts of a design and refining/abstracting them such that these relationships can be verified.
- Relating together the architectural platform and the functionality in different ways to explore different realizations of the system. This design space exploration process may be carried out in terms of different metrics, such as throughput, latency, jitter, power consumption etc.

Like Metropolis the semantics of the Metropolis II framework will be centered around the connection and coordination of components. Unlike Metropolis, the components will be specified using external languages and the framework will serve 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 as Metropolis can describe with these primitive concepts both functionality and architectures. The role of quantity managers is essential in 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. 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 works carried out for this platform are building on UML profiles, in particular MARTE and HRC. The main efforts this year concern back-end tool chains, starting from one of the envisaged semantic level formats and integrating validation and code generation tools. The work on the front-end tools, providing mappings from user level profiles to semantic level formalisms has only started for MARTE and will start within the next year for HRC.

Two important collaborative projects for the platform have started this year which will provide the main contributions on this platform:

- The French National project OpenEmbeDD (http://openembedd.inria.fr), which includes the ARTIST Partners CEA, France Telecom, INRIA, Thales, and VERIMAG, work will start on mappings from the user level formalisms SDL and the MARTE UML profile to the semantic framework of BIP, developed at VERIMAG and to INRIA’s Kermeta model for further connection with validation tools.
- The SPEEDS project IP SPEEDS, with partners INRIA, OFFIS, PARADES, and VERIMAG, has started this year. The work involves the development of a system level UML/SysML compliant framework for heterogeneous components, which will benefit from MARTE; it will be connected via semantic level formats like BIP to the validation platforms IF, Metropolis and RUVE.

The INRIA team developed a tool chain using tools of several ARTIST teams (mainly 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 model driven approach is then applied to build a platform dependent implementation. The concrete implementation is generated by model transformations using tools from *INRIA Triskell team*. The target architecture is the Giotto platform designed by the *EPFL* team. The tool chain covers the life cycle of timed components from the service specification in timed tree logic down to algorithms coded in Java and executed on a Giotto runtime. The tool chain implementation has been done by INRIA and is now completed. A future meeting of the RTC platform group will include demonstrations and technical discussions on further integration of this chain in the platform.

The BIP framework that will be extensively used in several projects has been implemented in a tool: the tool consists of a front-end for editing and parsing BIP and generating C++ code to be executed and analyzed on a backend platform consisting of an engine and the infrastructure for executing the generated C++ code. BIP 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 presently not for developing embedded operating systems kernels and low-level services. This will be tackled in the next period and a connection to the analysis tools of the IF tool-set is ongoing.

BIP has been and is being used for modelling several smaller case studies and some larger on systems in the context of performance oriented systems satisfying hard timing constraints, in the context of planning tasks of autonomous robots and in the context of modelling energy consumption in sensor networks.

BIP/THINK collaboration between FTRD and VERIMAG has started this year. The goal of this BIP/THINK joint effort is to get 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 for being able to handle UML specifications. It has been integrated in the Eclipse platform and the UPPAAL modelling language has been extended with hierarchical state machines, to support modelling of hierarchical structures and abstract behaviours of components. Presently, we are in progress to extend the UPPAAL modelling language with asynchronous communication channels. The idea is to use timed automata to describe the communication patterns and relative speeds of components in producing and consuming messages.

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 mainly) to functional UML modelling tools for high-level performance analysis, in particular service specifications expressed in terms of activity diagrams [BCG*06] and sequence diagrams. For this purpose, a profile for the use of activity diagrams has been defined and a formal semantics

has been through a mapping to a restricted class of coloured Petri nets plus annotations with probabilities and distribution concerning timing and resource usage. 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.

The initial chain has been applied to two industrial case studies on which the tool chain can be demonstrated.

For real time systems, work is performed on design specifications with performance annotations, compatible with the MARTE profile. These specifications will be transformed into IF models for validation of real time properties [HAB*05].

In the next period, mappings to tools for functional validation, in particular to IF or BIP are planned. As well as some work on representing observed traces during simulation by MSC. In the future, we consider mappings to other performance models.

4. Platform for the certification of smart-card applications

The work on this platform is supported by a 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, that pursue the work done in the previous one, EDEN, in order to reach a consolidated implementation for industrial exploitation. It has not progressed exactly according to the plans which foresaw the definition of a UML profile for security properties, but it turned out to be more important to concentrate in the first year rather 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; this topic is covered by the Verification cluster and platform activities and the background tools of the platform have been described in the year 1 deliverable. We describe here on some new developments directly linked to the connection of existing verification tools to the modelling languages considered in the platform.

An interesting technical challenge for adapting **UPPAAL for asynchronous models** is to check the boundedness of channels, and to synthesize the maximal size of memory blocks needed to implement the channels. Preliminary results are reported in [KY06] showing that the expressive power of such systems with two channels -- that are no more expressive than finite-state machines in the untimed setting -- is Turing-equivalent. We have been developing methods based on approximations. As an abstraction for communication interfaces, we have adopted arrival curves from network calculus. Some preliminary results are achieved, and they will be implemented in the coming versions of UPPAAL for verification of systems with asynchronous communication. The work will be extended and integrated in the TIMES tool [FMPY06] for approximate schedulability analysis of systems with multi-resource and heterogeneous components.

The **symbolic execution kernel**, Agatha [GLRT06], has been extended to support analysis of heterogeneous model using **heterogeneous models of computing**. 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 and within EDEN 2 project it is connected to the VERIMAG IF tool in the context of the platform 3 for certification of smart-card applications.

We developed sufficient criteria 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 [GGMSM06]. The criteria depend on different degrees of abstractions of the behaviours of the individual components and on the global interaction and priority model. We also investigated the incremental construction of proofs of such properties.

One-line Description of the Global Outcome

Some connections of the planned overall picture have been implemented, including some complete path(s) from modelling languages to validation engines which can be demonstrated on case studies.

One-line Description of the Difficulties Encountered

No major difficulties encountered, but the new planned projects OpenEmBeDD and SPEEDS have started later than initially expected and in the project EDEN-2, the initial work plan has considerably changed. Some planned work, considered lower priority, has been postponed.

2.2.2 Publications Related to these Achievements

[ÅCF+06] Mikael Åkerholm, Jan Carlson, Johan Fredriksson, Hans Hansson, John Håkansson, Anders Möller, Paul Pettersson, Massimo Tivoli, The SAVE approach to component-based development of vehicular systems, Journal of Systems and Software, Elsevier, to be published

[BBS06] A. Basu, M. Bozga, J. Sifakis Modelling Heterogeneous Real-time Components in BIP, invited keynote speech at SEFM 2006, Pune, LNCS, 2006

[BCGMM-06] Marius Bozga, Pierre Combes, Susanne Graf, Wei Monin, Nicolas Moteau, Qualification d'architectures fontionnelles. In Notere'06 2006

[BFGS06] Céline Bigot, Alain Faivre, Christophe Gaston and Julien Simon. Automatic test generation on a (U)SIM smartcard, in 7th IFIP WG 8.8/11.2 International Conference, CARDIS'06: Smart Card Research and Advanced Applications, LNCS n° 3928, pp 345-358, Tarragona, Spain, April 2006.

[CHP05] J. Carlsson, J. Håkansson, P. Pettersson. SaveCCM: An analyzable component model for real-time systems. Proc. Int. Workshop on Formal Aspects of Component Software, Oct. 2005.

[DHO06] W. Damm, H. Hungar, E. Olderog. Verification of cooperating traffic agents. International Journal of Control 79 (5). 2006.

[EDMG05] Huáscar Espinoza, Hubert Dubois, Julio L. Medina, Sébastien Gérard. A General Structure for the Analysis Framework of the UML MARTE Profile. In Proc. Workshop MARTES: Modelling and Analysis of Real-Time and Embedded Systems, Satellite event of MoDELS 2005. Montego Bay - Jamaica. 4 october 2005

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

[GGMSM06] Gregor Gössler, Susanne Graf, Mila Majster-Cederbaum, M. Martens, Joseph Sifakis, Ensuring Properties of Interaction Systems by Construction, Seminar in Honor of Reinhard Wilhelm's 60th Birthday, Dagstuhl 2006, to appear in LNCS

[GLRT06] Christophe Gaston, Pascale Le Gall, Nicolas Rapin and Assia Touil. Symbolic Execution Techniques for Test Purpose Definition. In Proceedings of 18th IFIP TC6/WG6.1 International Conference, TestCom 2006. LNCS 3964.

[HM06a] N. Halbwachs and L. Mandel. Simulation and verification of asynchronous systems by means of a synchronous model. Sixth International Conference on Application of Concurrency to System Design, ACSD 2006. Turku, Finland, June 2006

[KY06] Communicating Timed Automata: The More Synchronous, the More Difficult to Verify. Pavel Krcál and Wang Yi, CAV 2006: 249-262

[LMD06] P. López, J.L. Medina y J.M. Drake. Real-Time Modelling of Distributed Component-based Applications. Proceedings of the 2006 32nd Euromicro Conference on Software Engineering and Advanced Applications (EUROMICRO-SEAA'06). IEEE Computer Society Press, August 2006.

[MFFHSGJ06] P-A Muller, F. Fleury, F. Fondement, M. Hassenforder, R. Schneckenburger, S. Gérard, J-M Jézéquel. Model-Driven Aanalysis and Synthesis of Concrete Syntax. In: MoDELS 2006, October 2006, Genoa, Italy.

[MFJ05] Pierre-Alain Muller, Franck Fleurey and Jean-Marc Jézéquel. -- Weaving executability into object-oriented meta-languages. -- In S. Kent L. Briand, editor, *Proceedings of MODELS/UML'2005*, volume 3713 of *LNCS* pages 264--278, Montego Bay, Jamaica, October 2005. Springer.

[MFHS06] A. Metzner, M. Fränzle, C. Herde und I. Stierand. An Optimal Approach to the Task Allocation Problem on Hierarchical Architectures. In: Proceedings of the 20th IEEE International Parallel and Distributed Processing Symposium. IEEE Computer Society, April 25-29 ,2006 Rhodes Island, Greece

[MH05] A. Metzner und C. Herde. RTSAT - Scheduling Tasks in Distributed Real-Time Systems by Enhanced Satisifiability Checking. In: Proceedings of the IEEE Real-Time Systems Symposium, Work in Progress Session. December 5-8, 2005 Miami, Florida, USA

[MLD06] Medina Julio, Lopez Patricia and Drake José María. Towards a UML Profile for Real-Time Modelling of Component-Based Distributed Embedded Systems. Proceedings of the FDL'06 - Forum on Specification & Design Languages, Darmstadt - Germany, 19 to 22 September 2006, ISSN: 1636-9874.

[OGL06] Iulian Ober, Susanne Graf, David Lesens: Modelling and Validation of a Software Architecture for the Ariane-5 Launcher. FMOODS 2006: 48-62

[OGY05] Iulian Ober, Susanne Graf, Yuri Yushtein. "Timing analysis and validation of the embedded MARS bus manager". In Intl Workshop on Modeling and Analysis of Real Time Embedded Systems, MARTES 2005, with MoDELS 2005, October 2005

[PDR2005] G. Pinto, W. Damm and S. Ratschan. Guaranteed termination in the verification of LTL properties of non-linear robust hybrid systems. In: In ATVA Automated Technology for Verification and Analysis 2005. Taipei, Taiwan, October 4-7, 2005, LNCS 3707

[SBD06] S. Saudrais, O. Barais and L. Duchien, Using Model-driven Engineering to generate QoS Monitors from a Formal Specification, AquSerm workshop, Hong Kong, 2006

2.2.3 Keynotes, Workshops, Summerschools, Tutorials

Keynote: "A Framework for Component-based Construction"
3rd IEEE International Conference on Software Engineering and Formal Methods (SEFM05)
Koblenz (D)– September 7-9, 2005

Joseph Sifakis (Verimag) presents the component framework BIP and plans for implementing it; which meanwhile has been achieved and will be used for connecting modelling and validation tools

Keynote: "Modelling Heterogeneous Real-time Components in BIP"
IEEE International Conference on Software Engineering and Formal Methods (SEFM06)
Pune, India – September 11-16, 2006

Josef Sifakis (VERIMAG) presented the BIP framework and its implementation focussing on case studies
http://www-verimag.imag.fr/~async/index.php?view=components

Keynote: "Modelling and verification of RTES: a framework & experimental results"
Workshop QAPL on quantitative aspects in programming languages at ETAPS 2006
Vienna (A)– April 2, 2006

Keynote talk by Susanne Graf (VERIMAG) on the modelling and validation problems encountered in the context of RTES, the modelling and IF-based validation framework implemented in OMEGA on hand of an industrial case study
http://www-verimag.imag.fr/~async/

Keynote: "UML and Components for System Modelling"
Conference name Euromicro – SEAA (Software Engineering and Advanced Applications) -
Porto, Portugal – August 30 – September 3, 2006

François Terrier (CEA) presented an overview of the component concepts proposed by the standard UML2, its relations with middleware related component concepts and their benefits in a Model Driven Engineering process.
http://euromicro2005.fe.up.pt/keynotes.html#Francois

Workshop: MARTES 2005, Modelling and Analysis of Real Time and Embedded Systems
MoDELS/UML 2005, Int. Conf. on Model Driven Engineering Languages and Systems
Montego Bay, Jamaica, Oct. 4, 2005

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 2005 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/

Presently, the second edition, to be held on October 3, 2006 in Genoa, Italy in conjunction with MoDELS/UML 2006 is being prepared.. Almost 40 participants are expected.

Workshop MoDeVa 2005: Model Design and Validation

MoDELS/UML 2005, Int. Conf. on Model Driven Engineering Languages and Systems
Montego Bay, Jamaica, Oct. 4, 2005

The second edition of this workshop has been organized conjointly by the IRISA Lab of the University of Rennes and the CEA (who is the initiator of this workshop). It was held in October 2005 as a one day satellite event of the MoDELS conference. Half of the duration of the workshop was dedicated to pre-selected papers presentations and the other part of the workshop was dedicated to active discussions on different topics. A summary of those discussions together with the two best papers of the workshop have been published in [1]. The third edition of MoDeVa will be a satellite event of MoDELS 2006.

Workshop: Requirements for Flexible Scheduling in Complex Embedded Systems
Massy (France) the 16th of June, 2006

This workshop was organized by Michael González, from the University of Cantabria and Thales. It represents a collaboration with the Adaptive Real Time Cluster. It was held in Massy (France) the 16th of June, 2006. J. Medina presented in this workshop "Notes on the RT components-based framework for FRESCOR: modelling, verification, and run-time support". This presentation dealt with a number of issues about the requirements for scheduling services in the component-based framework envisioned for the FRESCOR project.

Workshop: ***Safe-UML: Modellierung und Safty-Normen***, workshop at the Safetronic 2006, Munich, Germany, November 2006.

This workshop is organized by OFFIS together with OPRAIL partners. The topics of this workshop are related to the use of UML within the development of safety critical systems, where the development process has to be compliant to safety standards. Within this workshop the OPRAIL partners will report on there experience with Safe-UML.
http://www.safetronic-veranstaltung.de/

Summer school: MDD for Distributed Real Time Embedded Systems
Brest, France – September 4-8, 2006

This summer school was co-organized by CEA. It is the third edition of a series of summer school which focuses on model-driven related issues in the context of real-time and embedded systems development. The main goal of this summer school series is to provide participants with the most up-to-date information needed to understand and apply MDE approaches to the development of distributed, real-time and embedded systems. For that purpose, we have gathered experts from a variety of research labs and industries to give seminars that provide insights into the ongoing research works and practical applications related to MDE for DRES
http://www.mdd4dres.info

Summer school: ARTIST Summer school on Component & Modelling, Testing & Verification, and Static Analysis of Embedded Systems
Nässlingen, Sweden, September 29 to October 2, 2005

This summer school included contributions from several ARTIST clusters, and in particular several tutorials by the platform partners on relevant topics, such as modelling languages (MARTE), tools (IF, Metropolis), modelling techniques (BIP, Metropolis) and model transformation techniques (Kermeta)
http://www.artist-embedded.org/FP6/ARTIST2Events/SummerSchools/Artist05.html

Tutorial: The IF toolset
SDLforum 2005
Grimstad, Norway, June 20, 2005

Iulian Ober presented the IF tool, by focussing on case studies successfully carried out within the Omega project with the IF tool chain for validating UML specs; IF will be connected to the platform.
http://www-verimag.imag.fr/~graf/SLIDES/2005-sdlforum-IF-tutorial.pdf

3. Future Work and Evolution

3.1 Problems to be tackled over the next 18 months (Sep 2006 – Feb 2008)

Globally, the work will continue according to the last 18 month plan and the tool chains which started to be developed will be further extended and/or connected. The initially planned tool integration through the jETI tools is likely not to happen within the next 18 months, although an interesting future perspective. Also the work on the platform for the certification of smart-card applications is likely to be less important than initially foreseen.

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

Platform for the analysis of safety critical embedded systems

The main future work on this platform will be carried out within the projects System@tic/Usine Logicielle, OpenEmBeDD, ATTEST and SPEEDS. They will concern the missing connections between the modelling languages used and the back-end tools via semantic level intermediate formats. It concerns also some work on back-end tools which are specific for this platform.

UML analysis tools will be extended to support the HRC (heterogeneous rich component) models developed in SPEEDS. The HRC model will be mapped to semantic level formalisms so as to allow analysis and validation of such models by existing tools, in particular those developed by INRIA, OFFIS, Parades and VERIMAG. The analysis techniques will comprise *compatibility checks* on composition of HRC design units, including static checks as well as verification of connections of assumption/promise pairs as well as *refinement verification* using the verification of black box specifications against grey box specifications. Furthermore, one has to check whether the black box specification combined with all assumptions imply the promises of the component. Based on the rich component approach the analysis techniques will extend the aspects of systems covered from behaviour and real-time to encompass also safety and other non functional aspects, in particular those important for supervising the system development process.

The Kermeta-IF-Giotto prototype tool chain already *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; it* will be disseminated, strengthened and improved thanks to the platform participant's feedback. Furthermore, an integration work of the Kermeta-IF-Giotto chain with the SPEEDS semantics (see below) will start in November, 2006. It is expected that the chain will be merged into the larger SPEEDS platform in 2007.

The Metropolis II framework will be developed by PARADES in collaboration with several external partners such as the University of California at Berkeley, United Technology, Cadence and ST who will provide important test cases for system level design crossing company boundaries. In particular, design space exploration with multiple complex architectures described with functional and non functional properties will be addressed. Industrial applications will include automotive, wireless sensor networks, industrial control and multi-core chips.

The BIP engine will be connected with the analysis tools of the IF tool-set and analysis techniques using the particular structure of BIP specifications will be implemented and extended so as to provide a suitable verification and analysis engine for system level models provided by SPEEDS case studies. For the connection to the HRC meta-model, we consider reusing the Kermeta-IF tool chain.

The BIP/THINK tool chain represents a back-end of a tool chain for code generation for given platforms. This chain is intended to be used in combination with the validation backends for BIP and for models imported through front-end tools. Code generation is not directly in th objectives of SPEEDS, but the existence of some code generators may turn out to be very useful for demonstration purposes. Future work concerns both improving the existing compilation chain: some existing OS for small targets and sensor nodes (TinyOS, SOS, Nano-RK, Mantis ...) will be considered to check how they behaviour can be modelled using BIP formalism. Simultaneously, a component-based architecture of these systems will be proposed using the THINK Component Based Framework. This architecture will be completed by THINK control components obtained from the previously mentioned OS BIP model using the BIP/THINK translator developed this year. Finally, the resulting architecture will be implemented on concrete hardware platform using the available THINK environment.

The ultimate goal is making available these validation techniques, as well as code generation techniques to the designers in commercial tools, in particular those considered in SPEEDS, that is SCADE and Rhapsody. We expect that the work done within the SPEEDS project will contribute to a stronger integration of tools.

The implementation of development and validation frameworks building on the MARTE profile include also model transformation and the code generation of a concrete implementation of the Accord/UML modelling and design platform developed at CEA. Cantabria will study the appropriate level of abstraction to extract transactional analysis models. These models will then be used to apply the schedulability analysis and performance evaluation tools that are developed inside the MAST suite. Along the process it may result necessary to adapt, extend or restrict the applicable capabilities in any of the two modelling platforms, so both are subject to adaptation in the search for complementarities. The work for the next months will include revising and if necessary proposing methodological/practical strategies to the use of concrete components technologies. The first to be considered will be an implementation of RT-CORBA and then the combination of the Real-time and Distributed annexes of the new Ada2005 programming language, which includes now the capability to describe interfaces. Based on the achievement, we will further develop validation techniques taking into account the characteristics of the modelling languages used in the platforms, in particular for properties related to the interaction in component-based systems. In the OpenEmBeDD project, the connection with several back-end tools is planned. Some of those mentioned in the context of SPEEDS, will be made available in OpenEmBeDD. Joint use of both profiles is envisioned at a later time.

Integration between MARTE standard and 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. The project is strongly coordinated with ATESST by its leader, Siemens VDO, and involved in particular CEA and INRIA cluster partners (see www.memvatex.org).

Platform for the analysis of performance critical embedded systems

An important part of the work in the next period until the end of the Persiform project will consist in consolidating the existing tool chain and in evaluating it on hand of more extended case studies.

In addition, mappings to tools for functional validation, in particular to IF or BIP are planned. Such mappings may also be used for representing observed traces during simulation by MSC. It is also planned to set up a follow-up project, in which mappings to other performance models and a stronger integration with the design process is envisioned.

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. The definition of a UML profile for security properties is considered for the third year of the project.

Collaboration and Dissemination

Like already this year, we will privilege open meetings and organisations of workshops over cluster meetings in a close format. We are again organising the MARTES workshop with MoDELS 2006 in Genoa. As the workshop attracts an increasing number of submissions and participants (this year 40 participants are expected), it will probably be organised again in 2007. It is also planned to organise a platform workshop as a satellite workshop of an appropriate major conference.

3.2 Current and Future Milestones

Milestones as foreseen in the last 18 month workplan and their realisation

- 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 projects 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 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. This will allow realising 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 analysis tools as well as tools for model-based code generation.

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

3.3 Indicators for Integration

We consider the collaboration between the partners of the platform activity to be very good. 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). The affiliated partners have either strong connections to at least one of the core partners (such as U. of Cantabria) or bring in missing competences (such as U. of Dortmund with their tool integration tool). In addition to the already mentioned projects allowing financing our activities, several more informal collaborations exist, for example between Uppsala and Dortmund. Some concrete collaboration exists now, some of them have been established in the past project period:

- Collaboration on MARTE has lead for CEA and INRIA 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 and RSA plug-ins is performed.
- 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.
- Collaboration between CEA and INRIA on model transformation has been centred on the mapping between abstract and concrete syntax for action languages [MFFHSGJ06].
- 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 an initial version of a complete tool chain in this period
- Collaboration between CEA and KTH have resulted to set up the ATESST IST project and in the first implementation of an automotive ADL aligned on Autosar
- Collaborations on the rich component model and semantics with INRIA, OFFIS and PARADES and VERIMAG
- Collaborations between INRIA, EPFL and VERIMAG resulted in an initial Kermeta-IF-Giotto tool chain for deriving code from models
- Collaboration between FTRD and VERIMAG on porting THINK to BIP/IF has started this year and resulted in a first version of a tool chain
- Collaborations on a model-driven approach integrating validation started in projects like SafeAir, OMEGA and ARTIST have lead to collaboration with an important industrial participation in SPEEDS.

We would like to mention that the platform activity had a very positive effect on the collaborations 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.

Interesting new collaborations concern particularly, new interactions between specialists in modelling in model-transformation technology, specialists in real-time systems and specialists in analysis and verification techniques. For example, this collaboration activity gave birth to the Kermeta-IF-Giotto tool chain. As another example, due to ARTIST, a French national project OpenEmbeDD which includes all French ARTIST participants has started in spring. In addition, SPEEDS IP on Speculative and Exploratory Design in Systems Engineering emerged from an initiative of a set of ARTIST partners. These two projects will further elaborate on the definition of *semantic level formats* and scalable validation tools which will be coordinated in ARTIST in the "*Semantic Platform*" activity and contribute to the "platform for component modelling and verification". These projects involves also important tool builders, such as Esterel Tech., I-Logic, TNI and Extessy which will hopefully allow us to increase the impact.

The organization of the workshop MARTES in association with MoDels'2005 is another indicator of collaboration between these communities.

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
- Families (for CEA, INRIA, Thales), ITEA European project on component based modelling of product lines;
- EDEN and EDEN 2 (for CEA, VERIMAG), French national RNTL project on UML based development and verification of security critical system; the work in EDEN 2 will not immediately address the issues relevant for the platform. See http://wwwxxx.fr
- STACS (for CEA, Thales), French national RNTS project on validation and testing of component based models;
- PERSIFORM (for FTRD, INRIA and VERIMAG), a French National RNRT project on functional and performance analysis of service oriented specifications. See http://www-persiform.imag.fr
- SAVE (for Uppsala), Swedish national project on component based development of embedded systems.
- ASTEC (for Uppsala, ABB) on component-based modelling of embedded control systems
- OPRAIL (for OFFIS) a German national project on advanced design processes for train control systems compliant to standards.
- Usine Logicielle (Software Factory), French national 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. Main focus of this large project (19 partners) is on embedded systems and covers three aspects: modelling, validation and component based middleware.
- ATESST – IST project (CEA, KTH, Volvo Tech., Daimler Chrysler, etc.) addressing system modelling techniques for automotive software development under alignment constraints with Autosar, UML and SysML standards. See http://www.atesst.org

- MemVaTEx – French national RNTL project (CEA, INRIA, Siemens VDO, etc.), a modelling methodology that supports the development continuity, model refinement and interoperability between heterogeneous modelling formalisms.
- FAROS (for INRIA and FTRD), French national RNTL project on composition of service-oriented systems based on software contracts and components.
- OpenEmBeDD (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. see http://openembedd.inria.fr
- SPEEDS IP project, with the ARTIST partners INRIA, OFFIS, PARADES and VERIMAG and affiliated industrial partners Daimler and IAI.
- Industrial funding (Pirelli, Ferrari, United Technology, Cadence, ST) for the Metropolis II and its application were provided to PARADES.

3.5 Internal Reviewers for this Deliverable

Bengt Jonsson, Uppsala
Alberto Sangiovanni, Parades