IST-004527 ARTIST2
Network of Excellence
on Embedded Systems Design

Activity Progress Report for Year 4

JPRA-Cluster Integration

Component-Based Design of Heterogeneous Systems

Clusters:

Real Time Components

Activity Leader:

Prof. Bengt Jonsson (Uppsala)

http://user.it.uu.se/~bengt/

Policy Objective (abstract)

Developing a conceptual and technical basis for component-based design of heterogenous systems, focusing on three issues:

- Composing heterogeneous system components
- Interfaces for composition, achieving correctness-by-construction
- Industrial liaison through seminars and collaboration.

Table of Contents

1. Overview of the Activity

1.1 ARTIST Participants and Roles

Prof. Bengt Jonsson – Uppsala University (Sweden)

Responsible for activity.

Composition and Interfaces for Embedded Systems. Specification and compositional analysis of timing properties.

Prof. Francois Terrier – CEA (France)

Modeling and analysis of embedded systems, UML development.

Prof. Tom Henzinger – EPFL (Switzerland)

Development of abstract programming models for real-time computing [Giotto: time-triggered; xGiotto: both time- and event-triggered].

Dr. Albert Benveniste – INRIA (France)

Synchronous languages and heterogeneous systems modelling and deployment.

Organization and planning of meetings with industrial audience.

Prof. Jean-Marc Jézéquel - Inria (France)

Time and quality of service models for conventional component based design.

Automatic transformations of component based architectures for real-time model.

Prof. Werner Damm - OFFIS (Germany)

Responsible for sub-activity on "industrial liaison".

Embedded system modelling and validation, deep involvement in cooperation with the automotive industries.

Prof. Alberto Sangiovanni-Vincentelli - PARADES (Italy)

Strong interaction with automotive, design software and semiconductor industry (co-founder of Cadence and Synopsys); expertise in design flows, tools and modelling methodologies with particular attention to Hard Real-Time; Platform-Based Design and Metropolis design framework for integration of design processes from OEMs to suppliers involving functional and non functional aspects.

Prof. Paul Caspi – Verimag (France)

Synchronous languages and heterogeneous systems modelling and deployment; tight cooperation with Airbus.

Organization of meeting.

Prof. Joseph Sifakis – Verimag (France)

Responsible for sub-activity on "design of heterogeneous systems".

Synchronous languages and heterogeneous systems modelling and deployment; tight cooperation with Airbus.

Prof. Hermann Kopetz - TU Vienna (Austria)

Inventor of the TTA concept.

organization of meeting.

Jacques Pulou (FTRD, France)

Component behaviour modeling, Component Based OS construction.

1.2 Affiliated Participants and Roles

Prof. Anders Ravn – Aalborg (Denmark)
Modeling and verification of timed systems.

Peter Eriksson - ABB Automation Technology (Sweden)
Construction of large complex embedded systems.

Prof. Bernhard Steffen - Dortmund University (Germany)
Tool integration, modeling and verification, generation of models of communicating systems.

Prof. Ivica Crnkovic – MdH (Sweden)
Component models, industrial component-based software engineering, Component-based development processes.

Dr. Frédéric Boulanger – Supélec (France)
Modelling of the behaviour of heterogeneous systems.

Dr. Dominique Potier (Thales R&T, France)
Construction of large complex embedded systems, Model driven development.

Dr. Marius Minea - Institute e-Austria Timisoara (Romania)
Formal verification, specification of timed systems.

Dr. Julio Medina – University of Cantabria (Spain)
Model Based Schedulability Analysis and its usage from UML descriptions.

1.3 Starting Date, and Expected Ending Date

Starting date: December 1st, 2006

Expected ending date: December 31, 2008

1.4 Baseline

Existing component models and frameworks do not adequately support essential properties of real-time systems, such as heterogeneity, resources, behaviour, timing, and quality of service. Partners have been working towards a framework for component-based development of heterogeneous embedded systems, including the following approaches.

Design of Heterogeneous Systems:

A key characteristic of component-based embedded systems is **heterogeneity** of component models. This heterogeneity concerns different execution models (synchronous, asynchronous, vs. timed), communication models (synchronous vs. asynchronous), as well as different scheduling paradigms. The PARADES team has been a driving force in the development of the Metropolis (http://www.gigascale.org/metropolis) environment, which supports a variety of design notations and the concurrent management of different physical properties such as power, reliability, timing and cost. The Platform-Based Design approach to embedded system design began with the formation of PARADES. Already at the start of this activity, this design methodology was widely applied in all industrial segments and at all levels of abstraction. Lately, tool companies such as Cadence and National Instruments have used the graphical representation of the methodology in all their presentations. The design method is now being increasingly explored in the context of intelligent building, airplane engine, air conditioning systems and elevator design. The Metropolis environment supports the formal aspects of the design methodology.

As a foundational counterpart to the work on design environments, the PARADES team has been working with UC Berkeley and INRIA in the refinement of the *tag signal model* developed by Ed Lee and Alberto Sangiovanni Vincentelli to provide a unified modelling paradigm for models of computation. This denotational model has been used by several research organizations to reason about heterogeneous systems. It has been the basis for the work on desynchronization by INRIA, Verimag and PARADES. In this context, the *tag system model* has been developed as an extension of the tag signal model.

VERIMAG has developed the *Behavior, Interaction, Priority* (BIP) framework for component-based modelling of heterogeneous real-time systems [Si05, BBS]. BIP integrates research results developed at VERIMAG over the past five years. It is characterized by the following:

- It supports a component construction methodology based on the thesis that components are obtained as the superposition of three layers. The lower layer describes behavior. The intermediate layer includes a set of connectors describing the interactions between transitions of the behavior. The upper layer is a set of priority rules describing scheduling policies for interactions. Layering implies a clear separation between behavior and structure (connectors and priority rules).
- It uses a parameterized binary 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. The use of such a composition operator 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 whose parameters depend on the order of composition.
- It encompasses heterogeneity. It provides a powerful mechanism for structuring interactions involving strong synchronization (rendezvous) 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* × *Interaction* × *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.

BIP has been successfully applied to define operational semantics for the Heterogeneous Rich Component model in the SPEEDS project.

TU Vienna has developed the foundations for an integrated architecture that facilitates the development of distributed real-time applications consisting of multiple heterogeneous subsystems with different criticality levels. A central issue is a framework for providing standardized, validated and certified services that can be reused in different applications.

Interfaces and Composability

Several partners of the RTC cluster have been developing tools and techniques for specifying and reasoning about timing and resource properties of components and systems composed from components. These include the following.

- The MAST environment for schedulability modeling and analysis, which has been developed by the Univ. of Cantabria.
- The real-time calculus, developed by the team of ETHZ, which allows specify ingcomponents under less constraining assumptions, and represent many different kinds of properties (period, jitter, bursts) in a uniform way. A further advantage is that it supports separation of concerns, since computation resources are treated as first-class citizens along-side with functional and timing properties; the available computation resources are specified explicitly in a uniform representation.
- A more general technology for specifying and analyzing timing properties is offered by (variants of) timed automata. Several teams have developed tools for modeling and analysis of timed automata specification (UPPAAL by Uppsala and Aalborg, IF/Kronos by Verimag).
- An adaptation of automata-based techniques towards specifying components in terms of required and offered properties of their temporal behaviour is offered by the work on *interface automata* by the EPFL team and their collaborators. This work has also been extended to include quantitative timing properties as in timed automata in the work on *timed interfaces.*

Several partners have contributed to the development of component frameworks that can handle timing and resource properties. This has been done, e.g., in the on the *Omega* component model [DJPV05], Simpler component frameworks, which modestly extend existing mainstream techniques for design of real-time systems, include *Rubus.*

MdH, with contributions from Uppsala University, has developed SaveCCM, a component model and technology for real-time embedded systems with constarined resources. The technology aims for pratactibility of some properties and a transformation from the component model to an execution model optimised for resource usage (CPU or memory).

Industrial Liaison

The problem of developing framework for component-based development of embedded systems, has been partly addressed in previous projects and collaborations between partners and industries, e.g., within projects AIT-WOODDES, OMEGA, Families, EAST-AEE, PROGRESS, and Trusted Components. In addition, PARADES has been heavily involved with its partners (ST and Cadence) in the definition of design methodologies for fault tolerant systems in the automotive domain.

1.5 Problem Tackled in Year 4

Design of Heterogeneous Systems

Definition and classification of unified frameworks encompassing heterogeneity. System designers deal with a large variety of components, each having different characteristics, from a large variety of viewpoints, each highlighting different dimensions of a system. Two central problems are the meaningful composition of heterogeneous components to ensure their correct interoperation, and the meaningful refinement and integration of heterogeneous viewpoints during the design process. As subtasks we have identified

- defining and studying notions of **expressivity** for composition formalisms, in terms of their ability to form new behavior from components, and using it to compare existing composition formalisms,
- developing **Models of Computation** in which one can detect parallelism and generate "more parallel" versions of system models, e.g., for multicore implementation,
- incorporating techniques for formal modelling of herogeneous systems in **standardized formalisms, most notably in UML profiles**.

Implementing system behavior on distributed platforms. Communication (including protocols, models of computation and architectures) and interconnect (including topology, buffering and layout) design is the single most important and critical step in heterogeneous distributed system design. This entails several types of work

- On the conceptual side, work has been carried out to devise **semantical foundations for reasoning about the executions of a distributed system**. If a distributed implementation is generated from a non-distributed system specification, one must also devise techniques to compare the behaviour of the distributed implementation with that of its non-distributed specification, and devise appropriate notions of correctness. A particular challenge here is to consider the case when the specification includes some specification of reliability, which is realized by replication or other means in the distributed implementation.
- On the design methodology side, work has been done on techniques for **synthesizing a communication architecture** that optimizes system parameters within the constraints offered by the system specification and resources.
- **Design of a time-triggered Network on Chip.** We have designed an efficient Network-on-a-chip (NoC) architecture that interconnects heterogeneous cores with different criticality and diverse requirements with respect to the communication infrastructure.

Interfaces and Composability

Better Interface Theories: Existing general theories for interfaces, refinement, composition, etc. are able to guide the development of component frameworks, but they do not address the issue of reuse of component. An interface theory that encompasses also reuse has been developed.

Reasoning about systems of components: Techniques for analyzing and verifying properties of systems of components have been developed in several contexts, as follows.

- **For Heterogeneous Rich Components** The partners INRIA, OFFIS, PARADES, and VERIMAG has continued their work on the *Rich Component Model* paradigm. After the establishment of the metamodel, work has continued to make the metamodel more concrete, by instantiating it to different viewpoints, and to develop verification frameworks and tool support.
- **Correctness-by-construction**: Verimag continues the work on compositional deadlock detection/verification and its implementation in the DeadlockFinder tool. Structural analysis of BIP systems is extended for taking into account priorities.
- **Scalable Specification and analysis of timing properties** During Y4, the collaboration between ETHZ, Uppsala, and other partners, on developing techniques for scalable analysis of timing and resource properties, has continued by further work on the CATS tool, with the goal to eventually be able to subsume existing techniques including RMA, real-time calculus, and timed automata verification. The collaboration has also investigated the connection between analytical approaches, such as the real

time calculus, and operational ones, with the aim to provide an operational foundation for formalisms such as the real time calculus.

Component models: The SaveCCM component model has been developed to make it suitable for distributed embedded systems. We have also addressed the problem of developing techniques and tools to implement an existing component model by means of a real-time programming environment, such as Ada 2005: within the *FRESCOR* project, University of Cantabria and Thales has implemented the approach for deploying MicroCCM components, which was developed during Y3.

Synthesis of Controllers and Glue: This is a central problem in component-based design, which has been addressed from different directions, e.g., as the problem of synthesizing a winning strategy in a game, or as a problem of synthesizing an adaptor to bridge mismatches between components.

Synthesizing component models and interfaces from test data and observations. We have continued the work onu using automata learning techniques, to make the usable for synthesizine models of industrial protocols and interfaces.

Industrial Liaison

Interaction with the Avionics Industry: On November 12-13, 2007, an ARTIST2 meeting on IMA (Integrated Modular Avionics) was co-organized by Albert Benveniste (INRIA), Paul Caspi (Verimag), in tight cooperation with John Rushby, and hosted by Alberto Ferrari (PARADES) in Rome, Italy. Detailed minutes have been made available as for the workshop “Beyond AUTOSAR”, which was organized in 2006 by the cluster, to discuss real-time issues in the context of AUTOSAR, which is an open and standardized automotive software architecture.

Interaction with the Automotive Industry: Work has been carried out as follow-up of the “Beyond AUTOSAR” workshop, to discuss different technologies that can support design for the AUTOSAR system architecture, e.g., discussing how results from the IP project SPEEDS can be put to use.

1.6 Comments From Year 3 Review

1.6.1 Reviewers’ Comments

The document presents in detail the results of year 3. The document might have benefited from a more concise expression. The relationship with the industry seams to be a bit weak in term of actions. The dissemination aspects are impressive if we look at the number of publications and the level of conferences while in comparisons joint publications between partners are few showing that interactions between partners can be improved.
The updated version of the document now provides details on the work planned for year 4 and provides the role of partners that were missing in the original version.

1.6.2 How These Have Been Addressed

We have tried to make the description of Year 4 work more compact than that of Year 3.

The partners are engaged in significant industrial collaborations, aiming at adapting component-based development techniques in important industrial sectors. One of many examples is the series of meetings with industry to discuss how results from the IP project SPEEDS can be used in automotive software development.

Interactions between partners have increased, e.g., by launching of new collaboration projects. The number of joint publications has increased significantly since Year 3 (from 9 to 23).

2. Summary of Activity Progress

Since this activity continues efforts that have been conducted under different headings in years 1 and 2, we adapt from relevant activity descriptions for these years. For all sections, we structure the description of progress into the three sub-activities: *Design of heterogeneous systems*, *Interfaces and Composability*, and *Industrial liaison*.

2.1 Previous Work in Year 1

The activity started during Year 2.

2.2 Previous Work in Year 2

Design of Heterogeneous Systems

The theory on *tag systems* was further developed by Benoît Caillaud and Dumitru Potop-Butucaru (VERIMAG, then INRIA, team Aoste), who developed a theory for the correct deployment of synchronous designs over globally asynchronous, locally synchronous (GALS) architectures. This work introduced the notion of weak endochrony, at a macro-step level, which extends to a synchronous setting the classical theory of Mazurkiewicz traces. A micro-step model for the representation of asynchronous implementations of synchronous specifications was introduced. The model covers classical implementations, where a notion of global synchronization was preserved by means of signaling, and globally asynchronous, locally synchronous (GALS) implementations where the global clock is removed. This model offers a more refined framework for reasoning about essential correctness properties of an implementation: the preservation of semantics and the absence of deadlocks. Stavros Tripakis and Paul Caspi of VERIMAG actively collaborated with INRIA and PARADES in developing techniques for heterogeneous systems modelling and in automatic code generation from high level synchronous models on several platforms, notably asynchronous preemptive ones.

The *BIP (Behavior, Interaction, Priority)* framework for modeling heterogeneous real-time components which integrates results obtained at *VERIMAG* over the past 5 years was implemented in a tool allowing the efficient execution of specifications. BIP is a central semantic-level formalism that is connected to several modeling formalisms and validation tools in the work of *Plaform for Component Modeling and Verification,* but is also an effort to enable integration of heterogeneous systems. A mapping from BIP to Think/Fractal is being implemented jointly with *FTR&D* for achieving code generation for BIP descriptions. Several industrial case studies have been modelled using BIP, including an Adaptive QoS controller for a video encoder, a planner for autonomous robots and we started to work on a model of sensor networks (together with FTR&D) for fine grained energy consumption analysis.

TU Vienna has worked on a next-generation embedded architecture for Systems-on-a-Chip (SoCs) that provides a predictable integrated execution environment for the component-based design of many different types of embedded applications (e.g., consumer, avionics, automotive, industrial). The architecture is inspired by the research priorities that have been identified in the ARTEMIS Strategic Research Agenda (SRA), such as composability, networking, robustness/security, diagnosis, resource management, and evolvability. The network interface will be based on the Time-Triggered Ethernet (TTE) protocol that supports the coexistence of hard real-time communication and standard Ethernet messages [KAGS05, OPK05]. The *OFFIS* team has developed an approach to design space exploration within the development of distributed embedded real-time systems. The mapping of software parts onto suitable hardware parts is a crucial issue of optimization towards efficient and inexpensive implementations. An extended SMT checker is used in a binary search scheme in order to achieve optimal allocations of tasks and messages to architectural elements.

Interfaces and Composability

The work on developing the concept of *rich component models* into a mature framework for system design has been pursued within IP-SPEEDS by RTC partners INRIA, OFFIS, PARADES, and VERIMAG. A goal of SPEEDS is to provide an engineering environment enabling the creation, manipulation, and maintenance of rich component models and allowing system engineers to perform analysis, evaluate the maturity of the design and exchange design representations at different level of abstractions. Currently, the work is focussing on developing a meta-model for rich components. 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). The work in SPEEDS also involves a new theory of *interfaces*, allowing for cross-viewpoint assume-guarantee reasoning. More precisely, a novel notion of contract has been defined for embedded systems that takes their multiple viewpoint nature into account. It was found that the way contracts should be composed for different viewpoints of a same component differs from the one used for different components. The fusion of contracts is a new operator that subsumes both cases.

Several lines of work have focussed on timing properties. Different techniques for specifying and analyzing timing properties, including the real-time calculus (developed at ETHZ), classical schedulability analysis, and timed-automata techniques (implemented, e.g., in Uppaal) have been compared in the the workshop “Distributed Embedded Systems” at the Lorentz Center in Leiden in Nov. 2005. A diploma project at Timisoara implemented a translation from a dedicated description language for multiprocessor tasks into Uppaal models using timed automata. Uppsala has developed a translation between the real-time calculus of ETHZ and timed automata formalism. This translation is currently being implemented in Uppaal. The *EPFL* team has developed an assume-guarantee interface algebra for real-time components. In this formalism a component implements a set of task sequences that share a resource. The algebra defines compatibility and refinement relations on interfaces. The algebra thus formalizes an interface-based design methodology that supports both the incremental addition of new components and the independent stepwise refinement of existing components. The flexibility and efficiency of the framework has been demonstrated through simulation experiments.

Integration of techniques from schedulability analysis into component-based design methods are further developed by *Cantabria* and *Thales* in the FRESCOR project: Framework for Real-time Embedded Systems based on COntRacts (www.frescor.org, IST-034026), which aims to produce a framework for handling timing requirements with a focus on reconfigurable architectures. Within the context of the SAVE Swedish national project, the Uppsala and Mälardalen teams are developing *SaveCCM* (the SaveComp component model).

EPFL and PARADES have collaborated to adapt techniques for specifying component interfaces for the development of a structured coordination language for specifying the interaction of real-time tasks. Task communication happens through shared variables called communicators, which can be read and written only at specified time instances. Sensors and actuators are special kinds of communicators. The read and write times of communicators determine the release times and deadlines of tasks. Tasks may also depend on each other, be refined into sets of tasks, and be changed through mode switches. The language is a hierarchical extension of Giotto, and has been inspired by and used in the automotive domain.

Dortmund and Uppsala have collaborated to develop and implement automata learning techniques for automatically deriving behavioural models of components from legacy code or observations of system behavior. Part of the work concerns extending these techniques to derive timed models.

Industrial Liaison

The forums organized in the framework of this activity are an important contribution to the interaction between industry and academia in the considered sector. The meeting *Meeting Beyond AUTOSAR* was held on March 23rd - 24th, 2006 in Innsbruck, Austria. There were 52 registered participants, among which 15 from industry. The agenda of the meeting, as well as the detailed minutes and slides can be found at

http://www.artist-embedded.org/artist/-ARTIST2-Workshop-Beyond-AutoSar-.html

Here we summarize the most important conclusions from this meeting.

Regarding the interaction *control/embedded software*:

- There is a permanent misunderstanding between control & software engineers
- Regarding the relative merits of ET/TT, control design aspects provide complementary views, not considered before
- There is a need for a notion of component for control that would enable incremental development of control systems.

Regarding AUTOSAR:

- The AUTOSAR design flow for distributed embedded electronics is not completely plug-and-play, nor is it compositional, for reasons of scheduling: scheduling is, today, based on global systems models. Component-based techniques for real-time are needed. (This is an ongoing research activity at some ARTIST2 teams participating to RTC and Execution Platforms clusters.)
- Turning the AUTOSAR approach into an effective tool for dispatching the work efficiently among suppliers is still seen as a challenge.

2.3 Previous Work in Year 3

Design of Heterogeneous Systems

An algebraic framework for BIP (VERIMAG)

We worked for an algebraic formalization for the BIP framework [BS07]. The main difference with existing process algebras is the use of operators for composing connectors describing interactions and priority. We provided an algebraic formalisation of connectors in BIP. These are used to structure interactions in a component based system. A connector relates a set of typed ports. Types are used to describe different modes of synchronisation: rendezvous and broadcast, in particular. We used the system construction space *Behaviour* × *Interaction* × *Priority* to study relations between different classes of models. We studied in particular, characterizations of existing models of computation as regions of this space and relations between these regions. Furthermore, different subclasses of models e.g., untimed/timed, asynchronous/ synchronous, event-triggered/data-triggered, can be unified through transformations in the construction space.

Designing a timed BIP component model (INRIA and VERIMAG)

Verimag and INRIA have collaborated by merging their component models to design a timed BIP component model. This model will be integrated in the platform under construction by the Platform activity of the CBD cluster [SPB07].

A formal approach for modelling heterogeneous systems (CEA LIST)
In order to transfer the research on modeling of heterogeneous systems into the standardization domain, work started to build a specialisation of a standard modelling language (UML) to describe heterogeneous computation and communication models founded on a mathematical basis. This lead to create a common research action (THeSys: Tackling Heterogeneous Systems – www.thesys.eu.org) of the research cluster Digiteo Labs (www.digiteo-labs.org) with Suppelec, ARTIST 2 associated member. A first report on the state of the art was produced for Usine Logicielle and a first instantiation of a dedicated UML profile was provided.

Architecture for Heterogeneous Systems (TU Vienna)
The important aspects on error containment and diagnosis within heterogeneous distributed systems were addressed within [OKSH07] and [EOHPK07], as a continuation of the work on diagnosis that was started in year 1 in the HRT cluster. The proposed architecture enables the integration of mixed-criticality subsystems (cf. [EOHKS07]) within a distributed system and even within a single chip. Other problems addressed by the Vienna team included the following

- To facilitate the modeling and formal verification of distributed heterogeneous systems which are designed according to the time-triggered paradigm, The Periodic Finite-State Machines (PFSM) [KEHO07] were developed as extensions of the basic Finite State Machines (FSM) model, based on the concept of a sparse time base.
- [OH06] presented a solution for the model-based design of virtual networks in distributed heterogeneous networks enabling faster development time and avoiding design faults. This work was extended to an overall model-based development process of integrated computer systems based on the DECOS architecture in [HO07].
- [SOE07] attacked the problem of interfacing heterogeneous distributed applications to Hardware-in-the-Loop (HIL) simulators and presents a solution based on an interface at the sensor/actuator level.

.

Interfaces and Composability

Several interacting lines of work hwere performed in the context of efforts where component models for embedded system design are developed. The work on *Rich Component Model* in SPEEDS targets both heterogeneous and component-based systems. Other efforts (described subsequently) are more focussed on timing and resource problems in component based design.

Meta model for Heterogeneous Rich Components (INRIA, OFFIS, PARADES, VERIMAG)
Within the IP SPEEDS, the work on developing the *Rich Component Model* paradigm was focussing on the development of a metamodel, called **HRC (Heterogeneous Rich Components)**, which now forms the foundation for the component based construction of complete virtual system models. Its main objectives are: 1) to define a semantic-based meta-model used by all involved tools, 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 first year of the project, a first version of this meta-model was defined [BCSM07], [CMM+07], [BBCP06]. The main features of HRC are:

- *Design by contract* paradigm: attached to a component, contracts express constraints on assumed behaviour of the environment (assumption) and expected behaviour of the component (promise).

- *Organization in viewpoints: f*ollowing the principle of separation of concerns, different aspects are organized into viewpoints, each of which collects a part of the component's dynamics constraints from some perspective and can be used to filter the component's characteristics w.r.t. that view.

- *Uniform concepts across all layers:* different *layers* may be identified for expressing different architectural abstractions of an embedded system. Examples of layers are the functional layer representing the functionality of the system and the platform layer that together with the functional layer abstracts the system as a network of buses and ECUs (containing tasks and threads)..

- *Rich connectors*: in addition to SysML-like connectors expressing data or event flow with a unique predefined initiator, HRC contains more powerful connectors whose activation depends on the agreement between at least a subset of the connected components.

Validation and design space exploration. Different specific validation techniques were developed or adapted for HRC models. We mention as examples, efficient deadlock analysis using the structure provided by rich connectors, simulation using BIP (Verimag) or Metropolis (parades), Hybrid analysis using Ariadne (Parades), and specific methods for timing or safety analysis (OFFIS). They are reported in more details in the platform deliverable. OFFIS and PARADES collaborated on design space exploration based on HRC. Here, the deployment of executable components and communication links determines the extra-functional properties, such as timing. Finding a cost efficient and requirement preserving deployment is subject of optimization. The deployment synthesis OFFIS developed (RTSat) provides the capability of finding optimal deployments among the solution space for a given architecture, while preserving extra-functional requirements on real-time, memory, etc, which were shown to be fulfilled at the specification level [MH06].

The SaveComp component model (Mälardalen, Uppsala)

Another effort to develop a model for component based development is *SaveCCM* (the SaveComp component model), developed by the Mälardalen and Uppsala teams [ÅCF+07]. SaveCCM is based on a control-flow (pipes-and-filters) interaction model, combined with additional support for domain specific key functionality. Timing properties of a system of components can be analyzed using fixed-priority analysis techniques, using e.g., the MAST schedulability modeling and analysis environment developed by the Univ. of Cantabria. The *SaveCCM* component model has been employed in industrial case studies, e.g., at CC Systems, where a component-based repository is being built.

Deployment of LightWeigth CCM components within a Flexible scheduling framework. In the context of the effort to combine real-time implementation technology and contract technology to build techniques for component-based design, in the context of the FRESCOR project, University of Cantabria and Thales used a specialization of the Deployment and Configuration OMG standard to define an approach for the deployment of MicroCCM components. The initial design [LPDM07] was made by Patricia López from Cantabria and allows the generation of the analysis models from the same description.

Hierarchical Coordination Language for Interacting Real-Time Tasks (EPFL, PARADES)

As another concrete technology for component based development, EPFL and PARADES designed and implemented a new programming language called Hierarchical Timing Language (HTL) for hard real-time systems. HTL is a hierarchical version of Giotto. Critical timing constraints are specified within the language, and ensured by the compiler. As a case study, a distributed HTL implementation of an automotive steer-by-wire controller was implemented [GHIKS06].

Platform implementation technology for timed components (EPFL, INRIA, Verimag)
The work on a transformation chain for timed components was extended to allow assembly and automatic mapping onto the Giotto framework. The tool is able to accept assemblies of timed components, check the assemblies for compliance with timed logic properties and generate a set of monitor for execution on these assemblies on the Giotto infrastructure from EPFL. Moreover, the INRIA team also designed a special version of a Java machine able to run on the Lego Mindstorm platform (a tiny, low cost commercial platform for building robots). Mindstorm software is monitored in situ using automatically generated monitors. This joint work merges the advantages of BIP components on structuring and continuous time management [SBD06].

Scalable Specification and analysis of timing properties (Uppsala, ETHZ)
The work conducted on developing techniques for analysis of timing and resource properties, which are more precise and more scalable than existing ones was continued in Y3 with an implementation of translations between the real-time calculus, developed at ETHZ, and timed automata formalisms in the context of the Times tool (http://www.timestool.com). A prototype tool (named CATS) for compositional timing and performance analysis was developed.

Within software engineering for embedded systems generic reusable software components must often be discarded in favor of using resource optimized solutions. In cooperation with the Swedish company CC Systems, MdH has developed a model that enables the utilization of component-based principles even for embedded systems with high optimization demands. The model supports the creation of component variants optimized for different scenarios, through the introduction of an entrance preparation step and an ending verification step into the component design process. These activities are proposed to be supported by tools working on metadata associated with components, where the metadata can be automatically retrieved from many development tools [ÅFSC07]

A Model for Reuse and Optimization of Embedded Software Components (MdH) In cooperation with the Swedish company CC Systems, MdH developed a model that supports the creation of component variants optimized for different scenarios, through the introduction of an entrance preparation step and an ending verification step into the component design process [ÅFSC07].

Adapter synthesis for real-time components (INRIA and L'Aquila University)
An approach for overcoming compatibility problems in composition of available components, was developed by INRIA and L'Aquila University. An automated method was devised to build correct-by-construction adapters, to be inserted between components such that all inconsistencies are solved. This is possible thanks to the controllability of some input and output actions. The method uses a Petri Nets modelling and a specific controlled coverability graph generation algorithm. It is implemented inside a tool suite [TFGG07].

Algorithms for Interface Synthesis (EPFL, Uppsala, and Dortmund)
With the goal to extend the available repertoire of techniques for generating component models, Dortmund and Uppsala have beencollaborating to develop automata learning techniques (aka regular inference) for automatically deriving behavioural models of components from observations of system behavior. Such techniques can be useful to generate models of components for which no source code is available, e.g., libraries, hardware components. Dortmund has developed *LearnLib* [BRS06], a library for automata learning, with a flexible modular structure that can be configured to exploit specific properties of applications. During Y3 of ARTIST2, the collaboration has been motivated by the goal of using LearnLib to generate a model of an industrial protocol developed by an industrial partner of Uppsala (Mobile Arts AB). One difficulty in this protocol is that messages contain identifiers of connections, etc. from a potentially infinite domain. The main achievement during Y3 has been to extend automata learning techniques to a class of infinite-state systems that can handle this

situation [BJR]. Another line of work concerns extending automata learning techniques to generate models of timed systems, in the form of timed automata [GJP06].

EPFL compared and evaluated three different algorithms for automatically extracting temporal interfaces from code: (1) a game algorithm that computes the interface as a representation of the most general environment strategy to avoid a safety violation; (2) a learning algorithm that repeatedly queries the program to construct the minimal interface automaton; and (3) a CEGAR algorithm that iteratively refines an abstract interface hypothesis by adding relevant program variables. For each of the three algorithms a family of components was provided on which that algorithm outperforms the two alternatives. On the practical side, the three algorithms were evaluated experimentally on a variety of component libraries [BHS07].

Industrial Liaison

Organization of Workshops on Industrial Topics

The workshop “Beyond AUTOSAR” held in the Year 2 period gathered key industry players from AUTOSAR and key scientists to discuss fundamental issues for embedded automotive systems design. Werner Damm presented the results of the workshop in a keynote lecture at the EMSOFT Conference 2006 in Seoul and at a workshop organized by GM on the Future of Automotive Software Development in Bengalore (January 2007). The documentation for the findings of the workshop are at the “proceedings site” http://www.artist-embedded.org/artist/-ARTIST2-Workshop-Beyond-AutoSar-.html

PARADES is an industrial research consortium. Its partners (Cadence and ST) are constantly made aware of the technical advances pursued by the PARADES team. The interaction with people in the companies is at least weekly. ST has a strong interaction on fault tolerant architectures and fault analysis and uses PARADES expertise to interact with system customers such as Bosch and Nippon Denso. PARADES is also in contact with Freescale via the Joint Development Group with ST. Cadence relies on PARADES expertise for system-level design methodologies and tools. PARADES has interacted with Pirelli in a project involving intelligent tires for stability control in cars. PARADES has had significant interaction with United Technology Corporation (UTC), a large multi-national conglomerate, on sponsored research for embedded system architecture and design methodologies for OTIS Elevators, Carrier air conditioning systems and Chubb Securite’, a large division in charge of safety and security systems for buildings and large structures such as hospitals. In addition, PARADES has had collaboration with General Motors on research strategies and directions.

Establishment of SafeTRANS

During Y3, OFFIS was instrumental in creating SafeTRANS (http://www.safetrans-de.org), a non-profit organisation combining the expertise of German key industrial and academic players in the area of processes and methods for the development of safety critical embedded systems in the transportation domain. Building on OFFIS' strong industrial cooperation network and using experience gained from numerous activities in shaping European R&D roadmaps, SafeTRANS founding members are Airbus Germany, Bosch, Continental, DaimlerChrysler, Siemens VDO and Transportation Systems, OFFIS, DLR and the Carl von Ossietzky University of Oldenburg. SafeTRANS' mission is to to maintain the current high safety levels of transportation systems in spite of growing traffic density, and in spite of an exponential growth in Embedded Systems complexity, through model based development and analysis of safety-critical Embedded Systems enabling a holistic system analysis.

Together with two french Pôle de Compétitivités Aerospace Valley (http://www.aerospace-valley.com) and System@tic (http://www.systematic-paris-region.org), SafeTRANS formed EICOSE, the European Institute for COmplex and Safety Critical Embedded Systems

Engineering[1]. Through the participating competence centres, EICOSE clusters major industrial and academic organisations in the area of embedded systems in the transportation domain, namely Airbus, Alcatel Space, Alstom, Altis, Astrium, Bosch, CEA, Cegelec, CNES, CNRS, Continental, CS communication et Systèmes, DaimlerChrysler, Dassault-Aviation, Dassault Systems, DLR, EADS ST, EDF, ENSC, Ecole Polytechnique, France Telecom, IERSET, INRIA, IRC SCS, LAAS, Latécoère, Motorola, OFFIS, ONERA, RATP, Renault, SiemensVDO, SiemensTransportation, SNCF, SNECMA, Sogerm, Thales, University of Oldenburg, Valeo, Visteon, and many others. EICOSE has been selected the first ARTEMIS Innovation cluster, paving the way for EICOSE to participate in shaping those parts of the ARTEMIS Strategic Research Agenda dealing with the transportation domain, thus directly influencing calls in the forthcoming ARTEMIS JU. EICOSE has identified a priority list of research items from an industrial point of view, which lead to the formation of proposals of three so-called subprograms which were adopted by Artemis in its Artemis Multi-Annual Strategy Plan, and included in the call for proposals for the 1st call of the Artemis Joint Undertaking.

2.4 Final Results

2.4.1 Technical Achievements

Design of Heterogeneous Systems

Formalisms for modelling Heterogeneous Systems: The partners' different approaches to modelling heterogeneous systems have been further developed within the context of ARTIST2. Results achieved include

- **Further work on Tag Systems (INRIA, Parades, and Verimag):** The theory of Tag systems has been further developed [BCCCS08]. Tag systems are models of systems where data are enriched with tags, supporting a flexible and parameterizable notion of time. This approach supports heterogeneity by providing a mathematical basis for composing subsystems with different Models of Computation and Communication (MoCCs). Theorems have been provided that give conditions for the original semantics to be preserved at deployment phase, when a "less synchronous" architecture is used. This is work along lines similar to the efforts of Edward Lee regarding Ptolemy II. Ongoing work now includes participants from Cadence Berkeley. It consists in developing a functional version of Tag systems theory that strongly relies on Kahn Process Network techniques. In particular we were able to show that directors (in the sense of Ptolemy II) are not needed in order to coordinate different MoCCs in this family**.**
- **A notion of expressivity for composition formalisms (Verimag):** In Year3 and 4, the conceptual work on BIP has focussed on the development of an algebraic theory [BS07a, BS07b]. In the final year, Verimag has also proposed a new notion of expressiveness appropriate for formalisms that express composition of components. It compares component frameworks with respect to the ability to achieve new behaviours from a given set of component behaviours. The work proposes an SOS-style definition of glues, where operators are characterized as sets of SOS-rules, specifying the transition relation of composite components from the transition relations of their constituents. We provide expressiveness results for the glues used in BIP and for process algebras such as CCS, CSP and SCCS. We show that the glues used in CCS, CSP, and SCCS are less expressive than the general SOS glue, but that BIP has the same expressiveness as SOS-style rules, which means that when restricting to

[1] http://www.artemis-office.org/DotNetNuke/Activities/EICOSE/tabid/123/Default.aspx

memoryless composition or glue operators, BIP has maximal expressivity [BS08]. This is an indication that the concepts of BIP are as general as one may need.

- **Description of models of computation and of models of execution (CEA, Supélec):** The formal LEM language (PC-xUML) [CGMOBHM07] for modelling models of computation is now implemented as a UML profile available in the Papyrus modeler. The ModHel'X framework [BH08], which provides a generic meta model for describing heterogeneous systems, a generic execution engine for simulating heterogeneous models, and a language for describing models of execution and their interactions is also available in a preliminary version at http://wwwdi.supelec.fr/logiciels/modhelx/. We consider LEM as a language for specifying models of computation (rules of combination of behaviours), and ModHel'X as a framework for describing models of execution (algorithms for combining behaviours), which lead us to study the conformance of a model of execution to a model of computation in a way similar to the conformance of an implementation to a specification. These works are conducted in the context of the TheSys research group http://www.thesys.eu.org .

New Models of Computation (INRIA): Models of Computation was the focus of an ARTIST2 workshop in Zürich in Nov. 2006, which inspired further workon the topic. INRIA has proposed a novel Model of Computation (MoC): Kahn-extended Event Graph (KEG) which add "static control" (control known at compilation time) in the MoC Marked Graphs (MG). INRIA has also defined a process of *expansion*, which finds the parallelism in a model and transformes it to an “expanded” (more parallel) one. The approach has been illustrated on a simple C algorithm (a Sobel filter) [BCFMS08]. INRIA is also building a new version of their tool K-PASSA, which finds static schedules of system descriptions, in order to add the following MoCs: KEG, Synchronous Data Flow (SDF) and Latency-Insensitive Design (LID). A previous release was implementing Marked Graphs (MG) and a specific optimization called "equalization". In the context of the French regional CIM PACA collaborative center some of the results have been demonstrated to industrial partners (such as Texas Instruments, ST Microelectronics, NXP, Synopsys, and smaller French SMEs). INRIA is currently investigating the relevance of the KEG models and their associated static schedules for the design and optimization of Networks-on-Chip traffic. http://ralyx.inria.fr/2006/Raweb/aoste/uid27.html

Distributed Implementation of non-distributed specifications

The problem of realizing a distributed implementation of a non-distributed system description is a challenging problem, which has received attention by ARTIST partners, e.g., in the work on GALS (Globally Asynchronous, Locally Synchronous) systems. There are still many unsolved problems in establishing the foundations for distributed implementations. Progress at the end of ARTIST2 includes the following.

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

- **A new track on Loosely Time-Triggered Architectures (LTTA) (INRIA, Parades, and Verimag):** LTTA aims at relaxing the strict synchrony constraint of Kopetz' TTA by allowing local clocks of computing and communication units not to be synchronized. LTTA architectures are widely used (even more than strict TTA) in industrial control such as flight control, nuclear plant monitoring, railway control... and most of their programming uses synchronous formalisms (Simulink, SCADE/Lustre and similar control-based formalisms). We have studied several variants and have shown how specification semantics can be preserved [BCNPST07] [TPBSCN08] [CB08]. Verimag and INRIA have further developed initial work by Verimag on the study of Airbus system architecture for low level flight control. They have come up with the systematic idea of replacing token based mechanisms by the use of purely local counters with no additional link. Each unit maintains a local counter based on its own independent clock. This local counter controls the right to acquire new input data from the communication media, perform computation steps, and write output data to the communication media. This approach is entirely local. Pros and Cons of this approach are:
    - Pros: no back-pressure, no additional communication link, no blocking communication; this simplifies the design of fault-tolerance and degraded modes.
    - Cons: uses boundedness assumptions on the relative drift between local clocks (the management of the local counters depends on these bounds). This means a high cost when re-design is needed.
- **Implementing synchronous models on asynchronous architectures (PARADES, INRIA, SSA, and Verimag):** This item addresses the same question as the previous one by moving from loosely synchronised to fully asynchronous architectures and share in common some solutions. In collaboration with Cadence Berkeley Research Labs, and UCBerkely, a theory for the design of communication architectures has been developed, that would guarantee the same property as a synchronous architecture but would be implemented on an asynchronous one [MBFS07,TPBSCN08]. PARADES, INRIA, and Verimag, jointly with UC-Berkeley and Cadence Berkeley, have developed approach (a), resulting in publications [B&al07] and [T&al08]. The approach assumes a single-clocked synchronous specification – single-clocked is not really a restriction in this context as it can be relaxed by using the extra symbol *nil* meaning the absence of a certain data at a given reaction. It is known that such specifications can be seen as a Kahn Process Network with bounded buffers. This observation has been the basis for the development of so-called *elastic circuits* by Cortadella et al. and *latency insensitive designs with back-pressure* by Carloni and Sangiovanni-Vincentelli in the area of circuit design. These are circuits with token based mechanisms. Controlling buffer overflow is achieved by implementing backward tokens controlling the permission to write in buffers – hence the term of *back-pressure.* This idea has been adapted to our case where neither writing nor reading can be blocking, see the figure above. The idea is to replace blocking by skipping. Performance of such architectures is classically studied by means of Marked Graphs, a simple form of Petri nets where Max-Plus algebra applies. Pros and Cons of this approach are:
    - Pros: no assumption on local clocks; very adaptive, scales up easily to complex systems; easy upgrade.
    - Cons: need for back-pressure, which results in additional links, resulting in additional requests for fault tolerance mechanisms.

- **Reliability of distributed implementations (EPFL, PARADES):** EPFL and PARADES have designed and implemented a hierarchical version of the programming language Giotto, called Hierarchical Timing Language (HTL) for hard real-time systems. (see Section 2.3 on Y3 results). In Y4, the HTL framework has been extended to handle reliability. More precisely, EPFL, PARADES and UCB proposed an abstract notion of logical reliability for real-time program tasks that interact through periodically up-dated program variables. With each program variable is associated a *logical* (or *long-term*) *reliability constraint* (LRC), a real number between 0 and 1. If the LRC is 0.9, this means that in the long run, at least a 0.9 fraction of all periodic writes to this communicator are required to be valid values. The mapping of tasks to hosts must ensure the LRCs of all program variables. For this purpose, if hosts fail, it may be necessary that a task be replicated on several hosts. To check if an implementation satisfies all LRCs, the singular (or short-term) reliability guarantee (SRG) of updating a program variable with a valid value must be known. The SRG is again a real number between 0 and 1; for example, an SRG of 0.8 means that the probability that a host fails during the execution of a task invocation is 0.2. The SRG is a property of the architecture, just as WCETs are architectural properties. To achieve LRCs of 0.9 with hosts that guarantee only SRGs of 0.8, all tasks that write to communicators (with LRC 0.9) need to be replicated on two hosts. The HTL compiler has been extended to perform also a reliability analysis and to generate distributed code that satisfies the requirements [CGH+08] [PCS08].
- **New Heuristics in Scheduling for Reliability (INRIA):** As a contribution to scheduling for distributed reliable real-time systems, INRIA has proposed a new framework for the (length, reliability) bicriteria static multiprocessor scheduling problem. The first criterion remains the static schedule's length: this is crucial to assess the system's real-time property. For the second criterion, we consider the global system failure rate, seen as if the whole system were a single task scheduled onto a single processor, instead of the usual reliability, because it does not depend on the schedule length like the reliability does (due to its computation in the classical exponential distribution model). Therefore, we control better the replication factor of each individual task of the dependency task graph given as a specification, with respect to the desired failure rate. Compared to the other bicriteria (length, reliability) scheduling algorithms found in the literature, the algorithm we present here is the first able to improve significantly the reliability, by several orders of magnitude, making it suitable to safety critical systems [GK08].

Apart from conceptual contributions to the problem of distributed implementation, there is also a need for design principles and architectures for concretely realizing distributed implementations, typically on NoCs. Most VLSI circuits can be considered distributed systems. Since their components are designed independently, the assembly step is often a challenging problem that requires the design of communication interfaces to match different protocols and data parallelism, and the routing of global interconnect wires to meet the constraints imposed by the target clock period. The debate between those who favor standard bus architectures or variations thereof and those who advocate the adoption of NoC approaches ranging from constrained architectures to custom ones is vibrant.

- **Design of Communication Architectures (PARADES)**: UCBerkely, Columbia and PARADES, developed a common framework, COSI, for the synthesis of communication for distributed systems, including chips as well as buildings.The proposed approach embedded in COSI does not take sides even though the NoC approach has undisputable fundamental merits that may make it successful in the long run. Instead, COSI proposed a general methodology for the design of on-chip communication that can explore a large number of alternatives including as special cases NoCs, bus architectures and hybrid ones. Thanks to its generality the approach can be used to build a framework where different constrained solutions are compared using a number of evaluation factors. Models for functionality, cost, and performance of each element are captured in the library together with their composition rules. A mathematical framework was developed to model communication at different levels of abstraction from the point-to-point input specification to the library elements and the final implementation. The code is publicly available: http://embedded.eecs.berkeley.edu/cosi/Home.html

- **The Time-Triggered System-on-a-Chip (TTSoC) architecture (Vienna):** is a novel system architecture that enables the realization of mixed-criticality systems using SoCs. It represents the culmination of several years of effort by the TU Vienna team (see also previous results from previous years). The integration of subsystems with different criticality enables massive cost reduction by reducing the overall number of devices and networks (e.g., ECUs in car). To accomplish this goal, the TTSoC architecture offers inherent fault isolation mechanisms that prevent any unintended interference between application subsystems of different criticality. Vienna has demonstrated these capabilities using an automotive example with a safety-critical control subsystem and a multimedia subsystem. In the demo application, it is ensured by construction that any design fault in the multimedia subsystem cannot have any adverse effect on the safety-critical control subsystem. The central element of the presented System-on-Chip (SoC) architecture is a time-triggered Network-on-a-Chip (NoC) that interconnects multiple, possibly heterogeneous IP blocks called micro components. The SoC introduces a trusted subsystem, which ensures that a fault (e.g., a software fault) within the host of a micro component cannot lead to a violation of the micro component's temporal interface specification in a way that the communication between other micro components would be disrupted. For this reason, the trusted subsystem prevents a faulty micro component from sending messages during the sending slots of any other micro component. Furthermore, the time-triggered SoC architecture supports integrated resource management, and failure detection, masking, and encapsulation using Triple Modular Redundancy (TMR). In summary, The SoC architecture ensures *composability:* that upon the incremental integration of micro components, the prior services of the already existing micro components are not invalidated by the new micro components [KEHOP08,OEHK08,OFEH08,OKS08].

Interfaces and Composability

Interface theories with component reuse (EPFL): Interface theories have been proposed to support incremental design and independent implementability. Incremental design means that the compatibility checking of interfaces can proceed for partial system descriptions, without knowing the interfaces of all components. Independent implementability means that compatible interfaces can be refined separately, maintaining compatibility. General theories, which do not focus on a specific formalism for specifying interfaces but rather on what such formalisms can do, for interface-based design have been proposed, e.g., by EPFL (see report for Year 2). We have now shown that these interface theories provide no formal support for component reuse, meaning that the same component cannot be used to implement several different interfaces in a design. We therefore added a new operation to interface theories in order to support such reuse. For example, different interfaces for the same component may refer to different aspects such as functionality, timing, and power consumption. We gave both stateless and stateful examples for interface theories with component reuse. To illustrate component reuse in interface-based design, we showed how the stateful theory provides a natural framework for specifying and refining PCI bus clients [DHJP08].

Reasoning about systems of components. The problem of analyzing or verifying a system of components has continued to receive attention in several contexts developed by ARTIST2 members.

- **Contract-based verification for the Heterogeneous Rich Component (HRC) Model (INRIA, Parades, and Verimag):** In Y3, the SPEEDS project defined a meta-model for representing component systems which includes a notion of contract that can be attached to components (see Section 2.3). Work has progressed during Y4 [BCP07] [B08] [CMMSS08] [M etal08] [JM08] [Met08] [DJMNKSV08] [DM07]. We have defined a satisfaction relation between an implementation and a contract and a notion of refinement between contracts. Initially, these relationships have simply been defined in terms of inclusion between trace sets. We have also developed a general framework for contract-based reasoning, which handles (multipartner) rendez-vous – as in the HRC framework – as well as many different languages for describing behaviours notions of refinement under context [QG08]. We use BIP to represent contracts. First, we define a general notion of a component framework defined by (1) a set of composition operators (2) a family of possible behaviours, (3) a mapping from *n*-ary composition operators into *n*-ary composition operators on behaviours, and finally (4) a notion of refinement under context between behaviours. We provide then several sufficient conditions which can be used to prove refinement in any framework that satisfies a certain property ("allowing circular reasoning"). We consider two particular instances of such a framework: the first are I/O automata with the usual composition operator and a notion of refinement based on trace inclusion. The second one considers behaviours defined by modal transition systems, allows all composition operators definable in BIP and a notion of refinement under context obtained from the usual notion of simulation between modal transition systems. At the review of the Integrated Project Speeds, the project demonstrated the capability of integrating models from multiple commercial of the shelf modelling tools based on the SPEEDS HRC meta-model, as well as running various analysis methods on the HRC representation of such integrated models, including checks for refinement, design space exploration, contract based safety analysis and real-time analysis, and hosted simulation.
- **Compositional deadlock detection/verification (Verimag):** Verimag has continued its work on deadlock detection/verification and its implementation in the DeadlockFinder tool by combining structural analysis for component behaviours with structural analysis of connectors [BBSN08].
- **Integrating Modular Performance Analysis and Timed Automata Techniques (ETH, Uppsala)** During Year 2-4, Uppsala and ETH have been conducting work on combining the advantages of Modular Performance Analysis (MPA), which is based on the real-time calculus, and techniques based on timed automata. A prototype tool (named CATS) for compositional timing and performance analysis has been developed further during year 4. In CATS, a component can be characterized by equations over timed streams. The CATS tool is available at http://www.timestool.com/cats, and integrated in the Eclipse platform. During Y4, attention has also been given to handling cyclic dependencies in component-based real-time systems, which have not been well-understood in the context of modular performance analysis (MPA). To address this problem, a solid semantic foundation for MPA should be developed, linking operational behavior with the stram-based approach in MPA. ETH and Uppsala has developed a general operational semantics underlying the Real-Time Calculus, and used it to show that the behavior of systems with cyclic dependencies can be analyzed by fixpoint iterations. The work also characterizes conditions under which such iterations give safe results, and also show how precise the results can be [JPTY08].

Component Models: Existing approaches to enhancement of existing component models have been continued.

- **Unified component model for embedded middleware (CEA, INRIA, THALES, STMicroelectronics):** *The* First version of a unified common meta-model for CCM, UML, MARTE, Fractal and OASIS component models has been proposed (www.flex-eware.org).

- **ProCom component model for distributed embedded systems (MdH, Uppsala):** The work on SaveCCM by MdH and Uppala has continued with a component model suitable for distributed embedded systems, resulting in the ProCom component model. The ProCom component model is developed i) for scalable design of small or large embedded systems, ii) for integration of different models for prediction and analysis of components and system properties, and iii) to allow resource-efficient realizations at run-time. The desired characteristics have been obtained by designing a two-layered component model where the lower layer strictly defines the execution semantics and enables efficient timing and resource analysis, while the top level enables a variety of component designs and styles of communication. Together with ProCOM the Progress Integrated development Environemnt (Progress-IDE) is being developed, including, e.g., the UppaalPort analysis tool [HMP07]. In addition to the component model, MdH has developed techniques supporting the design and development, integrated with the component model. Some of them are: i) Context aware execution-time estimation ii) Stack-sharing in component-based systems, iii) Advanced flow analyis iv) Partial order verification v) Software component-based development process vi) Formalization and automation of component selection. [SVBCC08] http://www.mrtc.mdh.se/progress/

Deployment of LightWeight CCM components within a Flexible scheduling framework (Thales, Univ.Cantabria): In the context of the effort to combine real-time implementation technology and contract technology to build techniques for component-based design, in the FRESCOR project, University of Cantabria and Thales have continued their work on using a specialization of the Deployment and Configuration OMG standard to define an approach for the deployment of MicroCCM components [GHC+08] . A model based technology aiming at Ada implementation has been proposed [LDPM08]. The concept of interface in Ada 2005 significantly facilitates its usage as the basis for a software components technology. This technology, taking benefit of the resources that Ada offers for real-time systems development, is suitable for component-based real-time applications that run on embedded platforms with limited resources. The proposed technology uses the specification of components and the framework defined in the LwCCM standard, modifying it with some key features that make the temporal behaviour of the applications executed on it, predictable, and analysable with schedulability analysis tools. The dependency on CORBA is replaced by specialized communication components called connectors. The threads required by the components are created and managed by the environment, and interception mechanisms are placed to control their scheduling parameters in a per-transaction basis. This effort aims to proposing a new IDL to Ada mapping, a prospective standard of the OMG. http://www.ctr.unican.es/publications/plm-jmd-ppm-jlm-2008a.html.

Synthesis of Glue and Controllers from Specifications (EPFL, INRIA): This problem has been addressed by several lines of work. Controller synthesis problems are naturally formalized by games where one player (the program) has to entail some objective (the specification) no matter how the other players (other programs and external environment) behave. The winning strategy in such a game is a model of the controller to synthesize.

- EPFL has contributed several results on solving games, among them on timed games [CHP08].

- INRIA has proposed a schema of integrating Discrete Controller Synthesis (DCS) techniques into the modular compilation of an extended synchronous language. In this extended language, modularity is expressed by nodes, representing components associated with modular synthesis objectives; we can then obtain, by application of DCS tools on these components, some synchronous controllers controlling parts of programs. In this framework, we have implemented a translation schema of a subset of the Lucid Synchrone language into dynamic systems, for further application of Sigali, as DCS tool. Future work will consist in applying decentralized control methods, together with modular distribution of synchronous programs, in order to obtain automatically, from an annotated synchronous program, a distributed controlled system.

- INRIA has, together with Univ. of Auckland , developed a technique for synthesizing glue logic, termed as a converter, so that the parallel composition of the components and the converter also satisfies some desired specification. A converter is responsible for bridging different kinds of mismatches such as control, data, and clock mismatches. Mismatches are usually removed by the converter (similar to controllers in supervisory control of discrete event systems) by disabling undesirable paths in the protocol composition. We have generalized this convertibility verification problem, by using a new refinement called specification enforcing refinement (SER) between a protocol composition and a desired specification. The existence of such a refinement is shown to be a necessary and sufficient condition for the existence of a suitable converter. We have also proposed an approach to automatically synthesize a converter if a SER refinement relation exists.

Generating component models from observations of behaviour (Dortmund, Uppsala): Dortmund and Uppsala have been collaborating to develop automata learning techniques (aka regular inference) for automatically deriving behavioural models of components from observations of system behavior. They are intended to be used in situations where models or specifications are not available a priori, and where static source code analysis is not feasible.Potential uses of such models is in regression testing, as a guide for model based test suite generation, in generating models of systems and of component environments for various purposes. The work has resulted in the tool *LearnLib* [BRS06], mainly developed by Dortmund, which is a library for automata learning, with a flexible modular structure that can be configured to exploit specific properties of applications, in order to make automata learning scalable to realistic settings. During Year 4, standard automata learning techniques have been extended to a class of infinite-state systems that can handle this situation [BJR08]. Furthermore, work on developing techniques that make modelling of industrial protocols practical are in completion [BJ]. Finally, the work on.the work extending automata learning techniques to generate models of timed systems has been thoroughly worked out in the Ph.D. thesis of Olga Grinchtein [G08].

Industrial Liaison

Working meeting on Integrated Modular Avionics: On November 12-13, 2007, an ARTIST2 meeting on IMA (Integrated Modular Avionics) was co-organized by Albert Benveniste (INRIA), Paul Caspi (Verimag), in close cooperation with John Rushby (SRI), and hosted by Alberto Ferrari (PARADES) in Rome, Italy. The workshop has gathered participants from aeronautics industry, including manufacturers (Airbus, Boeing, Dassault-Aviation), system suppliers (Honeywell, Wind River), service companies (WW Technology group), labs (SRI, SAE AADL Committee), and academics (TU Vienna, Verimag). Detailed minutes are available from ARTIST2 Web site. More about conclusions are in Section 2.4.5.

Interaction with the Automotive industry

The integrated project SPEEDS has developed a layered meta-model of heterogeneous rich components (HRC) and standardized approaches for the integration of commercial industry standard modeling tools to assemble system-level design models with rich interface specifications by combining models expressed in any authoring tool compliant to the integration standard, including Matlab-Simulink/Stateflow, Rhapsody, and Scade. It is currently integrating a range of analysis methods supporting interface compliance testing and dominance analysis between contracts expressed in an extended automata model.

On March 4, 2008 a *SPEEDS Automotive Day* was organized to discuss with the automotive industry how the AUTOSAR methodology can be supported by SPEEDS technologies, striving to reconcile the advantage of early system-level analysis with the overall AUTOSAR objective of decoupling function design from its implementation. The discussion has been deepened in bilateral meetings between OFFIS and individual automotive companies (May 28: BMW, Sept 3: Bosch and ETAS; planned: Nov 6: Continental). The interaction with the automotive industry will be continued both through direct participation of Artist2 Members in Autosar (OFFIS, CEA), as well as through projects launched through EICOSE.

On June 16, 2008, a SPEEDS tutorial was held in the context of the INCOSE'08 6th biennial European systems engineering conference in Utrecht (http://www.incose.org/symp2008).

Since 2004, CEA has been strongly involved in setting up the Num@tec Automotive working group of System@tic Paris Région competitiveness cluster. In this context, a platform for component based development of automotive system has been launched in September 2007: the EDONA platform (www.edona.fr). It targets tool integration under the AUTOSAR standard and covers both requirements engineering, software architecture design and model based validation.

Interaction through EICOSE

Specifically related to the topic of component based design are strategic initiatives taken by the Artemis Innovation Cluster on Transportation, EICOSE, to create a reference technology platform for embedded systems design, which in particular will strive to harmonize major existing initiatives for component models in embedded systems design, taking into account industry standards such as Autosar and SysML. Eicose has launched project proposals both in the context of ITEA (with an emphasis on open-source developments) as well as the Joint Undertaking Artemis (with an emphasis on the safety critical embedded systems market) towards theses objectives, thus contributing to the overall Artemis objectives of driving future European Standards for Embedded Systems design. This initiative will in particular benefit from the Artist2 activity on component based design for heterogeous systems, as well as on results of related research projects such as SPEEDS and COMBEST.

2.4.2 Individual Publications Resulting from these Achievements

University of Cantabria

[LPDM07] P.López, P.Pacheco, J.M.Drake and J.L. Medina, "RT-CCM: Tecnología de componentes de tiempo real basada en Ada 2005". II Simposio de Sistemas de Tiempo Real in the 2º Congreso Español de Informática (CEDI 2007), Zaragoza, Spain September 2007.

[GHC+08] Jean-Louis Gilbert, Olivier Hachet, Jérôme Chauvin, Patricia López, José María Drake, Julio Medina, and Michael González Harbour. "Integration of Flexible Real-Time Scheduling Services in a Lightweight CCM-Based Framework". Proceedings of the Workshop on Distributed Object Computing for Real-time and Embedded Systems, July 14 – 16, 2008, Washington, DC, USA

[LDM08] Patricia López Martinez, José María Drake Moyano, Julio Medina Pasaje. "Real-Time Extensions to Deployment and Configuration of Component-based Distributed Applications". Proceedings of the Workshop on Distributed Object Computing for Real-time and Embedded Systems, July 14 – 16, 2008, Washington, DC, USA

[LDPM08] Patricia López Martínez, José M. Drake, Pablo Pacheco, and Julio L. Medina. "An Ada 2005 Technology for Distributed and Real-Time Component-based Applications". In Proceedings of the 13th International Conference on Reliable Software Technologies, Ada-Europe, Venice (Italy), in Lecture Notes on Computer Science, Springer, LNCS 5026, June, 2008, ISBN: 3-540-68621-7, pp. 254-267.

CEA

[FGG07] Alain Faivre, Alain Faivre, Christophe Gaston, Pascale Le Gall, *Symbolic Model Based Testing for Component Oriented Systems*, Proceeding of Joint 19th IFIP International Conference on Testing Communicating Systems and 7th International Workshop on Formal Approaches to Testing of Software (TestCom/Fates - 2007), Tallinn, Estonie, LNCS volume 4581/2007, Springer, 2007.

[TDGBT07] F. Thomas, J. Delatour, S. Gérard, M. Brun, F. Terrier. *Contribution to explicit modeling of execution platforms - Contribution à la modélisation explicite des plates-formes d'exécution pour l'IDM*, TSI - L'Objet, 0291-7335, 2007.

EPFL

[CHP08] Krishnendu Chatterjee, Thomas A. Henzinger, and Vinayak Prabhu. Timed parity games: Complexity and robustness. Proceedings of the Sixth International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS), Lecture Notes in Computer Science, Springer, 2008.

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

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

INRIA

[AFG08] T. Ayav, P. Fradet, A. Girault, ” Implementing Fault-Tolerance by Automatic Program Transformations”, *ACM Trans. on Embedded Computing Systems*, 7(4), July 2008.

[BCR08] Albert Benveniste, Benoît Caillaud, and Raclais. 2008.

[BCFMS08] J. Boucaron, A. Coadou, B. Ferrero, J.-V. Millo, R. de Simone, “Kahn-extended Event Graphs”, INRIA Research Report RR-6541, 2008.

[B08] A. Benveniste, “Multiple viewpoint contracts”, Invited talk at FIT2008.

[GK08] A. Girault, H. Kalla. “A novel bicriteria scheduling heuristics providing a guaranteed global system failure rate”, IEEE Trans. on Dependable and Secure Computing, To appear.

[PSS07] D. Potop-Butucaru, R. de Simone, Y. Sorel, “Necessary and sufficient conditions for deterministic desynchronization”, EMSOFT’07, Salzburg, Austria, October 2007.

[LMS08] S.-Y. Lee, F. Mallet, R. de Simone, “Dealing with AADL End-to-end Flow Latency with UML MARTE”, UML&AADL'08, Belfast, Ireland, April 2008.

[DDM08] J. Dubreil, P. Darondeau, H. Marchand, “Opacity enforcing control synthesis”, in Workshop on Discrete Event Systems, WODES'08, Gothenburg, Sweden, March 2008.

[DJM08] J. Dubreil, T. Jéron, H. Marchand, “Monitoring information flow by diagnosis techniques”, Research Report IRISA, No 1901, August 2008.

[SBDP07] S. Saudrais, O.Barais, L. Duchien, N. Plouzeau: "From formal specifications to QoS monitors", *Journal of Object Technology*, vol. 6, no. 11, Special Issue on Advances in Quality of Service Management, Dec. 2007, pp. 1–20.

[Sau07] S. Saudrais, "Qualité de service temporelle pour composants logiciels", Ph.D. Thesis, Université de Rennes 1, Dec. 5, 2007 (in French).

Mälardalen University (MdH)

[CCP07] V. Cortaliessa, I. Crnkovic, P. Potena, "Driving the selection of COTS components on the basis of system requirements", Automated Software Engineering (ASE) 2007, IEEE, Atlanta, US, November, 2007

[SVBCC08] S. Sentilles, A. Vulgarakis, T. Bures, J. Carlson, I.Crnkovic. "A Component Model for Control-Intensive Distributed Embedded Systems." Proc.11th Int. Symp. on Component Based Software Engineering (CBSE2008), Karlsruhe, Germany, October, 2008.

OFFIS

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

[Met08] A. Metzner. Scheduling of distributed real-time systems under functional constraints. In Proceedings of the 13th IEEE International Conference on Emerging Technologies and Factory Automation. IEEE Computer Society, 2008.

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

[DM07] W. Damm, A. Metzner. A Design Methodology for Distributed Real-Time Automotive Applications, Next Generation Design and Verification Methodologies for Distributed Embedded Control Systems. Proceedings of the GM R&D Workshop, pages 157 – 174, of Lecture Notes in Computer Science, Springer Verlag, 2007.

PARADES

[MBFS] L. Mangeruca, M. Baleani, A. Ferrari and A. Sangiovanni-Vincentelli, Semantics Preserving Design of Embedded Control Software from Synchronous Models, *IEEE Transactions on Software Engineering,* Vol. 33, N. 8, pp. 497-509, August 2007.

[PCS0508] C. Pinello, L.P. Carloni, and A.L. Sangiovanni-Vincentelli, "Fault-Tolerant Distributed Deployment of Embedded Control Software." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* Vol. 27, No. 5, May 2008.

[PCS07] A. Pinto, L.P. Carloni, and A.L. Sangiovanni-Vincentelli. "A Communication Synthesis Infrastructure for Heterogeneous Networked Control Systems and its Application to Building Automation and Control." Proceedings of the Seventh International Conference on Embedded Software (EMSOFT), 2007.

[PCS08] A. Pinto, L.P. Carloni, and A. Sangiovanni-Vincentelli, "COSI: A Framework for the Design of Interconnection Networks." *IEEE Design & Test of Computers.* Vol. 25, No. 5, September/October 2008.

[PCS] A. Pinto, L.P. Carloni, and A. Sangiovanni-Vincentelli, "A Methodology for Constrained-Driven Synthesis of On-Chip Communications." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (to appear).

Supélec

[HB08] C. Hardebolle, F. Boulanger, *ModHel'X: A Component-Oriented Approach to Multi-Formalism Modeling*, Models in Software Engineering, Holger Giese (editor), Reports and Revised Selected Papers. Workshop and Symposia at MoDELS 2007, Springer, LNCS 5002, pages 247—258, February 2008

[BH08] F. Boulanger, C. Hardebolle, *Simulation of Multi-Formalism Models with ModHel'X*, Proceedings of the IEEE International Conference on Software Testing, Verification and Validation (ICST2008), pages 318—327, Lillehammer, Norway, 9--11 April 2008

[JBM08] C. Jacquet, F. Boulanger, D. Marcadet, *From Data to Events: Checking Properties on the Control of a System. I*n: MEMOCODE 2008, Anaheim, CA, pp. 17-26.

Uppsala University

[BJ08] T. Berg, B. Jonsson: Regular Inference for Communication Protocols, in preparation, 2008.

[G08] O. Grinchtein. *Learning of Timed Systems,* Ph.D. Thesis, Uppsala University, May 2008.

Vienna

[KEHOP08] H. Kopetz, C. El Salloum, B. Huber, R. Obermaisser, C. Paukovits: "Composability in the Time-Triggered System-on-Chip Architecture" In "Proceedings of the 21st IEEE International SoC Conference (SOCC)", Newport Beach, CA, USA, Sept. 2008.

[OEHK08] R. Obermaisser, C. El Salloum, B. Huber, H. Kopetz: "The Time-Triggered System-on-a-Chip Architecture" In "Proceedings of the IEEE International Symposium on Industrial Electronics", Cambridge, UK, June 2008.

[OFEH08] R. Obermaisser, B. Froemel, C. El Salloum, B. Huber: "Integrating Safety and Multimedia Subsystems on a Time-Triggered System-on-a-Chip" In "Proceedings of the 6th IEEE International Conference on Industrial Informatics (INDIN 2008)", pp. 270-275, Daejeon, Korea, July 2008.

[OKS08] R. Obermaisser, H. Kraut, C. Salloum: "A Transient-Resilient System-on-a-Chip Architecture with Support for On-Chip and Off-Chip TMR" In "Proceedings of the 7th European Dependable Computing Conference", pp. 123-134, Kaunas, Lithuania, May 2008.

Verimag

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

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

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

[BS07b] Simon Bliudze and Joseph Sifakis. Causal semantics for the algebra of connectors. Technical report, Verimag, 2007. To appear in *Proc. Software Technologies Concertation on Formal Methods for Components and Objects* (FMCO 2007), 2008.

[BS08] Simon Bliudze and Joseph Sifakis, A Notion of Glue Expressiveness for Component-Based Systems. In *Proc. of the 19th International Conference on Concurrency Theory* (CONCUR'08), LNCS 5201, 508–522, Springer, 2008.

[QG08] Sophie Quinton and Susanne Graf. Contract-based verification of hierarchical systems of components. In IEEE International Conference on Software Engineering and Formal Methods (SEFM08), 2008.

2.4.3 Interaction and Building Excellence between Partners

The main concrete interaction between partners takes place by discussions at workshops, meetings and conferences, by mutual visits, and by collaboration in research projects.

Workshops organized by the cluster, or with significant cluster participation are used for discussions on central research topics. Such discussions have occurred, e.g., at the ARTIST2 plenary meeting (Nov. 2007), the workshop on Integrated Mocular Avionics (Nov. 2007), at the Embedded Systems Week (Salzburg, Oct. 2007), etc.

Interaction also occurs through direct mutual visits in connection with collaborative work. CEA LIST and Supélec worked together on a formal approach for modelling heterogeneous systems for the PC-xUML (Prospective Component - eXecutable UML) component of the OpenDev Factory sub-project of the Software Factory project of the System@tic Paris-Région competitiveness cluster. Gabriel Kalyon and Thierry Massart (ULB) visited INRIA-Rennes in Spring 2008 to work on control synthesis under partial observation. Thierry Legall (INRIA-Rennes) visited ULB in Spring 2008 to work on verification using abstract interpretation.

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

- SPEEDS where INRIA, OFFIS, PARADES and VERIMAG are collaborating intensely for developing a modelling framework, a design methodology and system level validation techniques.
- In the newly started COMBEST project, almost all partners of this cluster collaborate for developng a design theory for complex embedded systems, fully covering heterogeneity, interface specifications, composability, compositionality, and refinement for functional and extra-functional properties. In one line of work, INRIA, EPFL, Uni. Trento, and PARADES are together involved in further developing studies on *Interface Theories*. The objective is to allow for new services to be offered by such theories, in addition to substitutability which was offered from the beginning in original de Alfaro-Henzinger framework. We aim at offering also the possibility to associate multiple interfaces to a component, via conjunction. Also, we want to support Assume/Guarantee reasoning in a way compliant with engineering practice, with the help of *residuation theory*. A joint paper is in preparation.
- In the SAVE project, Uppsala and Mälardalen are collaborating on component models in the Swedish National project SAVE [ÅCF+07] [HP07].
- The automata learning work in which Dortmund and Uppsala collaborate, has lead to the European project CONNECT, which will start in 2009.
- Other projects with an analogous role include the still ongoing OpenEmBeDD and the now terminated Persiform projects.

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

2.4.4 Joint Publications Resulting from these Achievements

[BNBBG08] C. Baier, N. Bertrand, P. Bouyer, T. Brihaye, M. Groesser, “Almost-Sure Model Checking of Infinite Paths in One-Clock Timed Automata”, in Proceedings of the 23rd Annual IEEE Symposium on Logic in Computer Science (LICS'08), Pittsburgh, PA, USA, June 2008.

[BBBBG07] C. Baier, N. Bertrand, P. Bouyer, T. Brihaye, M. Groesser, “Probabilistic and Topological Semantics for Timed Automata”, in Proceedings of the 27th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'07), Arvind, Sanjiva Prasad (eds.), Volume 4855, New Delhi, India, December 2007.

[BBG08] C. Baier, N. Bertrand, M. Groesser, “On Decision Problems for Probabilistic Büchi Automata”, in Proceedings of the 11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'08), Budapest, Hungary, March 2008.

[BCCCS08] A. Benveniste, B. Caillaud, L.P. Carloni, P. Caspi, and A.L. Sangiovanni-Vincentelli, “Composing Heterogeneous Reactive Systems.” *ACM Transactions on Embedded Computing Systems*, Vol. 7, No. 4, July 2008.

[BCP07] A. Benveniste, B. Caillaud, and R. Passerone. A Generic Model of Contracts for Embedded Systems. INRIA Research Report 6214, June 2007.

[BCNPST07] A. Benveniste, P. Caspi, M. Di Natale, C. Pinello, A. Sangiovanni Vincentelli, and S. Tripakis. Loosely Time-Triggered Architectures based on Communication-by-Sampling. Proc. of EMSOFT'07, Oct. 1-3, 2007.

[BJR08] T. Berg, B. Jonsson, H. Raffelt: Regular Inference for State Machines Using Domains with Equality Tests. In Proc. FASE 2008, LNCS 4961, pp. 317-331.

[BBBM08] N. Bertrand, P. Bouyer, Th. Brihaye, N. Markey, “Quantitative Model-Checking of One-Clock Timed Automata under Probabilistic Semantics”, in Proceedings of the 5th International Conference on the Quantitative Evaluation of SysTems (QEST'08), Saint Malo, France, September 2008.

[CB08] P. Caspi and A. Benveniste. Time-Robust discrete control over networked Loosely Time-Triggered Architectures. In Proc. of 2008 IEEE Control and Decision Conference. Cancun, Dec. 9-11, 2008.

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

[CGH+08] C. Chatterjee, A. Ghosal, T. Henzinger, D. Iercan, C. Pinello, and A. Sangiovanni-Vincentelli. “Logical Reliability of Interacting Real-Time Tasks.” In Proc. DATE 2008.

[CJMR08] C. Constant, T. Jéron, H. Marchand, V. Rusu, “Validation of Reactive Systems”, in Modeling and Verification of Real-TIME Systems - Formalisms and software Tools, S. Merz, N. Navet (eds.), Chapter 2, Pages 51-76, Hermès Science, January 2008.

[CGMOBHM07] A.Cuccuru, C. Gaston, C. Mraidha, A. Ohayon, F. Boulanger, C. Hardebolle, D. Marcadet, *OpenDevFactory, PC-xUML : Rapport final*, final report of task 1.1.5 of the OpenDev Factory project, System@tic, November 2007.

[DJMNKS08] W. Damm, B. Josko, A. Metzner, M. Di Natale, H. Kopetz, A. Sangiovanni Vincentelli "Software Components for Reliable Automotive Systems", Proceedings of the Design, Automation, and Test in Europe Conference, München, 2008.

[FKPY07] E. Fersman, P. Krcal, P. Pettersson, W. Yi, Task Automata: Schedulability, Decidability and Undecidability. *International Journal of Information and Computation*, vol. 205, nr 8, pp. 1149-1172, Elsevier, August, 2007.

[HMP07] J. Håkansson , A. Möller, P. Pettersson, “Partial Order Reduction for Verification of Real-Time Components.” Proc. 5th Int. Conf. on Formal Modelling and Analysis of Timed Systems (FORMATS), LNCS 4763, pp. 211-226, Springer Verlag, October, 2007.

[JPTY08] B. Jonsson, S. Perathoner, L. Thiele, and W. Yi. Cyclic dependencies in modular performance analysis. Proc. EMSOFT 2008, Atlanta, Georgia, to appear.

[M etal08] C. Mrugalla et al.: SPEEDS Meta-model – Profile Definition. SPEEDS deliverable D2.1.4, May 2008

[PCS07] A. Pinto, L.P. Carloni, and A.L. Sangiovanni-Vincentelli. “A Communication Synthesis Infrastructure for Heterogeneous Networked Control Systems and its Application to Building Automation and Control.” Proceedings of the Seventh International Conference on Embedded Software (EMSOFT), 2007.

[PCS08] A. Pinto, L.P. Carloni, and A. Sangiovanni-Vincentelli, "COSI: A Framework for the Design of Interconnection Networks." *IEEE Design & Test of Computers* 25(5), September/October 2008.

[PCS] A. Pinto, L.P. Carloni, and A. Sangiovanni-Vincentelli, "A Methodology for Constraint-Driven Synthesis of On-Chip Communications." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (to appear).

[SHPC08] S.Sentilles, J. Håkansson, P. Pettersson, I. Crnkovic, Save-IDE – An Integrated development environment for building predictable component-based embedded systems. In Proceedings of the 23rd IEEE/ACM International Conference on Automated Software Engineering (ASE'08), September, 2008, ACM.

[TPBSCN08] S. Tripakis, C. Pinello, A. Benveniste, A. Sangiovanni Vincentelli, P. Caspi, and M. Di Natale. Implementing Synchronous models on Loosely Time-Triggered architectures. *IEEE Transactions on Computers* 57(10), 2008.

2.4.5 Keynotes, Workshops, Tutorials

Keynote : Adding SPEEDS to AUTOSAR.

Werner Damm, OFFIS - DATE 08, Automotive Session, Munich, Germany, March 12, 2008.

The invited talk discussed how AUTOSAR based design processes can be enriched with the SPEEDS enabled system leven analysis methods.
http://www.date-conference.com/

Keynote: Grand Challenges for Real-Time Systems

Thomas A. Henzinger - 20th Euromicro Conference on Real-Time Systems (ECRTS), Prague, Czech Republic, July 2008.

We summarized some current trends in embedded systems design and pointed out some of their characteristics, such as the chasm between analytical and computational models, and the gap between safety-critical and best-effort engineering practices. We called for a coherent scientific foundation for embedded systems design, and we discussed a few key demands on such a foundation: to provide support for building predictable and robust systems, to ncompass several manifestations of heterogeneity, and to achieve constructivity and compositionality in design. This talk was based on joint work with Joseph Sifakis.

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

Keynote: The Quest for Correctness -- Beyond Verification
Joseph Sifakis - CAV 2008, Princeton, July 2008, http://www.princeton.edu/cav2008/

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

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

Invited Lecture: Challenges in Embedded Systems Design: Predictability and Robustness

Thomas A. Henzinger - Royal Society Meeting: From Computers to Ubiquitous Computing, London, United Kingdom, March 2008.

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

Workshop: ARTIST International Workshop on IMA

Rome - November 12-13

On November 12-13, 2007, an ARTIST2 meeting on IMA (Integrated Modular Avionics)[2] was co-organized by Albert Benveniste (INRIA), Paul Caspi (Verimag), in close cooperation with John Rushby (SRI), and hosted by Alberto Ferrari (PARADES) in Rome, Italy. The workshop has gathered participants from aeronautics industry, including manufacturers (Airbus, Boeing, Dassault-Aviation), system suppliers (Honeywell, Wind River), service companies (WW Technology group), labs (SRI, SAE AADL Committee), and academics (TU Vienna, Verimag). Detailed minutes are available from ARTIST2 Web site[3]. Among the conclusions of this workshop we can briefly report some of the recommendations for research directions: How to mitigate the complexity of processors and architectures? Look at architectures that are going to mass market and look at how to accommodate them. We should develop concepts of platforms that allow getting desirable architecture on top of less desirable ones. We should develop research facilitating the reuse of partial certifications.

Workshop: Euromicro SEAA (Software Engineering and Advanced Applications), Component-Based Software Engineering (CBSE) Track

Parma, Italy, September 3-5, 2008

The goal of the CBSE track at Euromicro SEAA is to point out the overall challenges and problems of the component-based, or service-oriented, approach, and to show the new ideas, solutions and practices. The topics cover practice and research to improve the theories, technologies, and processes in component-based and service-oriented software development. Ivica Crnkovic, MdH, is co-chairing the workshop with Kung-Kui Lai.

PROGRESS Workshop on Component Models for Embedded Systems (COMES'08)

Sigtuna, Sweden, June 17th - 18th, 2008

The aim of the workshop was to i) present and discuss the current research and practical results in development of embedded systems using component-based development approaches ii) Discuss and point out the challenges and possible solution directions in applying the component-based approach to achieve predictability of component-based embedded software systems. The workshop was setup as a set of sessions in which each session focussed on particular challenges. Each session started with some introductory presentations and continued with discussions, hopefully leading to some conclusions. Orgranisers: HansHansson, Thomas Nolte, Ivica Crnkovic, http://www.mrtc.mdh.se/progress/COMES/

[2] http://www.artist-embedded.org/artist/-ARTIST2-meeting-on-Integrated-.html

[3] http://www.artist-embedded.org/docs/Events/2007/IMA/Artist2_IMA_Minutes.pdf

Summer school MOVEP 2008: Summer school on modeling and verifying parallel processes
Orléans, France – June 23-27, 2008

The purpose of MOVEP is to bring together researchers, students and people from industry working in the fields of control and verification of concurrent and reactive systems. The school seeks to offer a broad spectrum of current research in this area of theoretical and applied computer science. The topics covered by MOVEP include model checking, controller synthesis, software verification, temporal logics, real-time and hybrid systems, stochastic systems, security, etc. The program of the School consists of six 2h30 tutorials and five 1h30 talks.

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

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

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

Workshop : SafeCert 2008 International Workshop on the Certification of Safety-Critical Software Controlled Systems
ETAPS 2008
Budapest, Hungary –29 March, 2008, organized by TU Braunschweig and OFFIS

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

Tutorial: Contract-Based System Design - The SPEEDS Approach -- INCOSE 2008
Utrecht, The Netherlands – June 16, 2008

The aim of this half day tutorial was to disseminate the results of the SPEEDS project towards the community of the potential users of the developed technology. The tutorial focused on the contracts based development methodology being worked-out within the project. It aimed

specifically at iterative development as opposed to the traditional waterfall requirement flow down. At the centre of the methodology is the definition of a rich component model which allows the capture of functional and non functional system properties in the form of contracts.
http://www.incose.org/symp2008/

3. Milestones, and Future Evolution Beyond the NoE

3.1 Milestones

- Year 3:
  - Unification of models of computation and comparison beween frameworks using denotational and operational semantics*. We made some progress in that direction, which have been followed up in Year 4, e.g., byr establishing links between causal semantics for connectors and partial order semantics for clocks in Signal.*
  - Rich heterogeneous interfaces and associated verification techniques based on Assume/Guarantee. *Metamodel for Heterogeneous Rich Components established. Several programming language constructs and analysis approaches for timing and resource contracts have been developed. Techniques for synthesizing adaptors for component developed have ben developed.*
  - A meeting on *Integrated Modular Avionics* and its impact of embedded systems design in avionics; will be scheduled during spring 2007; expected for fall 2007. The approach for this meeting will be similar to the one followed for the Beyond Autosar meeting. *This meeting was held November 12-13 in Rome at the PARADES offices. Speakers include key persons from Airbus, Dassault-Aviation, Israeli Aerospace Industries, Honeywell and Windriver, plus John Rushby and ARTIST2 participants.*
- Year 4:
  - Definition and classification of unified frameworks encompassing heterogeneity. *In particular, unification has been achieved between synchronous reactive semantics and asynchronous semantics and its usefuleness demonstrated by the definition of a structural semantics for Lustre in the BIP language (PhD of Vassiliki Sfyrla, Work in Progress). We have also made a comparison between Signal and BIP (collaboration between Verimag and INRIA, work in Progress)*
  - Verification framework for rich heterogeneous interfaces. We started developing contract-based compositional verification methods as well as methods based on structural analysis. A *general framework for contract-based reasoning for component frameworks allowing also (multipartner) rendez-vous – as they exist in the HRC framework – has been developed. Methods for deadlock detection based on structural analysis have bee developed and implemented. Formalisms for stream-based and automata-based reasoning about component systems have been developed and implemented.*
  - Organize a meeting on *predictability of hardware in automotive/avionics and semiconductor industry*. The approach for this meeting will be similar to the one followed for the Beyond Autosar meeting. *Several meetings with industry have been organized to discuss technologies for the AUTOSAR architecture, notably those developed by the IP SPEEDS, e.g., the SPEEDS Automotive Day (March 4, 2008). Predictability of hardware and software has become the topic of the newly started project PREDATOR with Artist2 partners, plus one partner each from automotive and avionics industry.*

3.2 *Indicators for Integration*

The activity is expected to play a strong role in integration between cluster partners, as well as with partners of other Artist2 clusters, since techniques from component-based design have applications in a large variety of contexts.

One indicator is the number of joint publication, which has increased significantly (e.g., from 9 to 23 from Y3 to Y3). Another indicator is the setting up of joint projects between partners. We give examples:

- SPEEDS where INRIA, OFFIS, PARADES and VERIMAG are collaborating intensely for developing a modelling framework, a design methodology and system level validation techniques.
- Setting up the COMBEST project is a strong sign of integration between partners of this cluster (Verimag, EPFL, INRIA, OFFIS, PARADES) but also with the Execution Platforms Cluster (ETHZ and Braunschweig).
- The work on generating component models, in which Dortmund and Uppsala collaborate, has lead to the European project CONNECT, which will start in 2009.
- Other projects with an analogous role include the still ongoing OpenEmBeDD and the now terminated Persiform projects.

There are many other collaborations. E.g., Verimag and INRIA have collaborated on the unification between synchronous and asynchronous paradigms through the comparison between BIP and Signal on one hand, and through the work on loosely time-triggered architectures joint also with TU Vienna on the other hand. Verimag and ETHZ have collaborated on a translation from the DOL performance evaluation tool to BIP. A key issue is the generation of an executable model (BIP) from an analytic model (DOL).

3.3 *Main Funding*

Main sources of funding include:

- the Integrated Projects
  - DECOS https://www.decos.at/
  - MODELWARE
  - RUNES, http://www.control.lth.se/research/runes.html
  - SPEEDS
- the STREPS
  - DYSCAS - www.dyscas.org
  - ATESST + ATESST2 - www.atesst.org
  - Q-ImPrESS - Quality Impact Prediction for Evolving Service-Oriented Software
  - COMBEST – http://www.combest.eu/
  - FRESCOR
  - Genesys – http://www.genesys-platform.eu/
- ITEA2 Projects
  - FLEXI - Flexible Global Product Development and Integration, http://flexi-itea2.org/

- the national funding agencies
    - Swiss National Science Foundation
    - US National Science Foundation
    - French Agence Nationale de la Recherche
    - FLEXCON, SAVE, and SAVE++ Swedish research programs
    - PROGRESS - http://www.mrtc.mdh.se/progress/ funded from Swedish Foundation for Strategic Research (SSF)
    - Swedish Research Council
    - National Science Foundation under the CHESS program
    - AVACS (Automatic Verification and Analysis of Complex Systems, Transregional Collaborative Research Center, http://www.avacs.org)
    - Usine Logicielle, System@tic Paris-Région pole of competitivity (http://www.usine-logicielle.org).
    - EDONA (Open tool integration platform for AUTOSAR embedded system development), System@tic Paris-Région pole of competitivity (www.edona.fr).
    - Flex-eWare (Unified component based middleware platform – www.flex-eware.org), French national project.
    - Lambda (System level engineering using model and component based technologies), System@tic Paris-Région pole of competitivity.
- Industry
    - Cadence
    - Pirelli
    - ST Microelectronics
    - United Technology Corporation (Otis, Carrier, Chubb)
    - ABB
    - Ericsson
    - CC Systems
    - Geensys
    - Alstom

3.4 Future Evolution Beyond the Artist2 NoE

The work in Artist2 have made produced many important results towards making component-based design of heterogeneous embedded systems feasible in industrial embedded systems development. Many important challenges in modelling and reasoning have been overcome, and several industrial application projects are in progress. For the future, the challenge of putting model-based design of embedded systems on a firm scientific basis involves further problems that should be addressed. Important problems are the following.

- There is currently a dichotomy between operational and transformational modeling approaches. Operational means automata-based: these approaches work on a component level, and have been successful in model checking, protocol verification, and code generation. Transformational means stream-based: these approaches work on the system level, and have been successful in performance analysis. While operational approaches have difficulties to scale to systems, transformational approaches suffer a loss of precision. We plan to develop techniques for bridging and combining both approaches.

- Embedded software design differs from other software design in that behavioural properties must be reconciled with resource constraints. This suggests the important of resource modelins, to permit the exploration of trade-offs between multiple dimensions, such as functionality, reliability, performance, and resource consumption. We expect different formalisms to be appropriate for different purposes, such as time-power trade-offs in power-constrained computing. The relevant dimensions (e.g., time and power) must then be captured within interfaces in order to support component-based design.
- Our current models for modeling quantitative properties of systems systems (Markov processes; timed automata; hybrid automata) tend to be brittle and overly sensitive towards arbitrarily small numeric perturburances. We need robust models for stochastic, timed, and hybrid systems.

The above and other challenges will be addressed in current and to-be-initiated collaboration projects between Artist2 partners and others. Examples include ArtistDesign, and the omgoing IP project SPEEDS. Among further examples, Verimag will continue the work on BIP in the framework of the ArtsistDesign NoE as well as in the framework of the COMBEST and GENESYS ICT projects. GENESYS has adopted BIP to model reference architectures (see http://www.genesys-platform.eu/Genesys_Del_D6-1_31-03-2008.pdf). In COMBEST, BIP is used to model a complex avionic system based on AFDX (case study proposed by EADS, http://www.combest.eu/home/?link=Application1). Finally BIP is one of the two component frameworks used in the French industrial project MIND (main industrial partners STMicroelectronics and Schneider Electric).

4. Internal Reviewers for this Deliverable

Michael Gonzalez Harbour