IST-004527 ARTIST2
Network of Excellence
on Embedded Systems Design

Activity Progress Report for Year 3

JPIA-Platform / JPRA-Cluster Integration / JPRA-NoE 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 3
1.1 ARTIST Participants and Roles 3
1.2 Affiliated Participants and Roles 4
1.3 Starting Date, and Expected Ending Date 4
1.4 Baseline 4
1.5 Problem Tackled in Year 3 6
1.6 Comments From Year 2 Review 8
1.6.1 Reviewers' Comments 8
1.6.2 How These Have Been Addressed 8

2. Summary of Activity Progress 9
2.1 Previous Work in Year 1 9
2.2 Previous Work in Year 2 9
2.3 Current Results 11
2.3.1 Technical Achievements 11
2.3.2 Individual Publications Resulting from these Achievements 18
2.3.3 Interaction and Building Excellence between Partners 21
2.3.4 Joint Publications Resulting from these Achievements 21
2.3.5 Keynotes, Workshops, Tutorials 22

3. Future Work and Evolution 26
3.1 Problem to be Tackled over the next 12 months (Sept 2007 – Aug 2008) 26
3.2 Current and Future Milestones 28
3.3 Indicators for Integration 29
3.4 Main Funding 29

4. Internal Reviewers for this Deliverable 31

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. 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 HRC 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.*

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 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 3

Design of Heterogeneous Systems:

- Study component frameworks encompassing heterogeneity. This includes multiparty interaction involving strong or weak synchronization, synchronous and asynchronous execution, different abstraction levels and views. The results have been used for the defition of the HRC component model in the SPEEDS IP. This model is used a common exchange format between the modelling and validation tools.
- Study unifying semantics for the studied component frameworks. We distinguish two action lines. One in the continuation of the work by INRIA, Parades, and Verimag for the unification of models of computation based on denotational semantcis (tagged traces). The other based on operational semantics in the continuation of work pursued mainly by Verimag (BIP)

- Integrate existing knowledge in the field of real-time systems, dependable systems, modelling and component design into new application domains such as mobile embedded systems and wireless sensor networks.

Interfaces and Composability

- Development of a common meta model as the foundation for component based construction of complete virtual system models: 1) based on a compositional semantic, 2) providing a framework for multiple viewpoint (functional and non-functional), 3) enabling full-scale reuse of components, 4) offering, from COTS modelling tools, access to meta-model compliant components and, 5) allowing to early assess project risks at subsystem level to secure concurrent design processes.
- Study theory and rules for correctness-by-construction. Partially based on results from [GGM-CMS07], we developed new composability and compositionality techniques for deadlock-freedom. These are based on the separation of concerns underlying the layered BIP model. They use structural analysis techniques of the connectors of BIP models. Deadlock-freedom preservation is checked by analysis of a dependency graph relating the ports of the components. The dependency relation associates with a port the set of the ports with which synchronization is needed in some interaction. A circuit in the dependency graph characterizes a potential deadlock situation. More detailed analyses of the behaviour atomic components allow deciding deadlock-freedom. These techniques have been implemented in DeadlockFinder a prototype tool that generates from BIP models sufficient conditions for deadlockfreedom. These conditions can be checked interactively either by using model-checking tools or by using invariants provided by theuser.
- Develop programming language constructs for representing assemblies of components, together with timing and resource specifications, as well as techniques for deployment of component-based designs on embedded platforms, while preserving non-functional properties. A particular problem that will be addressed is how to avoid the explosion of code size by maintaining the component structure in the generated code.
- Study concepts of interfaces and associated (partial) composition operations. These operations shold encompass interface compatibility relations where noncomposatibility means violation of simple behavioural properties, such as deadlock-freedom. This may include the synthesis of adaptors to overcome problems in compositions.
- Inverstigate the application of assume/guarantee techniques to component frameworks. This work direction is strongly related to the previous one and focusses on compositionality of non-functional properties.
- Investigate the application of abstraction techniques to component frameworks. In particular to develop techniques that allow scalable but still sufficiently precise specification and analysis of timing and resource properties of component-based systems.
- Develop techniques for generating models of components, in order to support model-based techniques for design and analysis of systems.

Industrial Liaison

- Completing the documentation from the workshop *Beyond Autosar*, and further findings by ARTIST2 partners.

- The ARTIST2 Meeting on IMA (Integrated Modular Avionics)[1] *November 12-13, 2007, Rome, Italy.* Today, the exponentially increasing diversity of airborne systems results in an ever increasing number of computers and controllers for system management, monitoring, and control. The development of specific ad-hoc solutions causes increases in costs, which in turn impacts purchase prices and operational costs. To overcome this, standardization principles and reuse of function units are now considered, via Integrated Modular Avionics. Integrated Modular Avionics (IMA) has set the principles of standardized components and interfaces of hardware and software in aircraft. These principles have been applied in particular in the development of the Airbus A380. Further developing IMA raises a number of issues that require fundamental research efforts, in tight coordination with engineering needs. ARTIST2 has decided to organize, as part of its activity on "scientific challenges in specific industrial sectors", a two-day workshop dedicated to Systems, Software, and Architecture aspects of IMA. The workshop aims to analyze: the issues and difficulties encountered by aircraft manufacturers and their suppliers, the specific research problems that result from the above issues, and, the recent advances in research that may contribute to overcoming the above difficulties. See the agenda[2]. This workshop will be a unique opportunity to gather best specialists of IMA in industry together with best academic researchers in the area of embedded systems.
  We will rather make sure that high quality minutes will be produced in the days after the meeting, for subsequent immediate exploitation – this was the method followed in some previous meetings of the cluster, with success.

1.6 Comments From Year 2 Review

1.6.1 Reviewers' Comments

This is a new activity, started at the end of Year 2, and reviewed for the first time at the end of year 3. Corresponding activities in Year 2 were accepted without comments. A general comment about the activities in the cluster was:

- *The domains of avionic, automotive, railways and energy are far to cover the domains of embedded systems. The consortium should make plans to extend its domain activities to better cover toe other system domains.*

1.6.2 How These Have Been Addressed

Activities have been extended to the area of networked mobile embedded systems (see the progress report). A seminar on *embedded systems security* was conducted in Trento, on February 22.

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

[2] http://www.artist-embedded.org/artist/Agenda,931.html

2. Summary of Activity Progress

Since this is formally a new activity, which continues efforts that have been conducted under different headings in previous years, we adapt from relevant activity descriptions of previous 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* has been further developed by Benoît Caillaud and Dumitru Potop-Butucaru (VERIMAG, then INRIA, team Aoste), who have developed a theory for the correct deployment of synchronous designs over globally asynchronous, locally synchronous (GALS) architectures. This work introduces 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 is introduced. The model covers classical implementations, where a notion of global synchronization is 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 has been 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. Work on the integration of existing validation techniques, implemented in the IF platform, is ongoing. 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 SAT checker modulo scheduling theory 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* is being developed, 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 newly started project FRESCOR: 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 Current Results

2.3.1 Technical Achievements

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. Connectors on a set of ports P are modelled as termsof the algebra AC(P), generated from P by using a binary fusion operator and a unary typing operator. Typing associates with terms (ports or connectors) synchronisation types *trigger* or *synchron*, which determine modes of synchronisation. Broadcast interactions are initiated by triggers. Rendezvous is a maximal interaction of a connector including only synchrons.

The semantics of AC(P) associates with a connector the set of its interactions. It induces on connectors an equivalence relation which is not a congruence as it is not stable for fusion. We provide a number of properties of AC(P) used to symbolically simplify and handle connectors. We provide examples illustrating applications of AC(P), including a general component model encompassing synchrony, methods for incremental model decomposition, and e-cient implementation by using symbolic techniques.

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, a research work has started this year to build a specialisation of a standard modelling language (UML) to describe heterogeneous computation and communication models founded on a mathematical basis, in the context of the Usine Logicielle project of the System@tic Paris-Région competitivity pole (www.usine-logicielle.org). This has lead to create a common research action (THeSys: Tackling Heterogeneous Systems – www.thesys.eu.org) with another team invoved in Usine Logicielle and member of the research cluster Digiteo Labs (www.digiteo-labs.org): the computer science department of SupElec (www.supelec.fr). A first report on the state of the art has been produced for Usine Logicielle and a first instantiation of a dedicated UML profile is planned for integration on Usine Logicielle platform for the end on 2007. Research reports and publications are planned for the next period. Next period work will be focussed on finalisation of the formal basis of the modelling language, implementation of a UML profile supporting it and its evaluation for modelling industrial and prototype development languages such as: Mathlab/Simulink, Oasis (Time Triggered approach for safety critical systems) and EAST ADL 2 (issued by the ATEST European project for AUTOSAR system development). This work will be partially supported by two project of the System@tic Paris-Région pole of competitivity: Usine Logicielle and EDONA (a tool integration platform for automotive embedded system development). Interactions with the NoE will be built to exchange on these first results.

Architecture for Heterogeneous Systems (TU Vienna)
The important aspects on error containment and diagnosis within heterogeneous distributed systems have been 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. The error containment and diagnostic mechanisms facilitate the establishment of a holistic system view in order to pinpoint erroneous subsystems. This aspect is of particular significance in the automotive domain where the trouble-not-identified phenomenon is a major problem.

The Periodic Finite-State Machines (PFSM) [KEHO07] expands the basic Finite State Machines (FSM) model to include the temporal properties of the physical execution environment. The timing model is based on the concept of a sparse time base in order to be able to establish a consistent view of the system state and to solve the problem of simultaneity

and consistent temporal order. PFSM facilitates the modeling and formal verification of distributed heterogeneous systems which are designed according to the time-triggered paradigm.

[OH06] presents a solution for the model-based design of virtual networks in distributed heterogeneous networks enabling faster development time and avoiding design faults. This work has been extended to an overall model-based development process of integrated computer systems based on the DECOS architecture in [HO07]. The execution platform can be described using a graphical model editor that was derived from the General Modeling Environment (GME), a tool provided by the Institute of Software Integrated Systems at Vanderbilt University.

[SOE07] attacks 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. The connection of a HIL simulator is straightforward, when the system-under-test employs a transducer network to interface its sensors and actuators. A discussion of three different transducer networks is given in [EPK07]. The work on the fixed point library implementation [ERW07] represents supplemental work that generally supports the implementation of embedded applications on small devices without hardware floating point support.

Interfaces and Composability

Several interacting lines of work are 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 has been focussing on the development of a metamodel, called **HRC (Heterogeneous Rich Components)**, which will form 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 has been defined [BCSM07], [CMM+07], [BBCP06]. The main features of HRC are:

- *Design by contract* paradigm. In addition to traditional static interfaces that only define the interaction points of components, “richer” information is exposed on the boundaries of HRC’s, in terms of contracts. Attached to a component, contracts express constraints on assumed behaviour of the environment (assumption) and expected behaviour of the component (promise). We have started to explore two lines of compositional analysis methods. One inspired by Henzinger’s theory on interface automata which has been extended for components with multiple view points. The second is inspired by classical assume/guarantee reasoning rules and adapted to the setting with rich connectors [GQ07].

- *Organization in viewpoints.* HRC contracts cover functional and non-functional aspects of a component, such as real-time, safety, resource. Following 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. Arbitrary viewpoints can be defined, but in SPEEDS, we focus on functional, real-time and safety viewpoints.

Different viewpoints need not to be orthogonal. A contract may be related to several viewpoints. As an example, the end-to-end timing latency from the brake regulator (which sends the braking command) to the brake actuator (which receives the braking command and acts) may heavily influence the guarantee of the safety property that a car will not collide with a preceding car. Here, a promise in the safety viewpoint depends on an assumption in the real-time viewpoint, which in turn should be guaranteed by a promise in the real-time viewpoint. As a consequence, expressing assumptions and promises uniformly across different viewpoints becomes highly beneficial.

- *Uniform concepts across all layers*. In analogy to the distinction between a PIM (Platform Independent Model) and a PSM (Platform Specific Model) advocated by MDA (Model Driven Architecture), 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)..

Components of all layers are uniformly represented as HRC models. More specifically, HRC's serve as the basic syntactical units of construction for all layers, and we rely on the HRC methodology to further guide and distinguish the characteristic, definition, usage, and maintenance of different layers. Layers of one system are related via mappings or connectors, which represent "allocations" of elements of the higher-layer components to those of the lower-layers. As an example, the mapping between the functional layer and the ECU layer would tell how to implement the system functionality in terms of tasks and messages deployed on ECUs and buses.

- *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. Such connectors have been inspired by synchronous languages on one hand and including the BIP connectors on the other hand. These connectors will be exploited by specific analysis techniques.

Validation and design space exploration. Different specific validation techniques for this framework are being 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 collaborate on design space exploration based on HRC. For the verification of timing properties functionalities are mapped on entities in the platform layer. 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. This is achieved by a combination of verification technology and real-time analysis techniques. Furthermore, the approach can be used for limited architecture exploration and sensitivity analysis [MH06].

The SaveComp component model (Mälardalen, Uppsala)
Another effort which aims at developing a model for component based development is *SaveCCM* (the SaveComp component model), developed by the Mälardalen and Uppsala teams [ÅCF+07]. SaveCCM can be seen as an extension of the *Rubus* component model: it is based on a control-flow (pipes-and-filters) interaction model, combined with additional support

for domain specific key functionality, e.g., feedback control, system mode changes, and static configuration. SaveCCM allows derivation of specialised formal models, which enables automated integration of analysis tools. Further the resource efficiency is of high importance in embedded systems, and SaveCCM addresses this by an efficient synthesis mechanism. 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. During Y3, the project has resulted in the tool *Uppaal PORT* which is a model checker for component based real-time systems, in paticular for SaveCCM based on the UPPAAL tool [HP07], and on a first prototype of an Integrated Development Environment.

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 have agreed in using a specialization of the Deployment and Configuration OMG standard to define an approach for the deployment of MicroCCM components. The initial design [LPDM07] has been made by Patricia López from Cantabria and allows the generation of the analysis models from the same description. This design is being refined in cooperation between Thales and Cantabria and will be implemented in the following year.

Hierarchical Coordination Language for Interacting Real-Time Tasks (EPFL, PARADES)
As another concrete technology for component based development, EPFL and PARADES have 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. HTL programs are extensible in two dimensions without changing their timing behavior: new program modules can be added, and individual program tasks can be refined. The mechanism supporting time invariance under parallel composition is that different program modules communicate at specified instances of time. Time invariance under refinement is achieved by conservative scheduling of the top level. As a case study, we implemented a distributed HTL implementation of an automotive steer-by-wire controller [GHIKS06].

Platform implementation technology for timed components (EPFL, INRIA, Verimag)
The work on a transformation chain for timed components has now been completed 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. These monitors rely on a scaled downed Giotto infrastructure. Monitors are also able to act on the global Mindstorm application behaviour. Joint work between INRIA and Verimag has led to the adaptation of some algorithms to handle time BIP components. Timing monitors tailored to supervise assemblies of BIP components are now generated automatically. 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 in previous years on developing techniques for analysis of timing and resource properties, which are more precise and more scalable than existing ones has during Y3 beed continued with ans implementation of translations between developed a translation between the real-time calculus, developed at ETHZ, and timed automata formalisms in the context of the Times tool (http://www.timestool.com). The motivation is to obtain a more

scalable analysis tool for analyzing timing properties in component-based systems, by employing the approximation and abstraction methods of the real time calculus for representing timing, communication, and resource consumption interfaces. A prototype tool (named CATS) for compositional timing and performance analysis has been developed, in which a component can be characterized by equations over timed streams. Many interesting properties such as schedulability and buffer boundedness can be checked by solving the equations. The CATS tool is available at http://www.timestool/cats, and integrated in the Eclipse platform.

A Model for Reuse and Optimization of Embedded Software Components (MdH, CC Systems)
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]

Adapter synthesis for real-time components (INRIA and L'Aquila University)
An approach for overcoming compatibility problems in composition of available components, has been developed by INRIA and L'Aquila Universit. Each component is modeled as a finite state automaton, whose transitions are labelled with input reading and output writing actions to communicate with the environment and with other components. Each such action is further enriched with timing properties specifying its duration and its latency, and can be either controllable or uncontrollable; in the first case the component has the choice to perform the action or not, while in the latter case it must execute the action whatsoever. Building an assembly of such components is bound to introduce compatibility problems, either related to timing inconsistencies or to interaction mismatches, which can cause the components in the assembly to deadlock. We have devised an automated method 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. Our 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, Dortmund)
With the goal to extend the available repertoire of techniques for generating component models, Dortmund and Uppsala are collaborating 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. They can also be used to derive (timed or untimed) models of environments of component-based system for modelling and analysis. As a concrete implementation basis, 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, in order to make automata learning scalable to realistic settings. 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 has 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. On the theoretical side, we provided for each of the three algorithms a family of components on which that algorithm outperforms the two alternatives. On the practical side, we evaluate the three algorithms 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 has 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). As documentation for the findings of the workshop *Beyond Autosar*, we are completing the "proceedings site" http://www.artist-embedded.org/artist/-ARTIST2-Workshop-Beyond-AutoSar-.html regarding this event with the additional material that the organizers still have in hand, and with contributions from ARTIST2 partners that were originally intended for a post-workshop paper, but will be more timely disseminated in this way.

Albert Benveniste (INRIA) and Paul Caspi (Verimag), in tight cooperation with John Rushby (SRI, Stanford), are organizing an ARTIST2 workshop on IMA, to be held November 12-13 in Rome. Speakers include key persons from Airbus, Dassault-Aviation, Israeli Aerospace Industries, Honeywell and Windriver, plus John Rushby and ARTIST2 participants.

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 the reporting period, OFFIS has been 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 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 has formed EICOSE, the European Institute for COmplex and Safety Critical Embedded Systems Engineering[3]. 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.

2.3.2 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 Septiember 2007.

[MAP+07] R. Marau, L. Almeida, P. Pedreiras, M. González Harbour, D.Sangorrín, and J. Medina, "Integration of a flexible network in a resource contracting framework" ; Proceedings of the 13th IEEE Real-Time and Embedded Technology and Applications Symposium WiP; Bellevue, USA, April 2007

EPFL

[BHS07] D. Beyer, T. A. Henzinger, and V. Singh. “Algorithms for interface synthesis.” Proceedings of the 19th International Conference on Computer-Aided Verification (CAV), Lecture Notes in Computer Science 4590, Springer, 2007, pp. 4-19.

INRIA

[SBD06] S. Saudrais, O. Barais and L. Duchien, "Using Model-Driven Engineering to generate QoS Monitors from a Formal Specification", EDOCW’06: 10th IEEE International Enterprise Distributed Object Computing Conference Workshops, Hong Kong, Oct. 2006.

[SPB07] S. Saudrais, N. Plouzeau and O. Barais, "Integration of time issues into component-based applications", CBSE 2007: 10th International ACM SIGSOFT Symposium on Component-Based Software Engineering, Medford, MA, July 2007.

[TFGG07] M. Tivoli, P. Fradet, A. Girault, and G. Goessler, “Adaptor synthesis for real-time components”, TACAS 2007: International Conference on Tools and Algorithms for the Construction and Analysis of Systems, Braga, Portugal, March 2007.

Mälardalen University (MdH)

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

[ÅFSC07] M. Åkerholm, J. Fröberg, K. Sandström, I. Crnkovic, "A Model for Reuse and Optimization of Embedded Software Components", 29th International Conference on Information technology Interface, (ITI 2007), IEEE, Cavtat, Croatia, June, 2007

[FÅSN07] J. Fröberg, M. Åkerholm, K. Sandström, C. Norström, "Key Factors for Achieving Project Success in Integration of Automotive Mechatronics", Journal of Innovations in Systems and Software Engineering, vol 11334 2007/3/16, p15, Springer, March, 2007

[FNNS07] J. Fredriksson, T. Nolte, M. Nolin, H. Schmidt, "Contract-Based Reusable Worst-Case Execution Time Estimate", Proceedings of the 13th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'07), Daegu, Korea, August, 2007

[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

[NHL06] T. Nolte, H. Hansson, L. Lo Bello, "Integration of networked subsystems in a resource constrained environment", Proceedings of 11th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'06), Prague, Czech Republic, September, 2006

OFFIS

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

[MH06] A. Metzner, C. Herde. "RTSat - An Optimal and Efficient Approach to the Task Allocation Problem." Proceedings of the IEEE Real-Time Systems Symposium, 2006

PARADES

[BBE+06] A. Balluchi, L. Benvenuti, S. Engell, T. Geyer, K. Johansson, F. Lamnabhi-Lagarrigue, J. Lygeros, M. Morari, G. Papafotiou, A. Sangiovanni-Vincentelli, F. Santucci, and O. Stursberg, "Hybrid Control of Networked Embedded Systems," European Journal of Control, vol. 11, no. 4-5, pp. 478-508, 2006. Special issue "Fundamental Issues in Control".

[BBFS06] A. Balluchi, L. Benvenuti, A. Ferrari, and A. Sangiovanni-Vincentelli, "Hybrid Systems in Automotive Electronics Design," International Journal of Control, vol. 79, pp. 375-394, May 2006. Special issue on "Advanced design methodologies in automotive control".

[DPS06] D. Densmore, R. Passerone and A. Sangiovanni-Vincentelli, A Platform-Based Taxonomy for ESL Design, IEEE Design and Test of Computers, vol. 23, no. 5, pp. 359-374, 2006.

[S-V07] A. Sangiovanni-Vincentelli, "Quo Vadis, SLD? Reasoning About the Trends and Challenges of System Level Design," Proceedings of the IEEE, Vol. 95:3, pp. 467-506, March 2007.

[MBFS06] L. Mangeruca, M. Baleani, A. Ferrari and A. L. Sangiovanni-Vincentelli, "Uniprocessor Scheduling Under Precedence Constraints," in Proceedings of the 12th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS'06), Washington, DC, 2006.

[GKUS07] A. Ghosal, S. Kanajan, R. Urbance and A. Sangiovanni-Vincentelli, "An Initial Study on Monetary Cost Evaluation for the Design of Automotive Electronic Architectures," Society of Automotive Engineers Congress, April, 2007.

[DZdN+07] A. Davare, Q. Zhu, M. Di Natale, C. Pinello, S. Kanajan and A. Sangiovanni-Vincentelli, "Period Optimization for Hard Real-time Distributed Automotive Systems," in Proceedings of the 44th Design Automation Conference (DAC'07), San Diego, California, June, 2007.

TU Vienna

[OKSH07] R. Obermaisser, H. Kopetz, C. El Salloum, and B. Huber, "Error containment in the time-triggered system-on-a-chip architecture"; In Proceedings of International Embedded Systems Symposium (IESS'07), Irvine, CA, USA, May 2007.

[KEHO07] H. Kopetz, C. El Salloum, B. Huber, and R. Obermaisser, "Periodic finite-state machines"; In Proceedings of 10th IEEE International Symposium on Object and Component-Oriented Real-time Distributed Computing (ISORC'07), Santorini, Greece, May 2007.

[EOHPK07] C. El Salloum, R. Obermaisser, B. Huber, H. Paulitsch, and H. Kopetz, "A time-triggered system-on-a-chip architecture with integrated support for diagnosis"; In Proceedings of Design, Automation and Test in Europe (DATE'07), Nice, France, April 2007.

[EOHKS06] C. El Salloum, R. Obermaisser, B. Huber, H. Kopetz, and N. Suri, "Supporting heterogeneous applications in the DECOS integrated architecture"; In Proceedings of International DECOS Workshop at the Mikroelektroniktagung 2006, pages 183–193, Vienna, Austria, October 2006.

[OH06] R. Obermaisser and B. Huber: "Model-based design of the communication system in an integrated architecture"; In Proceedings of International Conference on Parallel and Distributed Computing and Systems (PDCS 2006), Dallas, USA, October 2006.

[EPK07] W. Elmenreich, H. Piontek, and J. Kaiser, "Interface Design for Real-Time Smart Transducer Networks - Examining COSMIC, LIN, and TTP/A as Case Study"; In Proceedings of the International Conference on Real-Time and Network Systems (RTNS), Nancy, France; 2007

[SOE07] M. Schlager, R. Obermaisser, and W. Elmenreich, "A Framework for Hardware-in-the-Loop Testing of an Integrated Architecture" Fifth IFIP Workshop on Software Technologies for Future Embedded and Ubiquitous Systems (SEUS). Published in Springer Lecture Notes on Computer Science LNCS 4761, 2007

[HO07] B. Huber and R. Obermaisser, "Model-Based Development of Integrated Computer Systems: Modeling the Execution Platform"; In Proceedings of 5th International Workshop on Intelligent Solutions in Embedded Systems (WISES'07), Madrid, Spain, June 2007.

[ERW07] W. Elmenreich, M. Rosenblattl, and A. Wolf, "Fixed Point Library Based on ISO/IEC Standard DTR 18037 for Atmel AVR Microcontrollers"; In Proceedings of 5th International Workshop on Intelligent Solutions in Embedded Systems (WISES'07), Madrid, Spain, June 2007.

Uppsala University

[GJP06] O. Grinchtein, B. Jonsson, and P. Pettersson: Inference of Event-Recording Automata Using Timed Decision Trees. In Proc. CONCUR 2006, Bonn, Aug. 2006, LNCS 4137, pp 435-449. A revised and extended journal version is in preparation

VERIMAG

[BMPPS07] A. Basu, L. Mounier, M. Poulhiès, J. Pulou and J. Sifakis. Using BIP for Modeling and Verification of Networked Systems - A Case Study on TinyOS-based Networks, Sixth IEEE International Symposium on Network Computing and Applications (NCA 2007), 12 - 14 July 2007, Cambridge, MA, USA, pages 257-260.

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

[BS07c] Simon Bliudze and Joseph Sifakis. Causal semantics for the algebra of connectors. Technical report, Verimag, 2007. submitted for publication.

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

[GGM-CMS07] G. Gössler, S. Graf, M. Majster-Cederbaum, M. Martens, J. Sifakis An Approach to Modeling and Verification of Component Based Systems in Current Trends in Theory and Practice of Computer Science, SOFSEM'07, LNCS 4362, 2007.

2.3.3 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 Models/UML (Oct. 2006), the Embedded Systems week (Seoul, Oct. 2006), the ARTIST2 plenary meeting (Nov. 2007), the workshop on “Models of Computation and Communication” (Zurich, Nov. 2006), FMCO (Formal Methods for Components and Objects) (Amsterdam, Nov. 2006), the ARTIST Workshop on Basic Concepts in Mobile Embedded Systems (Vienna, Dec. 2006), etc.

Interaction also occurs through direct mutual visits. Harald Raffelt (Dortmund) has visited Uppsala in Sprint 2007 for the work on generating component models from observations of test traces.

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.

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 focusing on modelling frameworks and methodology and system level validation techniques. The results of the project will be integrated in commercial development platforms and academic analysis tools connected to them. SPEEDS will build upon work of previous projects, in particular WOODDES, SAFEAIR, NexTTA and OMEGA. In the SAVE project, Uppsala and Mälardalen are collaborating on component models in the Swedish National project SAVE [ÅCF+07] [HP07]. Other projects with an analogous role include OpenEmBeDD and Persiforme.

2.3.4 Joint Publications Resulting from these Achievements

[ÅCF+07] M. Åkerholm, J. Carlson, J. Fredriksson, H. Hansson, J. Håkansson , A. Möller, P. Pettersson, M. Tivoli, “The SAVE approach to component-based development of vehicular systemsJournal of Systems and Software, vol 80, nr 5, p655-667, Elsevier, May, 2007

[BBCP06] E. Badouel, A. Benveniste, B. Caillaud, and R. Passerone. Heterogeneous rich component definition, mathematical semantics. SPEEDS deliverable D2.1b/sem, annex of deliverable D2.1b, December 2006.

[BCC+06] A. Benveniste, B. Caillaud, L.P. Carloni, P. Caspi, A.L. Sangiovanni-Vincentelli and S. Tripakis, “Communication by Sampling in Time-Sensitive Distributed Systems.” in Proceedings of the Sixth International Conference on Embedded Software (EMSOFT), Seoul, Korea, October, 2006.

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

[CMM+07] Olivier Constant, Qin Ma, Lionel Morel, Mark Skipper, and Sofronis Christos. L-1 hrc meta-model, 1st version (1st round). SPEEDS Deliverable D2.1.d, August 2007.

[BJR] T. Berg, B. Jonsson, and H. Raffelt: Regular Inference for State Machines with Equality tests. In preparation

[GHIKS06] A. Ghosal, T. A. Henzinger, D. Iercan, C. M. Kirsch, and A. Sangiovanni-Vincentelli. "A hierarchical coordination language for interacting real-time tasks." Proceedings of the Sixth Annual Conference on Embedded Software (EMSOFT), ACM Press, 2006, pp. 132-141.

[HP07] J. Håkansson , A. Möller, P. Pettersson, "Partial Order Reduction for Verification of Real-Time Components." Proceedings of the 5th International Conference on Formal Modelling and Analysis of Timed Systems, LNCS 4763, p 211-226, Springer Verlag, October, 2007.

[HS06] T. A. Henzinger and J. Sifakis. "The embedded systems design challenge." Proceedings of the 14th International Symposium on Formal Methods (FM), Lecture Notes in Computer Science 4085, Springer, 2006, pp. 1-15.

2.3.5 Keynotes, Workshops, Tutorials

Workshop: SYNCHRON'06
L'Alpe d'Huez, France: November 27th – December 1st, 2006.

This workshop is devoted to all aspects of synchronous programming: languages, compiling techniques, formal methods, programming environments, execution platforms, semantics issues, code generation... This year was the occasion of recalling the career and the achievemens of Paul Caspi for his retirement in 2007.

http://www.artist-embedded.org/artist/Synchron-06.html

Workshop: ARTIST2 Workshop on Basic Concepts in Mobile Embedded Systems
Vienna, Austria: December 4-5th, 2006.

Recent advantages in mobile and wireless technology have enabled a field of mobile embedded systems in new domains like pervasive computing but also in traditional domains like automation and process control. Thus, the time has come to integrate existing knowledge in the field of real-time systems, dependable systems, modelling and component design into the paradigm of mobile embedded systems. For example, this subject requires novel models of naming and addressing of the employed devices. While in static, wire-bound system, the address and route to a particular device implicitly identifies the device's function, in the mobile computing paradigm a particular device may appear on different routes in the network and take different roles as it moves in space and therefore interact with a another part of the environment. Moreover, when considering faults, a faulty node may also infiltrate multiple clusters. This has to be considered in the fault hypothesis for mobile embedded systems. Therefore, we need to extend existing models from the domain of real-time and distributed systems for mobile embedded systems that take into account naming, addressing, security, configuration, and dependability. The objective of this workshop was to elaborate the basic concepts on mobile embedded systems based on existing approaches in distributed, real-time, and dependable systems. The workshop has also mediated basic concepts of related fields like distributed systems and real-time systems to the mobile and wireless domains.

http://www.artist-embedded.org/artist/Objectives,679.html

Workshop: FMGALS'07
MEMOCODE'07
Nice, France: – May 29th, 2007

The ever increasing clock speed coupled with the ever decreasing engraving size of synchronous circuits raise taunting clock distribution and power leakage problems. For this

reason, the Globally Asynchronous Locally Synchronous (GALS) model of computation has emerged as the paradigm of choice for SoC design with multiple timing domains, as well as for the software embedded on such circuits. Due to the inherent subtleties of asynchronous circuit design, formal methods are vital to make the GALS paradigm a success in the CAD industry. The FMGALS workshop aims at bringing together researchers from different communities interested in GALS design, and in applying formal methods in creating CAD tools enabling correct by construction GALS design.

http://www.artist-embedded.org/artist/FMGALS-2007.html

Symposium: CBSE07

The 10th International ACM SIGSOFT Symposium on Component-Based Software Engineering - Global Software Services and Architecture

Boston, July 9 - 11, 2007

The CBSE symposium has a track record of bringing together researchers and practitioners from a variety of disciplines to promote a better understanding of CBSE from a diversity of perspectives, and to engage in active discussion and debate. The symposium addresses participants from both universities and industry. The scope of the symposium includes (i) the theoretical foundations of component specification, composition, analysis and verification continue to pose research challenges. While the engineering models and methods for component software development are slowly maturing, new trends in global services and distributed systems architectures push the limits of established and tested component-based methods, tools and platforms (ii) model-driven development and grid technologies with their high-performance demands in massive data storage, computational complexity and global co-scheduling of scientific models in flagship science, technology and medicine research; (iii) global software development with its lowering of cost of software capabilities and production, through automation, off-shoring and outsourcing of key components and subsystems; (iv) networked enterprise information systems and services architectures crossing enterprise, nation, legal and discipline boundaries; (v) shift from (globally distributed) software products to pervasive and ubiquitous services supported by deep software-intensive infrastructures and middleware and by increasingly flexible, adaptive and autonomous client and application server software.

Tutorial: Evaluating Dependability Attributes of Component-Based Specifications at Internatonal Conference on Software Engineering (ICSE 2007)

Ivica Crnkovic, MDH and Lars Grunske

20 May 2007, Full Day Tutorial

Summary: Component-Based Development (CBD) and more specifically Component-based Software Engineering (CBSE) are established in many application domains. There is strong trend in applying the same approach in different domains of dependable systems, in particular safety-, mission- or business-critical systems. However, a precondition of a successful application of CBD in these domains is the existence of theories, methods and technologies to predict and evaluate dependability attributes such as safety, reliability, availability, maintainability, performance, security and temporal correctness, based on component-based specifications. The experience has shown that this is not a trivial task, since most of CBD technologies do not have built-in support for dependability. This tutorial gives an analysis of current methodologies of attribute-specific evaluation methods for dependable component-based systems; we identify limitations of the current technologies and discuss existing and possible new solutions to overcome these limitations both from a research-oriented and practical perspective. The tutorial is aimed for researchers and practitioners either working with CBD or dependability, or who are interested in getting deeper insights in these areas.

Tutorial: Emerging Technologies in Industrial Context: Component-Based and Service-Based Software Engineering at COMPSAC 2007-09-11

Ivica Crnkovic,MDH, and Honyu Pei-Breivold

27 July, 2007

Component-based software engineering (CBSE) and service-oriented software engineering (SOSE) are two similar but distinguished approaches in software engineering. In this tutorial, we compare CBSE and SOSE and analyze them from different perspectives. We discuss the possibility of combining the strengths of the two paradigms.

Tutorial : Modeling, Verification, and Synthesis of Component Interfaces
19th International Conference on Computer-Aided Verification (CAV),
Berlin, Germany- July 3-7, 2007

Invited tutorial by Tom Henzinger, EPFL

http://www.cav2007.org/

Invited Lecture : The Embedded Systems Design Challenge
12th International Workshop on Formal Methods for Industrial-Critical Systems (FMICS),
Berlin, Germany- July 2007

Invited lecture by Tom Henzinger, EPFL

http://fmics07.lcc.uma.es/

Invited Lecture : The Embedded Systems Design Challenge
14th International Symposium on Formal Methods (FM)
Hamilton, Ontario, August 2006

Invited lecture by Tom Henzinger, EPFL

http://fm06.mcmaster.ca/

Invited Lecture: Tackling Heterogeneity in Embedded (Software) Systems Development
EU-US workshop on Wireless Networked Embedded Systems
Edinburgh, July 10, 2007

Invited lecture by François Terrier, CEA LIST

http://euusworkshop07.specknet.org

Keynote Speech: Real Time Communication - What Are the Real Issues?
SNART Real-Time in Sweden Conference (RTiS)
Västerås, Sweden, August 21-22, 2007

Invited talk by Hermann Kopetz, TU Vienna

http://www.idt.mdh.se/RTiS2007/

Keynote Talk: Embedded System Development for Automotive Applications: Trends and Challenges
EMSOFT 2006
Seoul, South Korea – October 22-25, 2006

Invited talk by Werner Damm, OFFIS

http://www.emsoft.org/

Key Note Speech: Reasoning about the Trends and Challenges of Engineering Design Automation
20th International Conference on VLSI Design and 6th International Conference on Embedded System Design, Bangalore, January 6-10,2007, Bangalore, India
Invited talk by Alberto Sangiovanni-Vincentelli

Tutorial: Clock Synchronization and Determinism, Fault Tolerance, and System Design ARTES Summer School
Västerås, Sweden, August 20-24, 2007
Invited tutorial by Hermann Kopetz, TU Vienna
http://www.artes.uu.se/events/summer07/

3. Future Work and Evolution

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

Design of Heterogeneous Systems

Design of a time-triggered Network on Chip An important aspect in the future will be the possibility to build networked systems on a single chip. Therefore, future work in this area will include the design of an efficient Network-on-a-chip (NoC) architecture that interconnects heterogeneous cores with different criticality and diverse requirements with respect to the communication infrastructure. A central ingredient in this architecture will be the design of a time-triggered Network on Chip (TT NoC) for the predictable interconnection of heterogeneous components. Its design will be lead by the TU Vienna team, based on its strong background on communication architectures. The TT NoC will offer inherent fault isolation to support the seamless integration of independently developed components, possibly with different criticality levels. A pivotal property of the architecture will be the integrated error containment, which facilitates modular certification, robustness, and composability. By dividing the complete SoC into physically separated components that interact exclusively by the timely exchange of messages on a TT NoC, we can achieve error containment for both computational and communication resources. The time-triggered design allows protecting the access to the NoC with guardians that are associated with each component. Based on the protection of the time-triggered NoC with inherent predictability and determinism, the architecture also enables error containment for faulty computational results. These value message failures can be masked using active redundancy (e.g., off-chip and on-chip Triple Modular Redundancy (TMR)) or detected using diagnostic assertions on messages. The design of the error containment mechanisms will systematically follow a categorization of significant fault classes that an SoC is subject to (e.g., physical/design, transient/permanent). Furthermore, mechanisms for integrated resource management will support dynamically changing resource requirements (e.g., different operational modes of an application), fault-tolerance, and a power-aware system behavior.

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. Superficial classifications may distinguish between hardware and software components, or between continuous-time (analog) and discrete-time (digital) components, but heterogeneity has two more fundamental sources: the composition of subsystems with different execution and interaction semantics; and the abstract view of a system from different perspectives. During Y4, cluster partners, including EPFL, ETHZ, INRIA, Uppsala, Verimag, will meet informally, in workshops, and in the scope of projects such as the newly started COMBEST to address the problem of developing concepts and theories that support unification and integration of frameworks encompassing heterogeneity.

UML profile for modeling heterogeneous systems. An important challenge is to integrate in standard formalisms the means to describe formally semantics of heterogeneous systems. As being more and more used and adapted to embedded domain UML is of particular interest due to its build in possibilities of extension. Work on developing a UML profile mapped to mathematical fundations to describe model of computation and communications will be continued during this year, lead by the CEA team, in order to be able to formalise semantic of UML models of heterogeneous component architectures.

Interfaces and Composability

Correctness-by-construction: Verimag will continue the work on compositional deadlock detection/verification and its implementation in the DeadlockFinder tool. Verimag will combine structural analysis for connectors with structural analysis for priorities. The latter will be based on the composion of the priority orders applied in BIP models. The composition consists in computing the transitive closure of the union of the priority orders. If the resulting relation is a priority order, then global deadlock-freedom is preserved.

We will enhance and extend the existing structural analysis techniques in several directions: We will find sufficient conditions for individual deadlock-freedom of components or clusters of components. These techniques will be applied to other classes of properties such as liveness. Finally, we will use the system construction space *Behavior* × *Interaction* × *Priority* to study property preserving transformations. We will study in particular, transformations preserving deadlock-freedom of an untimed system when it is transformed into a timed one by adding timing constraints.

Heterogeneous Rich Components The partners INRIA, OFFIS, PARADES, and VERIMAG will continue their work on the *Rich Component Model* paradigm. After the establishment of the metamodel, work will continue to make the metamodel more concrete, by instantiating it to different viewpoints, and to develop verification frameworks and tool support.

Implementation of LightWeigth CCM components Within the *FRESCOR* project, University of Cantabria and Thales will implement the approach for deploying MicroCCM components, that was developed during Y3. Within the SAVE project, driven by the Mälardalen Team, one objective during the next year is to develop an automotive demonstrator illustrating the component-based development technology developed within the SAVE project. This will include an integrated tool environment, a concrete target system, and an application used for evaluation and demonstration purposes.

Extending specifications with reliability requirements EPFL and PARADES will collaborate on extend9ng HTL (the Hierarchical Timing Language generalizing Giotto) with reliability requirements. A reliability requirement specifies what percentage, in the long run, of periodic values of a variable (e.g., actuator) needs to be valid. The compiler matches such reliability requirements against the failure rates of the hosts and links in the underlying platform. To meet the reliability requirements, the compiler may have to replicate certain tasks on multiple hosts. This work extends the separation of specification from implementation beyond timing, to reliability.

Scalable Specification and analysis of timing properties During Y4, the collaboration between ETHZ, Uppsala, and other partners, on developing techniques for scalabel analysis of timing and resource properties, will continue 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 will also investigate 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.

Algorithms for Interface Synthesis During Y4, a main goal of the collaboration between Uppsala and Dortmund on synthesis of interface specifications will be to evaluate the developed techniques on the generation of model of several realistic communication protocols, using test data and experimentation.

Industrial Liaison

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.

A meeting on predictability of hardware in automotive/avionics and semiconductor industry will be organized during 2008.

3.2 Current and Future Milestones

- Year 3:
  - Unification of models of computation and comparison beween frameworks using denotational and operational semantics*. We made some progress in that direction although the results are not yet visible. There is a possibility for 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 will be 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 seems possible between synchronous reactive semantics and asynchronous semantics by relating causal semantics for connectors in BIP [BS07c] and partial order semantics for clocks in Signal.
  - Verification framework for rich heterogeneous interfaces. We will develop contract-based compositional verification methods as well as methods based on structural analysis.
  - UML profile to describe computation and communication models developed with the support of the research group THeSys (www.thesys.eu.org) among CEA, Supélec and Ecole Centrale de Paris of Didgiteo Labs cluster (www.digiteo-labs.org).
  - 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.

3.3 Indicators for Integration

This activity is expected to play a strong role in integration, as the important events typically involve different topics covered by Artist2 clusters, and thus require the involvement of several clusters. Hence an obvious indicator for integration with regard to this activity is the list of Artist2 clusters as well as non core members of Artist2 or external partners who will be involved in the preparation and contents of the main events. The same applies to the post-event exploitation, if any.

Setting up the COMBEST project is a strong sign of integration between partners of this cluster (Verimag, INRIA, OFFIS, PARADES) but also with the Execution Platforms Cluster (ETHZ and Braunschweig). The project focuses on all fundamental aspects of component-based design. Its capitalizes on common achievements of the teams of this cluster and synergy with other teams.

3.4 Main Funding

Main sources of funding include:

- the Integrated Projects
  - DECOS https://www.decos.at/
  - ASSERT http://www.assert-online.net/
  - MODELWARE
  - RUNES, http://www.control.lth.se/research/runes.html
  - SPEEDS
- the STREPS
  - DYSCAS - www.dyscas.org
  - ATESST - www.atesst.org
  - OMEGA
  - Q-ImPrESS - Quality Impact Prediction for Evolving Service-Oriented Software
  - COMBEST
  - FRESCOR
- 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 (www.usine-logicielle.org).
- EDONA (to be started beginning of October), System@tic Paris-Région pole of competitivity (www.usine-logicielle.org).

- Industry
  - Cadence
  - Pirelli
  - ST Microelectronics
  - United Technology Corporation (Otis, Carrier, Chubb)

4. Internal Reviewers for this Deliverable

Albert Benveniste, INRIA (internal)

Michael Gonzalez-Harbour (external)