



IST-214373 ArtistDesign
Network of Excellence
on Design for Embedded Systems

Cluster - Progress Report for Year 1

Cluster:
Modeling and Validation

Cluster Leader:

Professor Kim G. Larsen (CISS, Aalborg University)

<http://www.cs.aau.dk/~kgl>

Policy Objective (abstract)

The sheer complexity of future embedded devices seriously challenges current development practice; new, integrated and scalable methods are urgently needed. The use of *modeldriven* and *component-based* approaches are seen as a way of obtaining dependable embedded implementations with high performance and with reduced time and cost. Embedded systems involve monitoring and control of complex physical objects or phenomena using a number of dedicated hardware and software components often within a networked solution.

Therefore, an objective of the cluster is to advance the utilization of *models*, *analysis techniques* and *supporting tools* spanning the areas of control theory, computer science, hardware, networks and even mechatronic all well established research areas which however – by and large – have been developed independently.

Versions

| number | comment | date |
|--------|---|--------------------------------|
| 1.0 | First version delivered to the reviewers erroneous version | December 19 th 2008 |
| 1.1 | Second (correct) version delivered | January 20 th 2009 |

Table of Contents

| | |
|--|----|
| 1. Overview | 3 |
| 1.1 High-Level Objectives..... | 3 |
| 1.2 Industrial Sectors..... | 3 |
| 1.3 Main Research Trends | 4 |
| 2. State of the Integration in Europe | 5 |
| 2.1 Brief State of the Art | 5 |
| 2.2 Main Aims for Integration and Building Excellence through ArtistDesign | 5 |
| 2.3 Other Research Teams | 6 |
| 2.4 Interaction of the Cluster with Other Communities | 6 |
| 3. Overall Assessment and Vision for the Cluster | 7 |
| 3.1 Assessment for Year 1 | 7 |
| 3.2 Overall Assesment since the start of the ArtistDesign NoE..... | 7 |
| 3.3 Indicators for Integration..... | 8 |
| 3.4 Long-Term Vision | 8 |
| 4. Work Related to the Joint Programme of Integration Activities (JPIA)..... | 9 |
| 4.1 Joint Technical Meetings | 9 |
| 4.2 Staff Mobility and Exchanges | 12 |
| 4.3 Tools and Platforms..... | 14 |
| 5. Cluster Participants | 17 |
| 5.1 Core Partners | 17 |
| 5.2 Affiliated Partners | 21 |
| 6. Internal Reviewers for this Deliverable..... | 24 |

1. Overview

In this section we give an overview of the current situation for the cluster's research area in terms of overall objectives and trends.

1.1 High-Level Objectives

The sheer complexity of future embedded devices seriously challenges current development practice; new, integrated and scalable methods are urgently needed. The use of *model-driven* and *component-based* approaches are seen as a way of obtaining dependable embedded implementations with high performance and with reduced time and cost. Embedded systems involve monitoring and control of complex physical objects or phenomena using a number of dedicated hardware and software components often within a networked solution. Therefore, the use of models, analysis techniques and supporting tools span the areas of control theory, computer science, hardware, networks and even mechatronic all well established research areas which however – by and large – have been developed independently. This has the unfortunate consequence that it often becomes impossible to state, not to mention validate, overall properties of an embedded system.

Overall objectives of the cluster are:

1. Establish a coherent family of modelling formalisms spanning the areas of computer science, control, hardware and networks covering all aspects of embedded systems.
2. Development and combination of efficient means for analysis of models including simulation, testing, static analysis, model-checking, run-time verification, monitoring, diagnosability, controller synthesis.
3. Emphasis on support for compositional methodologies in terms of allowing new complex systems to be assembled from already constructed and validated components.
4. Realization of coherent tool chain obtained by adjusting and combining the models and tools from the different research areas. This will provide the basis for a cost-efficiency development process allowing for early design-space exploration and verification as well as reduce the sizeable amount of final testing-time and –cost.
5. Interaction with the thematic activities in the Transversal Integration workpackage on validating the formalisms and tools through real industrial development projects and case studies.

1.2 Industrial Sectors

The modeling and validation techniques and supporting tools developed and disseminated within the cluster have relevance and potential impact on literally *all* industrial sectors developing or using embedded systems solutions. Within the Strategic Research Agenda of the ARTEMIS research platform¹ *Design Methods and Tools* is one of the three research priorities put forward. Here model- and component-based approaches are proposed as necessary for coping with the growing complexity of systems while meeting “time-to-market” requirements. Methods and tools for testing and verification are to play a central role in the ARTEMIS research strategy, as can be seen from the following citations:

¹ <http://www.artemis-office.org/>

- “.. methods and tools for simulation, automatic validation and proving, and virtual Verification and Validation (V&V). Methods and tools for developing product lines of embedded systems.”
- “.. reduce the cost of the system design by 50%. Matured product family technologies will enable a much higher degree of strategic reuse of all artifacts, while component technology will permit predictable assembly of Embedded Systems.”
- “.. achieve 50% reduction in development cycles. Design excellence will aim to reach a goal of “right first time, every time” by 2016, including Validation, Verification and certification (to the same and higher standards as today).”
- “..manage a complexity increase of 100% with 20% effort reduction. The capability to manage uncertainty in the design process and to maintain independent hardware and software upgradeability all along the life cycle will be crucial.”
- “.. reduce by 50% the effort and time required for re-validation and recertification after change, so that they are linearly related to the changes in functionality.”

The industrial needs for improved tools and methods for system validation have also been witnessed by a number of industrial and industry inspired case-studies and projects using model-based testing and verification carried out by the individual partners. Detailed information of these (and others) is to be found in the ARTIST2 Open Repository for Test and Verification Case Studies (<https://bugsy.grid.aau.dk/artist2>). Based on the above case-studies, it seems that the actual financial benefits of using a model-driven approach are likely to be even greater than those of the ARTEMIS goals, due to the capabilities of capturing functional as well as non-functional problems early on in the development process.

1.3 Main Research Trends

With respect to modeling and validation of embedded systems the overall trends include the need for dealing with increasingly complex systems with an increasing number of (functional and non-functional) features.

The need for a scientific foundation for embedded systems dealing simultaneously with software, hardware resources and physical environments have received substantial attention during the last year with significant contributions from the partners of the ARTIST Design Modeling and Validation Cluster. Emphasis is on quantitative modeling as well as component-based design methodology with the ambition of establishing a coherent family of design flows spanning computer science, control and hardware.

The quantitative and component-based modeling formalism are accompanied with advances in analysis techniques allowing for early exploration and assessment of alternative design solutions as well as validation of final implementations. Efforts in combining techniques ranging from simulation, testing, model-checking, run-time verification, artificial intelligence, compositionality, refinement as well as abstract interpretation are currently pursued.

Also, a number of newly started STREP, IP and ARTEMIS projects are actively pursuing the accessibility of state-of-the-art research results on quantitative modeling and validation from industrial tool-chains.

2. State of the Integration in Europe

The objective of the Modeling and Validation cluster is to combine the efforts and skills of the individual leading researchers and research groups in Europe into a world-class virtual team, for advancing the state-of-the-art. The partners span the leading research teams in European level and are well connected with leading research teams outside Europe.

2.1 *Brief State of the Art*

An important class of industrially applied model-based methodologies is those based on a synchronous execution model (e.g. Lustre, Esterel, and Signal). Other model-based approaches are built around a class of popular languages exemplified by Matlab Simulink. Originating from the design automation community, SystemC also chooses synchronous hardware semantics, but allows for the introduction of asynchronous execution and interaction mechanisms from software (C++). More recent modeling languages, such as UML and AADL, attempt to be more generic in their choice of semantics and thus bring extensions in two directions: independence from a particular programming language; and emphasis on system architecture as a means to organize computation, communication, and constraints.

Design often involves the use of multiple models that represent different views of a system at different levels of granularity. Some transformations between models can be automated; at other times, the designer must guide the model construction. While the compilation and code generation for functional requirements is often routine, for non-functional requirements, such as timing, the separation of human-guided design decisions from automatic model transformations is not well understood

By far the most common validation technique applied in embedded industrial today is based on rather ad-hoc and manual (hence quite error-prone) testing. Given that some 30-50% of the overall development time and cost are related to testing activities it is clear that the impact of improved validation technologies is substantial.

Whereas validation techniques for assessing functional correctness have reached a certain level of maturity and industrial acceptance, there is a need for mature validation techniques addressing quantitative being accessible from within industrial tool-chains.

2.2 *Main Aims for Integration and Building Excellence through ArtistDesign*

The integration of the research groups within the cluster is well established and with significant impact on the larger research community on modeling and validation through strong impact on a number of important international conferences within the area. Also, partners of the cluster – often in collaboration with other clusters – have made significant effort in spreading of excellence beyond the ARTIST2 NoE through PhD schools and industrial seminars. More systematic knowledge transfer to industry through long-term collaboration on industrial development projects has been performed by individual partners. Here the national centers ESI (Embedded Systems Institute, Eindhoven, The Netherlands) and CISS (Center for Embedded Software Systems, Aalborg, Denmark) have specific resources reserved for such activities.

Also at the national level of the various partners in the Testing and Verification cluster involvement in ARTEMIS are planned with the ambition of having an impact on the long-term take-up of testing and verification technology in industrial practice.

2.3 Other Research Teams

During the first year the number of affiliated partners contributing actively to the cluster has been growing significantly as can be seen from the detailed activity reports on Modeling (D5-(3.1)-Y1) and Validation (D6-(3.2)-Y1) in comparison with the original DoW.

Other prominent research groups not being partner of the cluster include a number of teams from United Kingdom, in particular School of Computer Science, Birmingham (probabilistic model checking), Oxford University Computing Laboratory (real-time verification), Microsoft Research Laboratory at Cambridge and Royal Holloway, University of London. From Italy important contributions come from the Automated Verification and Synthesis Group, Trento University (symbolic model-checking, SAT-solving, applications to planning) with support of the nuSMV tool. In all of the above cases individual partners of the cluster are collaborating with the particular research group.

The partners of the cluster are collaborating extensively with leading research teams outside Europe both on the level of concrete research problems and topics and in terms of organising the testing and verification research community. The cluster has strong links to the work on software verification and testing taking place at Microsoft Research, Redmond, (Ball), NASA Ames and Kestrel Technologies (Holzman, Visser and Havelund) and Kansas (Hatcliff). Extraordinary strong links exist to Cadence (Sangiovanni Vincentelli, director of Cadence and core-partner of ARTIST Design), Rice University, Texas (Vardi, longstanding collaboration with Wolper on the highly appreciated and influential automata theoretic approach). Also ARTIST Design has collaborated with leading research groups and researchers from Israel including Weizmann Institute (Pnueli, Harel), Haifa (Grumberg) and Hebrew University (Kupfermann).

2.4 Interaction of the Cluster with Other Communities

During the first year the methods of the cluster has been successfully applied to the automatic generation of test suites (with guaranteed coverage), and is also increasingly applied successfully within and by other communities including hardware/software co-design, control theory, discrete event systems, fault-tolerance, planning and scheduling and performance evaluation.

Members of the cluster has published and given invited talks at main conferences and in journals of these neighbouring communities.

Similarly leading research groups within AI are finding applications of existing search heuristics from planning to the improved model-checking (e.g. Freiburg University, Germany within the AVACS project and Trento University, Italy).

At the *organization* level, members of the cluster have been active in the European ARTEMIS initiative, and are involved in several of the to-be-funded projects from the first ARTEMIS call.

3. Overall Assessment and Vision for the Cluster

3.1 Assessment for Year 1

Both research activities with the cluster – the *Modeling Activity* and the *Validation Activity* – have progressed substantially within the first year, and with significant synergy between modeling formalisms proposed and enabled validation techniques:

With the sub-activities on *Component Modeling* and *Compositional Validation* substantial efforts have been made towards frameworks for modelling composite systems with heterogeneous systems permitting a variety of non-functional aspects. The work includes generic frameworks allowing for contract-based circular reasoning as well as industrial application of component-based methods allowing for compositional safety, robustness and failure analysis. Also, in several cases the work has been motivated and validated by industrial needs.

Within the sub-activity *Resource Modeling* (of the *Modeling Activity*) – studied the design of resource-constrained systems, where resource can be quantitative (e.g energy) or not (e.g. shared memory access) and with a number of applications considered. Within the sub-activity *Quantitative Modeling* (of the *Modeling Activity*) focus has been on design frameworks for quantitative modeling, mainly timing and resources.

Within the sub-activity *Quantitative Validation* (of the *Validation Activity*) an array of validation techniques dealing with timing, hybrid behaviour, stochastic aspects as well as resource including energy and memory consumption have been put forward. Still, techniques for simultaneous analysis of multiple quantitative aspects are less developed.

Within the sub-activity *Cross-layer Validation* (of the *Validation Activity*) progress on testing real-time and data-intensive systems have been made. Also substantial effort has been made by several partners on controller synthesis of controllers taking partial observability, quantitative aspects (time and probabilities) as well as resource constraints into account. Predictable realisation of synthesized strategies on specific platforms is still to be dealt with.

3.2 Overall Assessment since the start of the ArtistDesign NoE

During the period of ARTIST Design the partners of the Modeling and Validation cluster have demonstrated true research excellence as witnessed by the extensive list of publications at leading conferences and journals, numerous invited keynote presentations by members of the cluster as well as the co-hosting of several PhD schools and workshops.

The industrial impact of the cluster has been significant during the period, witnessed by a large number of dissemination activities carried out by the partners. In particular, in several collaborative projects with companies the adaptation of model-driven development has resulted in notable reduced time-to-market.

Within the first year of ARTIST Design the partners have continued their involvement in building the European Embedded Systems community as clearly demonstrated by the high number of joint projects (FP7, ESF as well as national) that have been initiated by members of the cluster.

3.3 **Indicators for Integration**

Interactions planned between partners include:

- Tool Connection
 - Connections to SPEEDS;
The HRC component format has been stabilised enabling exploitation in the next years.
 - UPPAAL & RAPTURE & MODEST;
Partially obtained with the introduction of a branch of UPPAAL supporting Probabilistic Timed Automata. The goal is extended to link to the probabilistic model checkers MRMC and PRISS
 - Metropolis and HDL (Giotto);
Partially obtained.
 - UPPAAL & IF;
Not pursued during the first year.
 - ARTS & UPPAAL (from simulation to verification);
Has been achieved allowing for simulation as well as verification of schedulability properties of MPSoC to be made. Future effort includes simulation and verification of performance properties (energy and memory consumption).
 - TrueTime.
Has not been achieved during the first year.
- 10 Joint publications between partners/year
 - *Achieved*
- 2 open workshops / year
 - *Achieved*
- Connections between tools of partners; joint meetings.
 - *Achieved*

3.4 **Long-Term Vision**

The long-term vision of the cluster is to enable future development of embedded devices to cope with the growing complexity.

In particular, the cluster wants to develop model-driven and component approaches based on rigorous modeling formalisms and supporting validation techniques spanning allowing all relevant aspects of embedded systems (hardware, software and physical environment) to be taken into account. Here, a special challenge is to overcome the current weakness of model-driven development methodologies in dealing with physical constraints and quantitative aspects.

This calls for development of efficient means for analysing and validating such designs, as well as realization of coherent tool chains integrating academic efficient tool components into existing industrial tool chains.

4. Work Related to the Joint Programme of Integration Activities (JPIA)

4.1 Joint Technical Meetings

Organization of the workshop, Veronique Bruyere and Jean-Francois Raskin. "Automata and Verification", University of Mons-Hainaut, Belgium, August 25-26, 2008.

Summer school: Movep 08: Co-organization of the Movep school (<http://www.univ-orleans.fr/movep2008/>) about modeling and verifying parallel processes in June 2008, partially funded by Artist 2.

RTSS08 track on Design and Verification of Embedded Real-Time Systems, the 29th IEEE Real-Time Systems Symposium. Barcelona, Spain. November 30 - December 3, 2008. This is one of the four tracks of RTSS 2008.

The objective is to promote research on design and analysis, and verification of embedded real-time systems. It intends to cover the whole spectrum from theoretical results to concrete applications with an emphasis on practical and scalable techniques and tools providing the designers with automated support for obtaining high-quality software and hardware systems. A particular goal is to provide a forum for interaction between different research communities, such as scheduling, hardware/software co-design, and formal techniques. <http://www.rtss.org>

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.

The need for certification, like for instance in the rail sector, imposes the burden of not only validating a system, but also proving in a juridical sense, that the validation can be trusted. The major question addressed in the workshop was how to embed formal methods and tools in a seamless design process which covers several development phases and which includes an efficient construction of a safety case for the product. <http://safecert08.offis.de/>

Workshop FIT 2008: Foudnation of Interface Theories ETAPS 2008 Budapest, Hungary, 29 March, 2008, organized by CISS, Aalborg University and ITU, Copenhagen. Invited presentations from INRIA, Rennes, and Twente U.

Component-based design is widely considered as a major approach to developing systems in a time and cost effective way. Central in this approach is the notion of an interface. Interfaces summarize the externally visible properties of a component and are seen as a key to achieving component interoperability and to predict global system behavior based on the component behavior. To capture the intricacy of complex software products, rich interfaces have been proposed. These interfaces do not only specify syntactic properties, such as the signatures of methods and operations, but also take into account behavioral and extra-functional properties, such as quality of service, security and dependability. Rich interfaces have been proposed for describing, e.g., the legal sequences of messages or method calls accepted by components, or the resource and timing constraints in embedded software. The development of a rigorous framework for the specification and analysis of rich interfaces is challenging. The aim of this

workshop is to bring together researchers who are interested in the formal underpinnings of interface technologies.

Workshop: 1st International Workshop on Model Based Architecting and Construction of Embedded Systems

Toulouse -- September 29th, 2008

This ARTIST workshop is held in conjunction with MODELS 2008 as a follow-up workshop of the SVERTS and MARTE workshops organised in previous years, the objective of this workshop is to bring together researchers and practitioners interested in model-based software engineering for real-time embedded systems. We are seeking contributions relating to this subject at different levels, from modelling languages and semantics to concrete application experiments, from model analysis techniques to model-based implementation and deployment. Given the criticality of the application domain, we particularly focus on model-based approaches yielding efficient and provably correct designs. Concerning models and languages, we welcome contributions presenting novel modelling approaches as well as contributions evaluating existing ones. The organisers of this workshop are partners from the ASSERT and SPICES project; the ARTIST partners are CEA and Verimag.

<http://www.artist-embedded.org/artist/ACES-MB-08.html>

Workshop 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 : ACESMB 2008, 1st Int. Workshop on Model Based Architecting and Construction of Embedded Systems

ACM/IEEE 11th Int. Conf. on Model Driven Engineering Languages and Systems

Toulouse, France - September 29th, 2008

New real-time systems have increasingly complex architectures because of the intricacy of the multiple interdependent features they have to manage. They must meet new requirements of reusability, interoperability, flexibility and portability. These new dimensions favour the use of an architecture description language that offers a global vision of the system, and which is particularly suitable for handling real-time characteristics. Due to the even more increased complexity of distributed, real-time and embedded systems (DRE), the need for a model-driven approach is more obvious in this domain than in monolithic RT systems. The purpose of this

workshop is to provide an opportunity to gather researchers and industrial practitioners to survey existing efforts related to behaviour modelling and model-based analysis of DRE systems. This workshop sought contribution from researchers and practitioners interested in all aspects of the representation, analysis, and implementation of DRE system behaviour and/or architecture models.

<http://www.artist-embedded.org/artist/ACES-MB-08.html>

Workshop : UML & AADL 2008

13th IEEE International Conference on Engineering of Complex Computer Systems

Belfast, Northern Ireland - April 2nd, 2008

New real-time systems have increasingly complex architectures because of the intricacy of the multiple interdependent features they have to manage. They must meet new requirements of reusability, interoperability, flexibility and portability. These new dimensions favour the use of an architecture description language that offers a global vision of the system, and which is particularly suitable for handling real-time characteristics. Due to the even more increased complexity of distributed, real-time and embedded systems (DRE), the need for a model-driven approach is more obvious in this domain than in monolithic RT systems. The purpose of this workshop is to provide an opportunity to gather researchers and industrial practitioners to survey existing efforts related to behaviour modelling and model-based analysis of DRE systems. This workshop sought contribution from researchers and practitioners interested in all aspects of the representation, analysis, and implementation of DRE system behaviour and/or architecture models.

http://www.artist-embedded.org/artist/Topics_1199.html

4.2 Staff Mobility and Exchanges

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.

Dr. Pierre America participated and provided a presentation during the ArtistDesign workshop Intercluster activity: Integration Driven by Industrial Applications. Title of his presentation was Embedded Systems in Healthcare.

Dr. Ir. Twan Basten participated in the ArtistDesign WFCD 2008 workshop, held on 19th of October during the Embedded Systems Week.

Dr. Michael Borth participated and provided a presentation during the ArtistDesign Workshop Intercluster activity: Integration Driven by Industrial Applications, 13-14 November, Rome. His presentation was titled: Future Car Platform Development.

Kim Larsen was awarded Doctor Honoris Causa at ENS Cachan acknowledging his regular collaboration with LSV. Kim Larsen also spent a month as an invited professor at LSV.

From Aalborg to CFV (Brussels): one week visit of Prof. Kim Larsen to the team of Prof. JF Raskin.

From ENS Cachan to Aalborg: one week visit of Patricia Bouyer and Nicolas Markey.

From Aalborg to ENS Cachan: one week visit of Ulrich Fahrenberg.

Ghassan Oreiby will after his position as PhD student at LSV go to Aalborg University for a post doc position starting November 1, 2008.

EPFL + CFV collaborated on efficient algorithms for classical decision problems in automata theory (emptiness, language inclusion, universality), with application to the model-checking of linear time properties.

EPFL + LSV collaborated on games with imperfect information. We work on building a tool to solve such games, with parity objectives.

From INRIA to LSV and CVF (Mons): one week visit of Nathalie Bertrand in each place on probabilistic semantics for timed automata.

From CFV (Brussels) to Inria Rennes: two month visit of Gabriel Kalyon and one month visit of Thierry Massart.

From INRIA to CFV (Brussels) one week visit of T. Legall to ULB followed by post-doc started in September 2008.

From ESI to Inria Rennes: one week visit of Jan Tretmans to Inria for participation to the summer school EJCP.

Uppsala has collaborated with ETH in Zurich on modular performance analysis. Jointly, we have established a fixed point theorem on the existence of fixed points for component networks containing feedback cycles. Uppsala has also initiated collaboration with North Eastern University in China, on multiprocessor scheduling.

The SPEEDS project lead to an important collaboration between INRIA, OFFIS, PARADES and VERIMAG on the definition of the SPEEDS metamodel HRC [BCSM07] which is the basis of an important analysis platform (platform 1). This collaboration continues for the definition of a verification methodology. From the collaboration in SPEEDS has started a broader collaboration on a general framework for the semantics of communication in distributed

systems with INRIA, PARADES and VERIMAG with external collaboration of University of Columbia and Cadence Design Systems [BCC+].

In the Combest project several joint activities are being carried out. In particular, Verimag and ETHZ collaborate on the combination of analytical performance analysis via performance analysis of a corresponding more precise operational model in order to obtain more precise results.

Interaction between RWTH and Saarland University on design notations and model checking
interaction between CISS and RWTH on quantitative versions of priced timed automata

From Aalborg to CFV (Brussels): one week visit of Prof. Kim Larsen to the team of Prof. JF Raskin.

From CFV (Brussels) to EPFL (Henzinger): Dr. Laurent Doyen formerly in CFV is post-doct at EPFL.

From CFV (Brussels) to EPFL (Henzinger): several visits during 2007-2008 by Prof. JF Raskin.

From EPFL (Henzinger) to CFV (Brussels): several visits during 2007-2008 by Dr. L Doyen.

4.3 Tools and Platforms

Here we list some of the stable, downloadable tools and platforms of the cluster. The cluster are working on several other tools and platforms. For more and detailed information we refer to the reports of the activities *Modeling* and *Validation*.

- **AMT**

- AMT (Analog Monitoring Tool) is a tool for checking the correctness of analog and mixed-signal simulation traces with respect to a formal specification expressed as an assertion. The specification language supported by the tool is STL/PSL, an extension of the temporal logic inspired by the PSL language, which allows to express properties of real-valued continuous-time behaviors.
<http://www-verimag.imag.fr/~nickovic/index.php?id=nickovic&page=amt>

- **IF TOOLBOX**

- IF is a language for the structured representation of concurrent real-time systems and a set of tools allowing the analysis and verification of requirements on such systems. The tool evolved from the CADP toolset. Its development was motivated by the need for a structured representation of systems, allowing the application of simplifications for avoiding state explosion before its translation into a global (symbolic) transition relation. In particular, IF has frontends allowing the verification and analysis of models of real-time systems represented in SDL and UML.
<http://www-if.imag.fr/>

- **MARTE**

- MARTE consists in defining foundations for model-based description of real time and embedded systems. These core concepts are then refined for both modeling and analyzing concerns. Modeling parts provides support required from specification to detailed design of real-time and embedded characteristics of systems. MARTE concerns also model-based analysis. In this sense, the intent is not to define new techniques for analyzing real-time and embedded systems, but to support them. Hence, it provides facilities to annotate models with information required to perform specific analysis. Especially, MARTE focuses on performance and schedulability analysis. But, it defines also a general framework for quantitative analysis which intends to refine/specialize any other kind of analysis.
<http://www.omgmarte.org/>

- **METROPOLIS**

- Establishing formal design methodologies is imperative to effectively manage complex design tasks required in modern-date system designs. It involves defining levels of abstraction to formally represent systems being designed, as well as formulating problems to be addressed at and across the abstraction levels. This calls for a design environment in which systems can be unambiguously represented throughout the abstraction levels, the design problems can be mathematically formulated, and tools can be incorporated to solve some of the problems automatically. Developing such an environment is precisely the goal of Metropolis.

Metropolis consists of an infrastructure, a tool set, and design methodologies for various application domains. The infrastructure provides a mechanism such that heterogeneous components of a system can be represented uniformly and tools for formal methods can be applied naturally.

<http://embedded.eecs.berkeley.edu/metropolis/index.html>

- **PHAVER**

- PHAVer is a tool for verifying safety properties of hybrid systems. It stands out from other tools with the following features:
 - exact and robust arithmetic with unlimited precision,
 - on-the-fly over-approximation of piecewise affine dynamics
 - improved algorithms and termination heuristics
 - support for compositional and assume-guarantee reasoning.

- http://www-verimag.imag.fr/~frehse/phaver_web/index.html

- **UPPAAL**

- Uppaal is an integrated tool environment for modeling, validation and verification of real-time systems modeled as networks of timed automata, extended with data types (bounded integers, arrays, etc.).

The tool is developed in collaboration between the Department of Information Technology at Uppsala University, Sweden and the Department of Computer Science at Aalborg University in Denmark.

www.uppaal.com

- **UPPAAL TIGA**

- UPPAAL TIGA (Fig. 1) is an extension of [UPPAAL \[BDL04\]](#) and it implements the first efficient on-the-fly algorithm for solving games based on timed game automata with respect to reachability and safety properties. Though timed games for long have been known to be decidable there has until now been a lack of efficient and truly on-the-fly algorithms for their analysis.

<http://www.cs.aau.dk/~adavid/tiga/>

- **UPPAAL TRON**

- Uppaal TRON is a testing tool, based on Uppaal engine, suited for black-box conformance testing of timed systems, mainly targeted for embedded software commonly found in various controllers. By online we mean that tests are derived, executed and checked simultaneously while maintaining the connection to the system in real-time.

<http://www.cs.aau.dk/~marius/tron/>

- **SARTS**

- SARTS is a model based schedulability analysis tool used for hard real-time systems. SARTS is used to translate hard real-time systems, implemented in Java, to a finite state machine in the modeling tool Uppaal.

The system being analyzed must be implemented in SCJ2, a safety critical profile for Java developed in this project, based on SCJ. The target hardware is the time predictable Java processor JOP, developed specifically for hard real-time systems.

Several experiments have been conducted to illustrate the accuracy of SARTS compared to existing tools. It is shown how the model based approach can result in a more accurate analysis, than possible with traditional analyses.

<http://sarts.boegholm.dk/>

- **STG**

- STG (Symbolic Test Generator) generates conformance tests, based on this framework:
 - Implementation: black-box, only input/output behavior is observable.
 - Specification: IOSTS(input/output behavior + internal structure)
 - Test Purpose: IOSTS, tells which part of the specification is to be tested
 - Test Case: IOSTS generated by STG from a specification and a test purpose
 - Test Cases are symbolic, and possibly parameterized by constants
 - They take into account possible non-determinism of the Spec;
 - They include a verdict (no manual interpretation needed)

- <http://www.irisa.fr/prive/ployette/stg-doc/stg-web.html>


- **TIMES**


- TIMES is a **T**ool for **M**odeling and **I**mplementation of **E**mbedded **S**ystems. It is a tool set for modelling, schedulability analysis, synthesis of (optimal) schedules and executable code. It is appropriate for systems that can be described as a set of tasks which are triggered periodically or sporadically by time or external events.


<http://www.timestool.com/>


5. Cluster Participants


5.1 Core Partners


| Cluster Leader | |
|---|--|
|  | Professor Kim G Larsen (Aalborg) http://www.cs.aau.dk/~kgl/ |
| Technical role(s) within ArtistDesign | Leads and coordinates the overall activities in the cluster together with Tom Henzinger; Team Leader for Aalborg. Contributes with expertise on timed automata based models with particular emphasis on extensions with cost, probabilities and multiplayer extensions. Verification, synthesis, performance evaluation and model-based testing. |


| Cluster Leader | |
|---|--|
|  | Professor Tom Henzinger (EPFL) http://mtc.epfl.ch/~tah/ |
| Technical role(s) within ArtistDesign | Leads and coordinates the overall activities in the cluster together with Kim Larsen; Team Leader for EPFL. Contributes with expertise on Rich interface theory for component-based design. Quantitative properties for the design of reactive systems with resource constraints. Languages and algorithms for specifying, checking and comparing resource-dependent specifications. |
| | |


| Team Leader | |
|---|--|
|  | Professor, Director Ed Brinksma (University of Twente/Embedded Systems Institute) http://wwwhome.cs.utwente.nl/~brinksma/ |
| Technical role(s) within ArtistDesign | Team Leader for ESI; Contributes with expertise on quantitative and resource modelling as well as model based testing. |


| Team Leader | |
|--|--|
|  | Professor Wang Yi (Uppsala) http://user.it.uu.se/~yi/ |
| Technical role(s) within ArtistDesign | Contributes with expertise on Resource modelling and Timing Analysis. |


| Team Leader | |
|---|---|
|  | Scientific Leader Thierry Jeron (INRIA) http://www.irisa.fr/prive/jeron/ |
| Technical role(s) within ArtistDesign | Team Leader for INRIA. Contributes with his expertise on models with data and time for model-based test selection and coverage criteria, as well as for quantitative verification, control and diagnosis. |


| Team Leader | |
|---|--|
|  | Susanne Graf (VERIMAG) http://www-verimag.imag.fr/~graf/ |
| Technical role(s) within ArtistDesign | Team Leader for Verimag. Contributes with expertise on component-based design, the BIP framework, platform-aware implementation of embedded systems, structural verification. Modelling taking into account extra-functional properties. |


| Team Leader | |
|--|--|
|  | Prof. Dr. Werner Damm (OFFIS) http://www.offis.de/ |
| Technical role(s) within ArtistDesign | Team Leader for OFFIS. Contributes with expertise on component-based design and semantic foundation, in particular non-functional aspects as real-time and safety. |


| Team Leader | |
|---|--|
|  | Dr. Sébastien Gérard, CEA. |
| Technical role(s) within ArtistDesign | Team Leader for CEA. Contributes with expertise on model-based engineering, specific focus on standard modelling (specially OMG UML, SYSML and MARTE standards) and RT/E (Real-Time/Embedded) domains. |

| Team Leader | |
|---|--|
|  | Professor Bengt Jonsson (Uppsala) http://user.it.uu.se/~bengt/ |
| Technical role(s) within ArtistDesign | Team Leader for Uppsala. Contributes with expertise on Component Modeling and Verification. |

| Team Leader | |
|--|---|
|  | Professor Martin Törngren (KTH) http://www.md.kth.se/~martin/ |
| Technical role(s) within ArtistDesign | Team Leader for KTH. Contributes with expertise on Integrated models supporting cross-layer validation. Methods for validation of self-configuring systems. Compositional validation of integrated models/components. |

| Team Leader | |
|---|--|
|  | Professor Christoph Kirsch (Salzburg) http://cs.uni-salzburg.at/~ck/ |
| Technical role(s) within ArtistDesign | Team Leader for Salzburg. Contributes with expertise on Compositional timing and reliability modeling in the Giotto family of languages. |

| Team Leader | |
|---|--|
|  | <p>Professor Alberto L. Sangiovanni-Vincentelli (Parades)</p> <p>http://www.eecs.berkeley.edu/Faculty/Homepages/sangiovanni-vincentelli.html</p> |
| Technical role(s) within ArtistDesign | Team leader for Parades. Contributes with expertise on Platform-Based Design, the Metropolis and COSI frameworks, industrial applications and international activities. |

| Team Leader | |
|--|---|
|  | <p>Joseph Sifakis (Director of VERIMAG)</p> <p>http://www-verimag.imag.fr/~sifakis/</p> |
| Technical role(s) within ArtistDesign | Team Leader for Verimag. Contributes with expertise on component-based design, the BIP framework, platform-aware implementation of embedded systems, structural verification. Context-based analysis. |

5.2 Affiliated Partners

| | |
|---------------------------------------|--|
| | Dr Henrik Lönn, Volvo Technology |
| Technical role(s) within ArtistDesign | <i>System engineering and modelling at Volvo. Leading the effort in developing the EAST-ADL modelling language for automotive embedded systems, through the series of projects EAST-EAA, ATESSST and ATESSST2.</i> |

| | |
|---------------------------------------|---|
| | Jacques Pulou (France Telecom R&D, France) |
| Technical role(s) within ArtistDesign | <i>Component behaviour modeling, Component Based OS construction.</i> |

| | |
|--|--|
| | Prof. Albert Benveniste (INRIA Rennes, France) |
|--|--|

| | |
|---------------------------------------|---|
| | |
| Technical role(s) within ArtistDesign | <i>Interfaces and modal automata</i> |
| | Prof. Roderick Bloem (TU Graz, Austria) |
| Technical role(s) within ArtistDesign | <i>Game models for the synthesis problem.</i> |
| | Prof. Roberto Passerone (Uni. Trento, Italy) |
| Technical role(s) within ArtistDesign | <i>Formal analysis of heterogeneous composition, abstract algebra, and metamodeling.</i> |
| | Dr. Koos Rooda, (TU Eindhoven, The Netherlands) |
| Technical role(s) within ArtistDesign | <i>Systems engineering.</i> |
| | Prof. Dr. Paul van den Hof, (TU Delft, The Netherlands) |
| Technical role(s) within ArtistDesign | <i>Performance modelling</i> |
| | Prof. Tiziano Villa (Uni. Verona, Italy) |
| Technical role(s) within ArtistDesign | <i>Formal verification methods for hybrid systems. Competence in reachability for Hybrid Systems.</i> |
| | Prof. Pierre Wolper (CFV, Belgium) |
| Technical role(s) within ArtistDesign | <i>Computer-aided verification</i> |
| | Prof. Yiannis Papadopolis, Univ. Of Hull (UK) |
| Technical role(s) within ArtistDesign | <i>Compositional safety analysis and design optimization w.r.t. safety.</i> |
| | Ahmed Bouajjani - LIAFA (France) |
| Technical role(s) within ArtistDesign | <i>Real-time and hybrid model checking</i> |
| | Stavros Tripakis – Cadence Research lab (USA) |

| | |
|---------------------------------------|--|
| Technical role(s) within ArtistDesign | <i>Monitoring and test of real-time properties</i> |
| | Jean-Francois Raskin (CVF – Belgium); |
| Technical role(s) within ArtistDesign | <i>Efficient Model-checking of linear-time properties. Verification and synthesis for reactive systems. Timed and hybrid automata.</i> |
| | Joost-Pieter Katoen (Aachen – Germany) |
| Technical role(s) within ArtistDesign | <i>Model checking of quantitative system properties. Verification of (continuous-time) probabilistic and stochastic systems.</i> |
| | Holger Hermanns (Saarlandes U – Germany); |
| Technical role(s) within ArtistDesign | <i>Probabilistic and stochastic model checking.</i> |
| | Christel Baier (Dresden – Germany); |
| Technical role(s) within ArtistDesign | <i>Probabilistic and stochastic model checking</i> |
| | Patricia Bouyer, Nicola Markey and Phillippe Schnoebelen (LSV Cachan – France), |
| Technical role(s) within ArtistDesign | <i>Decidability and algorithms for priced timed automata and games. Algorithms for solving games of imperfect information</i> |
| | Prof. dr. ir. Wil van der Aalst, professor at Eindhoven University of Technology, The Netherlands |
| Technical role(s) within ArtistDesign | <i>Information System. Affiliated participant in the ESI Octopus project.</i> |
| | Prof. dr. Mehmet Aksit, professor at Twente University, The Netherlands. |
| Technical role(s) within ArtistDesign | <i>Software Engineering. Affiliated participant in the ESI Darwin project.</i> |
| | Prof. dr. Sandro Etalle, professor at Eindhoven University of Technology, The Netherlands. |
| Technical role(s) within ArtistDesign | <i>Security. Affiliated participant in the ESI Darwin project.</i> |
| | Prof. dr. Arjen van Gemund, professor at Delft University of |

| | |
|---------------------------------------|---|
| | Technology, The Netherlands. Embedded Software Laboratory. |
| Technical role(s) within ArtistDesign | <i>Affiliated participant in the ESI projects Trader and Octopus.</i> |
| | Prof. dr. Frits Vaandrager, professor at Radboud University, The Netherlands. |
| Technical role(s) within ArtistDesign | <i>Formal methods. Affiliated participant in the ESI Octopus project.</i> |

6. Internal Reviewers for this Deliverable

Bruno Bouyssounouse (Verimag)