



IST-004527 ARTIST2  
Network of Excellence  
on Embedded Systems Design

Cluster Progress Report for Year 4

Cluster:  
**Testing and Verification**

Cluster Leader:  
Director, Professor Kim Guldstrand Larsen  
CISS, Aalborg University, Denmark  
[www.ciss.dk](http://www.ciss.dk)

*Policy Objective (abstract)*

*The objective 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 in verification and testing methodologies. Meeting place*

*Testing and verification is a transversal topic interacting with all the other topics in embedded systems design aiming to ensure that the different design steps meet given properties as well as the overall correctness of the implementation. Focus within the cluster is on two aspects being of extreme importance for embedded systems. First is the verification and testing of quantitative properties ensuring that real-time constraints and quality of service constraints are met. Second is the verification of security properties. A particular objective is the successful transfer of knowledge, methods and tools to industry.*

## Table of Contents

1. Overview .....	3
1.1 High-Level Objectives.....	3
1.2 Industrial Sectors.....	4
1.3 Main Research Trends .....	6
2. State of the Integration in Europe .....	8
2.1 Brief State of the Art .....	8
2.2 Main Aims for Integration and Building Excellence through Artist2 .....	9
2.3 Other Research Teams .....	9
2.4 Interaction of the Cluster with Other Communities .....	10
3. Overall Assessment and Vision for the Cluster .....	11
3.1 Assessment for Year 4 .....	11
3.2 Overall Assessment since the start of the Artist2 NoE .....	11
3.3 Vision Beyond the Artist2 NoE.....	12
4. Cluster Participants .....	13
4.1 Core Partners .....	13
4.2 Affiliated Industrial Partners.....	17
4.3 Affiliated International Partners.....	18
5. Internal Reviewers for this Deliverable.....	20

# 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 high level objectives for the 18 months period, February 2007 until August 2008, are as follows:

- *Quantitative Testing and Verification*: included continued effort towards efficient tool components for controller synthesis, initiation of work on property-preserving code generation, development of generic frameworks using abstraction and compositionality for efficient analysis of quantitative models and new debugging and analysis techniques based on various combinations of testing and verification techniques

Also, based on existing powerful (real-time) verification techniques work towards maturing and further development of important topics such as optimal scheduling, monitoring and fault diagnosis, controller synthesis, robustness and implementability of quantitative models and analysis of hybrid models, stochastic and timed models has been planned.

- *Testing and Verification Platform for Embedded Systems*: Systems the objectives include continued improvement related to the individual tools, their advancement and dissemination as well as application on industrial case studies. Also, the objectives include a high performance tools server.
- *Verification of Security Properties*: Based on a decision made at the last review, the activities on security have been embedded within the two activities above.

For *Quantitative Testing and Verification* almost all objectives have been accomplished. Substantial research advancing state-of-the-art of controller synthesis has been made covering synthesis with budget constraints, partial observability, modular and distributed synthesis, cost-optimality, synthesis with respect to bounded response properties.

A variety of quantitative models have been introduced and thoroughly examined, including models with resources (e.g. cost, energy, memory consumption, stack size, etc) as well as stochastic aspects. Methods supporting compositionality and component based development using rich interfaces (i.e. quantitative component specifications) have been provided and abstraction of quantitative models (both stochastic and hybrid) have provided the basis for efficient analysis methods.

Novel debugging and analysis techniques have been provided including techniques based on heuristic and guided search, off-line test generation using games as well as symbolic model checking techniques.

Robustness and implementability has been subject to less activity than anticipated. However, within upcoming newly started FP7 STREP projects these topics will be pursued during the next years.

Within *Testing and Verification Platform for Embedded Systems* all objectives have been accomplished. The individual tools have been further refined – both with respect to functionality and performance. E.g. The tool UPPAAL TIGA now offers a mature tool for (time-

optimal) synthesis for timed games models with a growing number of industrial applications. Also, the work of dissemination of the tools through case study demonstrators has been continued and documented through the joint web page for industrial case studies. Finally, the high performance tools server has been completed making the tools suitable for 64 bit architectures and distributed PC clusters available via a common web interface.

## 1.2 Industrial Sectors

The testing and verification techniques and 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 platform<sup>1</sup> *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:

- “.. 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>), and include:

- Danfoss (Aalborg): The project has two main goals. One is to develop an automated test execution environment for system level testing of the EKC series refrigeration controllers. The other is to improve model-based online testing given the experiences from the first trials
- ESI (Embedded Systems Institute, Eindhoven) has carried out (is carrying out) large industrial case studies with Océ, ASML, Philips Semiconductors (now NXP), Philips Medical Systems, Vanderlande Industries.
- Ericsson Telebit (Aalborg): The goal of this project has been to use Live Sequence Charts in a model-driven approach to the testing of TCP/IP internet protocols. Live Sequence Charts are used to capture (informal) RFC in a formal, yet intuitive, way.

---

<sup>1</sup> <http://www.artemis-office.org/>

- Novo Nordisk A/S. (Aalborg) Automatic generation of test cases from UML statechart models of MMI (man machine interface) for medical devices. Each statechart model describes a specific class of usage scenarios, and test cases are derived in two steps. First the model is translated into an equivalent timed automata. Then the automata is analysed based on various parameters (coverage criteria, search depth, etc) resulting in a number of test cases expressed in the company specific scripting language. The obtained coverage and possibly unreachable states are reported.
- OFFIS, University of Freiburg, Aalborg University: The "Single-tracked Line Segment" (SLS) case study stems from an industrial partner of the UniForM-project. It is the specification of a control system for a single-tracked line segment for tramways. It is implemented by distributed PLC automata. We took three different models of the SLS case study as examples. As the safety property to verify, we chose the mutual exclusion of drive permissions, i.e., the control system never gives permission to both directions simultaneously.
- OFFIS; Univ. of Oldenburg; Albert-Ludwigs-Universität Freiburg; Max-Planck-Institut für Informatik: The flap controller (high-lift) case study is derived from a case study for Airbus, a controller for the flaps of an aircraft. The flaps are extended during take-off and landing to generate more lift at low velocity. They are not robust enough for high velocity, so they must be retracted for other periods. The controller can perform a load-relief function to correct the pilot's commands if he endangers the flaps. Additionally, there is also an extensive monitoring of the health of its sub-systems, checking for instance for hardware failures. Typically this will give rise to large discrete state spaces when model checking models derived from the flap controller.
- OFFIS, Univ. of Oldenburg : Automating verification of cooperation, control, and design in traffic applications. Here we present a verification methodology for cooperating traffic agents covering analysis of cooperation strategies, realization of strategies through control, and implementation of control. For each layer, we provide dedicated approaches to formal verification of safety and stability properties of the design. The range of employed verification techniques invoked to span this verification space includes application of pre-verified design patterns, automatic synthesis of Lyapunov functions, constraint generation for parameterized designs, model-checking in rich theories, and abstraction refinement. We illustrate this approach with a variant of the European Train Control System (ETCS), employing layer specific verification techniques to layer specific views of an ETCS design.
- Scott/Tiger Validate (Aalborg): From timed automata design models the verification engine of UPPAAL is used for off-line generation of test-sequences which covers the model. In the project a tool for translating these logical test-sequences to test-scripts executable in, e.g., QTP of Mercury's Test Director. The resulting tool-chain has been applied to automatic testing of web-services of TDC (Danish Telecom). A commercial spin-off tool (V+) has been developed.
- Skov A/S (Aalborg): In this work, we provide a complete tool chain for automatic controller synthesis using UPPAAL Tiga and Simulink. The tool chain is explored using an industrial case study for climate control in a pig stable. The problem is modelled as a game, and UPPAAL Tiga is used to automatically synthesize a safe strategy that is transformed for input to Simulink, which is used to run simulations on the controller and generate code that can be executed in the actual pig stable. The models allow for guiding the synthesis process and generate different strategies that are compared through simulations.
- Dependable Systems and Software (DSS) group at Saarland university, Formal Methods and Tools group (FMT) and Design and Analysis of Communication Systems

(DACS) group at the university of Twente: Arcade models. These include two case studies found in the literature, namely a Distributed Database Architecture and a Reactor Cooling System. Arcade tool was used which is based on the input/output interactive Markov chains formalism.

- DSS group at Saarland university, FMT and DACS groups at the university of Twente: Dynamic Fault Tree (DFT) models These include four case studies that also appeared in the literature, namely the cascaded PAND system, the cardiac assist system, the multi-processor distributed computing system, and the fault-tolerant parallel processor. Coral tool was used which is based on the input/output interactive Markov chains formalism.
- Software engineering group and FMT group at the university of Twente: Open-source Media Player. This case study was conducted on a publicly available open-source media player called MPlayer (<http://www.mplayerhq.hu/>). We have modeled the recovery mechanism implemented for the MPlayer and analyzed the availability of the system. Few tools were used including the FLORA framework and the CADP tool set (<http://www.inrialpes.fr/vasy/cadp/>). The input/output interactive Markov chains formalism was used.
- Uppsala University: As a case study, we have developed a formal model for a Biomedical Sensor Network (BSN). The sensor nodes of the network are constructed based on the IEEE 802.15.4 Zig-Bee standard for wireless communication. The UPPAAL tool is used to tune and validate the temporal configuration parameters of the network in order to guarantee the desired QoS properties for a medical application scenario. The case study shows that even though the main feature of UPPAAL is model checking, it is also a promising and competitive tool for efficient simulation.

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

Within the area of Testing and Verification the overall trend is that systems of increasing complexity with an increasing number of features taking into account may be dealt with.

A definite trend is also, that model-checking and testing techniques are being applied directly to software validation (in particular C and JAVA) with noticeable successes given by the SLAM, Blast, VeriSoft, Bandera and JAVA-Path-Finder projects. Here, the method of *abstraction-refinement* provides a combination of abstract interpretation with model-checking with success within given application domains (e.g. SLAM and Blast addresses debugging of device drivers). The method of so-called Counter-Example-Guided-Abstraction-Refinement (CEGAR) method has during the last period found its way into the analysis of quantitative models including timed, hybrid as well as probabilistic models.

Another trend within the research area of verification is the (re-)discovery of SAT-solving as a technique for performing so-called *bounded* model-checking. Advances made on SAT-solving during the last 5 years has made this approach competitive compared to other techniques including symbolic model-checking. Members of the T&V cluster have been active in pursuing extensions of SAT-solving to extended logics with quantitative aspects (difference constraints, linear constraints) in order to make bounded model-checking applicable to models of embedded systems.



Yet another trend is that the features and properties supported by current technology goes beyond that of pure functional correctness to also include timed, stochastic and hybrid phenomena. Within the Testing and Verification Cluster research on all of these quantitative extensions are pursued actively pursuing different techniques (bounded model checking, regular model checking, decision diagrams, automata for symbolic representation) are finding their way into powerful tools (e.g. UPPAAL, IF, CMC, MoDeST, EMTCC, FAST).

Advances in verification technology (in particular the development of symbolic data structures) are finding their way into mature testing tools (e.g. TGV, STG, ToRX). Substantial effort has been made by several partners on model-based testing and monitoring of real-time systems with UPPAAL Tron and IF being some resulting tools. Also, related work on monitoring, controller synthesis, planning and scheduling, and schedulability analysis for real-time systems has been made resulting in tools such as TIMES and UPPAAL Cora and UPPAAL Tiga and several applications. In particular, during the last period substantial progress has been made on the theoretical underpinning and efficient implementation of controller synthesis algorithms, for untimed as well as timed models. A growing number industrial applications has been witnessed, demonstrating the maturity of the technology.

Model-driven development is highly appreciated in software engineering particularly because of the possibility of automatic code-generation. However, for quantitative models the realization on real hardware raises several problems. Indeed, the quantitative models are theoretical frameworks, assuming infinitely fast hardware, infinitely precise clocks, etc. However, these characteristics are not fulfilled on real CPUs, that are digital and have a finite frequency. Current research within the cluster is addressing this problem in the setting of real-time and involves identification on when (and how) given quantitative automata models are implementable and to what extent properties proved by the model also may be guaranteed to hold of the final implementation.

Within verification of security properties work has been made on the semantic foundations and the verification of security protocols and web-services. A general verification method for security protocols with possible unbounded sessions has been provided as well as a sound and complete inference systems for bounded-sessions cryptographic protocols. The work also include a classification and relation of different existing specification methods (multi-set rewriting and process algebra) for security protocols as well as the use of standard model-checkers for analysing various security protocols (e.g. use of  $\mu$ CRL, SPIN and CADP) and for addressing security treats based on real-time issues (using UPPAAL).

In the area of parallel and distributed model checking of embedded systems we are in close collaboration with other research teams in Europe (INRIA Rhone-Alpes, CWI, Technical University Munich and Aachen Technical University) attempting to gather the European research communities working in the area on cluster and/or grids. Scientifically the work within the cluster has primarily focused on new algorithms for the enumerative distributed checking of reachability properties, and on extended the scope of *efficient* distributed algorithms to cover model checking of general CTL and LTL properties and of real-time models. The general environment DiVinE has been deployed and has also been extended by a Promela front-end for SPIN. In addition to the utilization of PC-clusters a trend during the last period has been the exploitation of multi-core and 64-bit architectures for high performance analysis and verification of large models.

## 2. State of the Integration in Europe

The objective of the Testing and Verification 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 in verification and testing methodologies. As will be described below 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*

We refer to section 1.3 in this deliverable for an account of the main trends within testing and verification. With respect to testing and verification of quantitative and security aspects and the construction of a testing and verification platform the following gives a brief state of the art:

#### *Quantitative Test and Verification*

An important step towards supporting quantitative analysis of real-time aspects is provided by the modeling formalism of timed automata. The potential of timed automata for the modeling and analysis of real-time systems has been documented extensively in the literature. Since their introduction by Alur and Dill in 1990, several verification tools for timed automata have been developed (in particular UPPAAL, Kronos and IF) which are now applied routinely to industrial-size case studies.

Significant effort on stochastic model checking has been made during the last decade, and performance and industrial application of tools (e.g. PRISM, MRMC and ETMCC) have been increasing substantially during this last period. A logical next step to be undertaken with the European projects Quasimodo and ARTIST Design is support for analysis of quantitative models involving both timing information as well as stochastic information.

However, also a number of formalisms allowing to model and reason about other quantitative aspects (e.g. energy or memory consumption) have been studied. The priced extensions of the timed automata formalism has been introduced - permitting consumption of resources to be taken into account. Efficient algorithms for analyzing these models are to be found within the special purpose tool UPPAAL Cora.

Also controller synthesis and stochastic extension has been considered as well as the transfer of successful techniques for timed automata to classes of hybrid automata. On a number of (industrial) cases the partners have successfully demonstrated a tool-chain combining synthesis based on very abstract models (UPPAAL Tiga), verification of the synthesized controller in the setting of a more realistic continuous environment (PHAVer or HyTECH) and finally performance evaluation using simulation (Simulink).

In addition, the foundational principles for generation of predictable code from timed automata models, and conformance testing based on timed automata models has been subject to research. In particular, efficient prototype implementation of "robust" model checking algorithms has been made.

The partners are participating very actively in the research aiming to improve the above state of the art on specific areas within quantitative testing and verification as mentioned below, i.e. within the areas of timing, resources, schedulability, stochastic and hybrid aspects as well as testing theory,

#### *Platform for Testing and Verification*

Testing and verification of embedded systems are computationally hard and memory intensive activities as the underlying models contain (multiple) quantitative aspects in



order to enable the expression of important properties concerning real-time constraints, impact on physical environment, expected resource consumption and performance of a given design, etc.

During this last period the partners of the cluster have been active in implementing, improving and disseminating a large number of testing and verification tools allowing for the analysis of quantitative models including real-time aspects, resource models, hybrid and stochastic models. In particular, substantial effort has been made towards exploiting architectural features (multi-core, clusters, grid, 64-bit) in order to realize the vision of a high-performance platform. We refer to the deliverable for the *Testing and Verification Platform* for a more detailed account. What is important to note here is that there is a very short distance (time-wise) from foundational decidability results to their impact on performance of tools in terms of improved data-structures and algorithms.

## **2.2 Main Aims for Integration and Building Excellence through Artist2**

As demonstrated in the section above the integration of the research groups within the cluster is excellent and with significant impact on the larger research community on testing and verification 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.

However, given the limited resources available within ARTIST2 it has been paramount that substantial, additional European funding was obtained to support the man-power required to fully transform the research ideas and prototype tools into industrial testing and verification practice with a supporting collection of tools integrated with existing industrial tool chains. This exercise will now be undertaken in the two newly started European projects Quasimodo and Multiform (STREP under FP7), in which several partners of the Testing and Verification Cluster are key members.

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**

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 (security).

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.

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 ARTIST2), Rice University, Texas (Vardi, longstanding collaboration with Wolper on the highly appreciated and influential automata theoretic approach). Also ARTIST2 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***

At the *scientific level* model checking technology forms the very basis for automatic verification with numerous applications. Its recognition in Computer Science as a core technology is clearly witnessed by the giving the Turing Award 2007 jointly to Edmund Clark, Allan Emerson and Joseph Sifakis for their original and continued research on model checking.

In the period of ARTIST2 model-checking 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. Friburg 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; in particular ESI is a member of ARTEMIS, and other partners of the cluster have been active in promoting ARTEMIS at national levels (e.g. Aalborg together with IMM/DTU have been initiators of the Danish D-ARTEMIS consortium).

### 3. Overall Assessment and Vision for the Cluster

#### 3.1 Assessment for Year 4

Each research activity within the cluster has successfully pursued the research goals of the given 18 months period.

As for the previous years the cluster integration activities within *Quantitative Testing and Verification* and *Verification of Security Properties* have been particularly active during this third year as is most clearly demonstrated by the (very) extensive lists of publications made by members of the cluster during the first year at leading scientific conferences and journals witnessing true excellence within the area

The activities within *Testing and Verification Platform* are tightly connected to the activities within *Quantitative Testing and Verification* in that the latter provides the theoretical foundation, as well as design of data-structures and algorithm necessary for the development of efficient and mature tools. Within this activity the objectives related to the individual tools, their advancement and dissemination has been fully accomplished. Finally, the high performance tools server has been completed making the tools suitable for 64 bit architectures and distributed PC clusters available via a common web interface.

Dissemination to research and industry has been done extensively during the third year period by partners individually and in concerted efforts as witnessed by the long list of key note presentations, tutorials and workshops organised.

#### 3.2 Overall Assessment since the start of the Artist2 NoE

During the period of Artist2 the partners of the Testing & Verification cluster have demonstrated true research excellence as witnessed by the extensive list of publications at leading conferences and journals, numerous invited keynote presentation 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 – and as detailed in the case study repository – in several collaborative projects with companies the adaptation of model-driven development has resulted in notable reduced time-to-market.

Within the period of the ARTIST2 NoE the partners have clearly contributed to the building of the European Testing&Verification community within embedded systems. This is clearly demonstrated by the high number of joint projects (FP7, ESF as well as national) that during the period have been initiated by members of the cluster.

Within the activities on Quantitative Testing and Verification major advances within controller synthesis were made during the period taking the technology from theoretical results to efficient algorithms and tools and with validation on industrial applications. Within the Tool Platform activities the ambition of a European Verification Grid did not emerge as certain key people left the cluster in order to concentrate on building a European/Nordic GRID facility for scientific computing in general. Instead a tool server giving access to tools key to the partners of the cluster has been implemented. During the first 3 years the activities on Verification of Security Properties has been performing at the highest level scientifically but somewhat disjoint from the other activities of the cluster.

### 3.3 *Vision Beyond the Artist2 NoE*

As clearly observed by the many industrial contacts of the two national embedded systems centers, ESI (The Netherlands) and CISS (Denmark), testing is *by far* the most used and important validation technique applied by industry today. It is estimated that some *30-70% of the total development cost* for embedded systems is spent on testing at various stages. It is also a general observation that current testing practice is very ad-hoc often with manual construction and even execution of test-scripts. There is clearly a gap between current industrial practice and existing academic state-of-the art technology. It is important that continued effort is made towards bridging this gap through collaborative projects attempting to make industry take-up existing state-of-the-art testing and verification techniques.


To focus on aspects such as performance, timeliness, and efficient resource-usage, the testing and verification techniques should be based on models with *quantitative information*. To provide a coherent model-based testing and verification methodology with a well-integrated chain of tools applied in industrial practice is a long-term vision beyond the ARTIST2 NoE. In addition to modelling, this will require a strong focus on analytical techniques that address the combination of non-determinism, real-time and stochastic information. Here we foresee the need for techniques that will combine Abstract Interpretation and Model Checker. Also support for high abstraction levels must be provided to overcome the inherent complexity of modern embedded systems. Finally, (semi-)automatic generation of code that preserves the relevant design properties will be essential to ensure industrial impact. These challenges on quantitative modelling and verification will be key activities within the ARTIST Design NoE.


The momentum and willingness of the partners of the cluster to continue working together is very strong. This is witnessed by the two newly started EU FP7 STREP projects *Quasimodo* and *Multiform*. Here *Quasimodo* is targeted towards quantitative modelling formalisms and tool plug-ins for the use in specification, analysis, implementation of embedded systems, and *Multiform* focuses on tool-integration of academic tools (e.g. PHAVer and UPPAAL) and commercial tools (e.g. Simulink). Other partners of the cluster are active in the SPEEDS project where formats for tool exchange are becoming available.


The partners of the cluster also intend to play an active role in the forth-coming Joint Technology Initiative ARTEMIS' research priority on Design Methods and Tools. Here ESI already play a leading role.

## 4. Cluster Participants


### 4.1 Core Partners


<b>Cluster Leader</b> <b>Activity Leader for “Testing and Verification Platform for Embedded Systems”</b> <b>Team Leader for Aalborg on the activities “Testing and Verification Platform for Embedded Systems” and “Quantitative Testing and Verification”</b>	
	Professor, Director Kim G. Larsen (Aalborg) <a href="http://www.cs.aau.dk/~kgl/">http://www.cs.aau.dk/~kgl/</a>
Technical role(s) within Artist2	Leads and coordinates the overall activities in the cluster; coordinates the activities of the “Test and Verification Platform for Embedded Systems”; member of the Artist2 strategic management board; highly active on the development of algorithms and tools within the activity on “Quantitative Testing and Verification”.


<b>Team Leader for Aalborg on the activity “Verification of Security Properties”</b>	
	Dr. Hans Hüttel (Aalborg) <a href="http://www.cs.aau.dk/~hans/">http://www.cs.aau.dk/~hans/</a>
Technical role(s) within Artist2	Contributes to the security activity with foundational work the development on process calculi to describe security aspect of embedded systems.

<b>Assistant for the Cluster Leader</b>	
	Dr. Arne Skou (Aalborg) <a href="http://www.cs.aau.dk/~ask/">http://www.cs.aau.dk/~ask/</a>
Technical role(s) within Artist2	Takes part in the cluster coordination; contributes with expertise on model based testing and tools, industrial contacts, and industrial

	dissemination.
--	----------------


Team Leader for CFV on the activity “Testing and Verification of Security Properties”	
	Professor Jean-François Raskin (CFV) <a href="http://www.ulb.ac.be/di/ssd/jfr/">http://www.ulb.ac.be/di/ssd/jfr/</a>
Technical role(s) within Artist2	Contributes with his expertise on controller synthesis and design and development of the LaSH tool.


Team Leader for CFV on the activities “Testing and Verification Platform for Embedded Systems” and “Quantitative Testing and Verification”	
	Professor Pierre Wolper (CFV) <a href="http://www.montefiore.ulq.ac.be/~pw/">http://www.montefiore.ulq.ac.be/~pw/</a>
Technical role(s) within Artist2	Contributes with his expertise to all activities on model checking within the cluster.


Team Leader for EPFL on the activities “Testing and Verification Platform for Embedded Systems” and “Quantitative Testing and Verification”	
	Professoer Tom Henzinger (EPFL) <a href="http://mtc.epfl.ch/~tah/">http://mtc.epfl.ch/~tah/</a>
Technical role(s) within Artist2	Contributes with his seminal expertise on models and tools for quantitative aspects of embedded systems.

Team Leader for FT-R&D on “Verification of Security Properties”	
	Researcher F. Klay (France Telecom R&D)
Technical role(s) within Artist2	Francis Klay is collaborating with protocol designers within FT R&D on two important case studies: an electronic purse protocol and e-vote protocol. He is acting as an intermediate between the protocol designers and some of the other partners in Artist in the sense that he is spending a great amount of effort explaining the validation tools and methods developed by these partners.




<b>Team Leader for INRIA on the activities “Testing and Verification Platform for Embedded Systems” and “Quantitative Testing and Verification”</b>	
	Scientific Leader Thierry Jeron (INRIA) <a href="http://www.irisa.fr/prive/jeron/">http://www.irisa.fr/prive/jeron/</a>
Technical role(s) within Artist2	Contributes with his expertise on model based testing and verification and in particular on design and development of the TGV too as well as industrial dissemination.


<b>Team Leader for LSV on “Verification of Security Properties”</b>	
	Hubert Comon (LSV) <a href="http://www.lsv.ens-cachan.fr/~comon/">http://www.lsv.ens-cachan.fr/~comon/</a>
Technical role(s) within Artist2	Contributes to the activity on security with his expertise on cryptographic protocols.


<b>Team Leader for LSV on the activities “Testing and Verification Platform for Embedded Systems” and “Quantitative Testing and Verification”</b>	
	Director Philippe Schnoebelen (LSV) <a href="http://www.lsv.ens-cachan.fr/~phs/">http://www.lsv.ens-cachan.fr/~phs/</a>
Technical role(s) within Artist2	Contributes with his expertise on logics and model checking in general.

<b>Team Leader for Offis on the activities “Testing and Verification Platform for Embedded Systems” and “Quantitative Testing and Verification”</b>	
	Professor, Director Werner Damm (Offis) <a href="http://www.php.informatik.uni-oldenburg.de/mitarbeiter.php?MNr=19">http://www.php.informatik.uni-oldenburg.de/mitarbeiter.php?MNr=19</a>

Technical role(s) within Artist2	Contributes with his expertise on specification formalisms, tool development as well as industrial dissemination
----------------------------------	--

<b>Activity Leader for “Quantitative Testing and Verification”</b> <b>Team Leader for Twente on the activities “Testing and Verification Platform for Embedded Systems” and “Quantitative Testing and Verification”</b>	
	Professor, Director Ed Brinksma (University of Twente/Embedded Systems Institute) <a href="http://wwwhome.cs.utwente.nl/~brinksma/">http://wwwhome.cs.utwente.nl/~brinksma/</a>
Technical role(s) within Artist2	Coordinates the cluster activities of “Quantitative Testing and Verification”; contributes with industrial dissemination and case studies as well as development of algorithms and tools.

<b>Activity Leader for “Verification of Security Properties”</b> <b>Team Leader for Twente on “Verification of Security Properties”</b>	
	Dr. Sandro Etalle (Twente) <a href="http://wwwhome.cs.utwente.nl/~etalle/">http://wwwhome.cs.utwente.nl/~etalle/</a>
Technical role(s) within Artist2	Coordinates the cluster activities on “Verification of Security Properties”; contributes with methods on constraint based logics and trust management.

<b>Team Leader for Uppsala on the activities “Testing and Verification Platform for Embedded Systems” and “Quantitative Testing and Verification”</b>	
	Professor Wang Yi (Uppsala) <a href="http://user.it.uu.se/~yi/">http://user.it.uu.se/~yi/</a>
Technical role(s) within Artist2	Contributes with his expertise on algorithms and tools for model checking of real time systems – in particular the development of the Uppaal tool and industrial dissemination.

<b>Team Leader for Verimag on the activity “Verification of Security Properties”</b>	
	Professor Yassine Lakhnech (Verimag) <a href="http://www-verimag.imag.fr/~lakhnech/">http://www-verimag.imag.fr/~lakhnech/</a>
Technical role(s) within Artist2	Contributes with his expertise on model checking in general and on verification of security properties and industrial dissemination in particular.

#### **4.2 Affiliated Industrial Partners**

	Boutheina Chetali (Axalto/SchlumbergerSema)
Technical role(s) within Artist2	Contributes with industrial needs wrt. security in embedded systems

	Thomas Hune (Terma A/S)
Technical role(s) within Artist2	Contributes with knowledge on industrial needs for mission critical systems; also with expertise on model driven development In general.


	System architect Jan Lindblad (Enea Embedded Technology )
Technical role(s) within Artist2	Contributes with industrial requirements to testing and verification as they are relevant for operating systems.

	Researcher Alain Ourghanlian (EDF)
Technical role(s) within Artist2	Contributes with knowledge about the industrial needs for efficient, verified code in embedded systems.

	Line Manager Sven H. Sørensen (Motorola A/S)
Technical role(s) within Artist2	Contributes with knowledge about industry needs on model driven development and testing.

### 4.3 Affiliated International Partners

	<p>Professor Andrea Bondavalli (University of Firenze)  <a href="http://rcl.dsi.unifi.it/aboutus/andrea.php">http://rcl.dsi.unifi.it/aboutus/andrea.php</a></p>
Technical role(s) within Artist2	Contributes with expert knowledge on the verification of dependability and fault tolerance for embedded systems.
	<p>Professor Ahmed Bouajjani (LIAFA)  <a href="http://www.liafa.jussieu.fr/~abou/">http://www.liafa.jussieu.fr/~abou/</a></p>
	Contributes with general knowledge on model checking – in particular within infinite state systems
	<p>Professor Lubos Brim (Brno)  <a href="http://www.fi.muni.cz/usr/brim/">http://www.fi.muni.cz/usr/brim/</a></p>
Technical role(s) within Artist2	Contributes significantly to the cluster activity on Platforms for Embedded Systems; in particular within the development of cluster based distributed model checking through the Distributed Verification Environment DeVinE.
	<p>Senior Researcher Fabio Martinelli (CNR-IIT)  <a href="http://www.iit.cnr.it/staff/fabio.martinelli/">http://www.iit.cnr.it/staff/fabio.martinelli/</a></p>
Technical role(s) within Artist2	Is an expert on security protocols and trust management and contributes with important knowledge to the security activity.
	<p>Researcher Michael Rusinowitch (INRIA)  <a href="http://www.loria.fr/~rusi/">http://www.loria.fr/~rusi/</a></p>
Technical role(s) within Artist2	Is an expert on formal methods on embedded systems – in particular on verification of security properties.

	<p>Professor Jan Tretmans (Nijmegen) <a href="http://www.cs.ru.nl/~tretmans/">http://www.cs.ru.nl/~tretmans/</a></p>
<p>Technical role(s) within Artist2</p>	<p>Contributes with expert knowledge on model based testing. Also tools and industrial dissemination.</p>

## **5. Internal Reviewers for this Deliverable**

Contributions and internal review has been made by Bruno Bouyssounouse (UJF/Verimag), Ed Brinksma (ESI and Twente University) and Arne Skou (Aalborg).