

ARTIST 2

Network of Excellence

IST-004527 ARTIST2:
Embedded Systems Design

Cluster Progress Report for Year 2

Cluster:
Testing and Verification

Cluster Leader:

Director, Professor Kim Guldstrand Larsen
CISS, Aalborg University

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.

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	5
2. State of the Integration in Europe	7
2.1 Other Research Teams	7
2.2 Interaction of the Cluster with Other Communities	9
2.3 Main Aims for Integration and Building Excellence through Artist2	9
3. Overall Technical View.....	10
3.1 Brief State of the Art	10
3.2 Ongoing Work in the Partner Institutions	11
3.3 Interaction and Building Excellence between Partners.....	12
4. Overall Assessment and Vision for the Cluster.....	14
4.1 Assessment	14
4.2 Vision and Long Term Goals	15
4.3 Future Work and Evolution	15
4.3.1 <i>Technical Description</i>	15
4.3.2 <i>Current and Future Milestones</i>	16
5. Cluster Participants	17
5.1 Core Partners	17
5.2 Affiliated Industrial Partners.....	21
5.3 Affiliated Academic Partners.....	21

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, September 2005 till February 2007, are as follows:

- *Quantitative Testing and Verification*: Work on test case generation will be continued and disseminated. Testing theories and analysis techniques for quantitative aspects of models and their implementation will be developed with metrics for testing coverage. Also new important areas to be studied includes robustness and implementability of timed models, stochastic model checking and controller synthesis.
- *Verification of Security Properties*: Engineering tools for security protocols including the construction of powerful and accessible tools for the engineering of security and communication protocols for embedded systems. Security and trust management including construction of a resource aware decentralized access control and trust management system for the specification and enforcement of high level access control (and privacy) policies in embedded systems.
- *Testing and Verification Platform for Embedded Systems*: the performance and availability of the individual tools "owned" by the participants of the cluster will be improved and evaluated more carefully through case studies. Also, the results will be disseminated in particular via the Yahooda web page at Brno and a new web page containing case studies. Work on distributed analysis tools will be strengthened and in particular a common coordination layer allowing individual PC-clusters to be combined in a European verification Grid will be initiated.

For *Quantitative Testing and Verification* all objectives have been accomplished with substantial amount of work focusing on robustness and implementability with a number of approaches having been put forward. Also several partners have contributed to the algorithmic foundation for controller synthesis with efficient on-the-fly algorithms and methods for controller synthesis under uncertainty. In particular a number of optimization control problems associated with priced timed automata and games have been settled. Finally, results on verification of hybrid and infinite-state systems have been obtained.

For *Verification of Security Properties* all objectives have been accomplished with the tackling of three related groups of problems: i) the verification of more realistic protocols, ii) the verification of more realistic security properties, and iii) bridging the gap between the verification of security properties and trust management.

For both of the above activities substantial effort has been made to the spreading of excellence by dissemination to industry and research students at workshops, seminars and summer school. Also substantial effort towards making techniques available in tools has been made.

Within *Testing and Verification Platform for Embedded Systems* the objectives related to the individual tools, their advancement and dissemination via web-portals containing (links to) tools and industrial case studies has been accomplished. ARTIST2 partners have participated in two European meetings on parallel and distributed model checking where the issue of exploiting on-going grid activities to build a joint infrastructure for verification has been discussed. Though there are a number of European projects applying high-performance and Grid-based computing to model checking, these projects are still in a build-up phase, and are

dependent on design decision made by the Grid-computing community at large. The long-term ambition of a European Verification Grid is still relevant and should be pursued. However, it requires direct involvement with (and from) Grid consortia (e.g. NorduGrid) and requires substantial additional, dedicated funding.

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 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:

- “.. 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 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 continuation (From February 2006, to approx. January 2007) emphasizes automated testing. 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
- 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.
- Ericsson (Uppsala): In this project we have worked on a case study where a model-based approach to black-box testing is applied to verify that a Wireless Application Protocol (WAP) gateway conforms to its specification. The WAP gateway is developed by Ericsson and used in mobile telephone networks to connect mobile phones with the Internet.

¹ <http://www.artemis-office.org/>

- Felix Ingrat at the LAAS Laboratory in Toulouse, France (Verimag). Advanced Methods for Autonomous Embedded Systems. In this project the monitoring and test generation technology and tools developed within the ARTIST2 Testing and Verification cluster is applied to case studies provided by this group.
- TK Systemtest (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 QTP of Mercury's Test Director. The resulting tool-chain has been applied to automatic testing of web-services of TDC (Danish Telecom).
- Skov A/S (Aalborg): The goal of the project is to evaluate automated model-based testing of selected parts of Skov's climate controllers, with the aim of improving testing practices at Skov as well as improving the research on model-based development conducted at CISS.
- 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.

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).

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 are 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.

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 timed 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 muCRL, 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.

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 Other Research Teams

The Testing and Verification cluster includes the leading European research groups within the area and is well connected to other prominent research teams.

In the Netherlands partners are Twente University (core) and Nijmegen University (affiliated). At Twente University research is focussed on testing and stochastic modelling – both with the desire of establishing theoretical foundations and providing tool support (TorX and MODEST). At Nijmegen University research is along two directions: modelling and analysis of real-time and embedded systems (largely with the use of model checkers SPIN and UPPAAL), and testing of data-intense systems. Other prominent research teams in The Netherlands not partners in the cluster include CWI, Technical University Eindhoven and the Embedded Systems Institute also in Eindhoven. The Dutch research teams are well-connected via national projects (PROGRESS), the teams at CWI and Technical University Eindhoven has just started a new Dutch project (VeriGEM) on distributed model checking which we intend to connect more closely to the activities on Testing and Verification within the cluster. The appointment of Ed Brinksma as scientific director of ESI ensures that the vast number of large industrial research projects on embedded systems carried out on routine basis by this center will be connected to the cluster.

In Germany OFFIS, Oldenburg, is partner of the cluster (core). OFFIS is a partner of the IST project EASIS (Electronic Architecture and System Engineering for Integrated Safety Systems, IST-507690) where the goal is to enable the realization of integrated safety systems by defining a powerful and highly dependable in-vehicle electronic architecture and an appropriate development support. EASIS integrates leading European car manufacturers, suppliers, tool vendors and research institutes to commonly achieve the project goals. Of particular relevance to the T&V cluster are AVACS and VERISOFT, two German top projects on verification and analysis of embedded systems, the DFG² funded long-term research project AVACS (Automatic Verification and Analysis of Complex Systems), a Transregional Collaborative Research Center (SFB/TR), and the BMBF³ funded applied research project VERISOFT. Whereas AVACS' research challenge is of foundational nature, developing novel verification algorithms covering the design space of complex embedded systems, VERISOFT's challenge is to achieve fully verified components for industry-critical systems, employing state-of-art automatic and interactive verification tools.

From the Nordic countries participants of the cluster are CISS, Aalborg University and Uppsala University both doing research on testing and verification of real-time systems with emphasis on tool support. The widely distributed real-time verification tool UPPAAL is the most clear witness of a long-term collaboration between these two sites with emerging tools like UPPAAL Cora, UPPAAL Tron and TIMES sharing the fundamental engine of UPPAAL but targeting towards optimal scheduling and planning, real-time testing and schedulability analysis and code-generation, respectively. Prominent Nordic research teams not being partners of the

² German Research Foundation

³ The German Federal Ministry of Education and Research

cluster are the group Chalmers, Gothenburg Technical University (focussing on SAT-solving and hardware verification), Theoretical Computer Science at Helsinki Technical University, Finland, focussing on LTL model checking and bounded model checking, and Institute of Software Systems, Tampere University of Technology, Finland, with original contributions on reduction methods (stubborn set, partial order reduction, minimization) applied during explicit state-space exploration of concurrent systems.

From France the cluster has Verimag and LSV Cachan as (core) partners with ground-breaking contributions on the theoretical foundation of verification, monitoring and controller synthesis for real-time and hybrid systems. Also, the groups are working actively on providing tool support (IF, Taxys and CMC). IRISA is also (core) partner of the cluster with important research contributions on test generation for models of infinite state systems with control and data. Affiliated partner is LIAFA, University of Paris 7, focussing on verification of infinite-state systems. Other research groups in France relevant to the activities on testing and verification are IRCCyN, Nantex (verification and control of timed and hybrid systems) that is well connected to LSV and Verimag through French national projects CORTOS and CHRONO. Also the VASY research group at INRIA Rhone-Alpes are focusing on analysis of complex systems using LOTOS, with significant tool support CADP and contributions to the state-of-the-art of parallel and distributed model-checking.

In Belgium, The *Centre Fédéré en Vérification* is a working group financed since 2002 by the Belgian National Scientific Research Fund. All the research teams from the French part of Belgium that are interested in computer aided verification are present in the working group including University of Brussels, University of Namur, University of Liège and University of Mons.

From Switzerland, EPFL Lausanne is (by now) core partner with a wide range of ground-breaking research contributions on real-time and hybrid systems, interface automata and games.

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).

Partners of the cluster have been the initiators, SC members and/or served as PC chairs of main conferences in the area such as CAV, TACAS, FORMATS, EMSOFT, CONCUR, ETAPS, PSTV/FORTE, PAPM, HSCC, ARTS, PDMC.

2.2 *Interaction of the Cluster with Other Communities*

Model-checking technology forms the basis for automatic verification and is utilized for test-case generation. However, model-checking is also increasingly applied successfully within and by other communities including control theory, planning and scheduling and performance evaluation. Members of the cluster has published and given invited talks at main conferences and in journals of these other communities (e.g. ICAPS, European Journal of Control, IFAC Annual Reviews in Control, ACM Performance Evaluation Review). 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).

2.3 *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 is paramount that substantial, additional European funding is 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.

3. Overall Technical View

3.1 *Brief State of the Art*

We refer to section 1.3 in this deliverable for a more detailed 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.

More recently priced extensions of the timed automata formalism has been introduced - permitting consumption of resources to be taken into account. During this second year partners within the cluster has provided a number of results concerning decision problems wrt to this model of priced timed automata providing the foundation on which the future implementation within tools will be based. This involves design of data-structures and efficient algorithms. These are now 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.

In addition, the foundational principles for generation of predictable code from timed automata models, and conformance testing based on timed automata models are being provided during this second year.

Significant effort on stochastic model checking has been made during the last decade. However, technology still lack for making stochastic analysis as tractable as that of analysis of timed or untimed models.

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,

Verification of Security Properties

Security engineering is about building systems to remain reliable despite the presence of malice errors. As a discipline, it studies and develops the tools and methods to design, implement and validate systems that guarantee security properties. Many security systems and in particular embedded systems have critical requirements. Their failure may cause serious economic damages (cash machines, electronic purse and other bank systems), endanger personal privacy (medical record systems), endanger the viability of whole business sectors (pay-tv), etc....

Within Artist2, the focus is on tools and methods needed to design embedded systems that guarantee security protocols. More specifically, the focus is on security protocols.

There are by now a number of efficient validation tools for authentication protocols, e.g., Hermes (Verimag), H1 (LSV), CASRUL (LORIA) mention tools developed by Artist2 partners.

Such validation tools have, however, not yet reached the level of maturity to be autonomously used by protocol designers. What is missing? A major obstacle is that these tools are based on a semantic model that is commonly called symbolic or Dolev-Yao model. This essentially means that cryptographic primitives are idealized and their behaviour is, hence, simplified.

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 the second year 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. 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.

3.2 Ongoing Work in the Partner Institutions

Building on the previous section and the deliverables on *Quantitative Testing and Verification*, *Verification of Security Properties* and *Testing and Verification Platform for Embedded Systems* we give a brief account of the specific work done in the various partner institutions:

- *Aalborg*: Foundation and tools for testing, verification and controller synthesis of timed systems. Optimal scheduling and planning using priced timed automata. Compositional methods. Distributed verification of real-time systems. Process calculi for handling authentication, automatic verification for ping-pong protocols.
- *Twente*: Test coverage. Testing probabilistic processes. Quantitative reasoning. Robustness of timed systems. Reliability analysis and scheduling stochastic systems. Reachability with cost and probabilities. Constraint-based protocol analysis, languages for the specification of trust management policies, analysis of attacks using real-time, application to Java Cards.
- *CVF*: Hybrid and timed systems, Infinite state systems, controller synthesis (with incomplete information), robustness and implementability, automata-based symbolic representation.
- *LSV-Cachan*: Models and logics for timed and hybrid systems. Controller synthesis. Theories for intruders in protocol analysis, symbolic protocol analysis, algebraic properties in cryptographic protocols. Complexity results for verification of security protocols, guessing attacks, electronic voting.
- *INRIA/IRISA*: Combination of verification and conformance testing. Symbolic test selection using abstract interpretation. Black-box testing of cryptographic protocols. Supervisory control of infinite systems using abstract interpretation.

- *Verimag*: Conformance testing for real-time systems. Monitoring and fault-diagnosis. notions of secrecy, verification of security properties, symbolic models for cryptographic primitives, development methodology with tool support for certification of Smart Card application at EAL7 of Common Criteria, specification and certification of cryptographic protocols.
- *Uppsala*: Schedulability and code-generation for timed models. Real-time testing and test-based model-estimation.. Verification of timed communication systems with buffers
- *EPFL*: abstraction-refinement for hybrid systems, robust modelling of timed systems, games for control and optimal control of timed systems.
- *OFFIS*: dissemination to industry; timing analysis, schedulability, distribution of task to architecture, hybrid systems, decomposition and reduction approaches to verification.
- *Brno*: Distributed-memory verification of stochastic systems. Parallel algorithms for state space reductions. Parallel verification tools.
- *Nijmegen*: Symbolic techniques for data testing. Action refinement theory with application to testing.
- *CNR-IT*: security and trust management, enforcing mechanisms for security policies,

3.3 *Interaction and Building Excellence between Partners*

During the second year integration within the cluster has been achieved by one cluster meetings, a number of open workshops organised by partners of the cluster, as well as a number of bi-/tri-lateral meetings and exchange visits between partners. Here we give logistic information of the meetings and workshops and refer to the deliverables of activities within the cluster for more detailed information and information about exchange visits.

Cluster Meeting: ARTIST2 Test and Verification Cluster Meeting. April 20-21, 2006, Embedded Systems Institute, Eindhoven.

ARTIST2 Summer School on Components & Modelling, Testing & Verification, and Static Analysis of Embedded Systems. Nässlingen, Swenden, September 2005.

Workshop: SENVA Meeting on Parallel and Distributed Verification CWI, Amsterdam, The Netherlands, April 3-4, 2006-09-19

Workshop : Specification and Verification of Secure Embedded Systems. Pisa, Italy- May 18, 2005.

Workshop: 2nd Workshop on Formal and Computational Cryptography (FCC 2006) Venice, Italy - July 9, 2006.

Workshop: FORMATS 2005. Paul Pettersson and Wang Yi organized and chaired FORMATS 2005. Uppsala, Sweden, September 29 - October 2, 2005.

Workshop: Control and Observation of Real-Time Open Systems (CORTOS) Affiliated with the 17th International Conference on Concurrency Theory, 30. August, 2006.

Workshop: Parallel and Distributed Model Checking (PDMC). Affiliated with the 17th International Conference on Concurrency Theory, 30. August, 2006.

Workshop: German Verification Day (GVD) Affiliated with the 17th International Conference on Concurrency Theory, 30. August, 2006.

Workshop: 4th International Workshop on Formal Aspects in Security and Trust. Hamilton, Ontario, Canada, August 26-27 2006.

Workshop: FORMATS 2006. Patricia Bouyer and Eugene Assarine organized and chaired FORMATS 2006, Paris, September 2006.

4. Overall Assessment and Vision for the Cluster

4.1 Assessment

Each research activity within the cluster has demonstrated a high level of affinity in goals pursued boding for successful integration of the research carried out by the individual partners.

The cluster integration activities within *Quantitative Testing and Verification* and *Verification of Security Properties* have been particularly active during this second 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. For both activities the objectives for the second year has been fully met and a number of new challenging directions has been initiated.

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. The objective of designing a joint infrastructure for a European verification grid has been addressed via two European meetings on parallel and distributed model checking. Though there are a number of European projects applying high-performance and Grid-based computing to model checking, these projects are dependent on design decision still to be made by the Grid-computing community at large. Thus establishing a common infrastructure will be postponed for the time being. However, the established link to European Grid projects checking (in particular involving INRIA Rhone-Alpes (France), Technical University Eindhoven and CWI (The Netherlands)).on verification will be maintained through regular meetings in order to pursue the overall vision of a powerful computing facility. Within ARTIST2, the challenge for establishing high performance resources will be pursued by exploiting resources that are immediately available, like e.g. the NorduGrid facility, which has two clusters in Aalborg that may be applied for experiments. In particular, the distributed version of Uppaal and the Devine tool will be made available on the 50-node PC cluster, and experiments will be made for exploiting the 52 Gbyte shared memory facility for analysing large models by single-CPU tools.

The activities within Quantitative Testing and Verification and Verification of Security properties are largely carried out by disjoint groups of people (not research institutions) resulting in less interaction than first anticipated. The activities within Quantitative Testing and Verification and Testing and Verification Platform are tightly connected, but to achieve critical mass in pursuing the vision of a European Verification Grid it is felt necessary to involve other prominent research teams working actively on the topic of parallel and distributed model checking (INRIA Rhone-Alpes (France), Technical University Eindhoven and CWI (The Netherlands)).

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

4.2 Vision and Long Term Goals

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 the cluster continues its contribution to the bridging of 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 testing and verification methodology with a well-integrated chain of tools applied in industrial practice is a long-term vision of the cluster.

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

4.3 Future Work and Evolution

4.3.1 Technical Description

It is overall important that the partners continue their effort on improving existing methods and their proprietary tools.

Given the limited resources available within ARTIST2 it is paramount that substantial, additional European funding is obtained to support the man-power required to fully transform the research ideas and prototype tools into an industrial testing and verification practice with a supporting collection of tools integrated with existing industrial tool chains.

On the technical level the work within the following 18 months period (September 2006-February 2008) will involve the following:

- **Quantitative Testing and Verification:** The planned work includes continuation of metrics for testing coverage, abstraction methods and compositional methods allowing properties of a composite system to be inferred from those of its components.

Also, based on existing powerful (real-time) verification techniques the new research challenges identified within the second year will be continued in the next period. This includes 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.

- **Verification of Security Properties** The verification of more realistic protocols including group protocols and lifting the verification to the level of service properties.. The verification of more realistic security properties including not only secrecy and authentication, but also anonymity properties and stronger versions of secrecy. Finally, bridging the gap between the verification of security properties and trust management is part of the future work.
- **Testing and Verification Platform for Embedded Systems** The work on tool evaluation through industrial case studies will be continued as well as links to stable and mature versions of the tools will be provided and updated for download. The challenge for

establishing high performance resources will be pursued by exploiting resources that are immediately available, and established links to European Grid projects on verification will be maintained through regular meetings.

For more detailed technical description we refer to the deliverables for the individual activities within the cluster.

4.3.2 *Current and Future Milestones*

The future milestones planned are as follows:

Year3:

Quantitative Testing & Verification

- Development of algorithms and implementation of tools for optimal controller synthesis, robust model checking, coverage-based test selection and code generation.
- Existing verification tools and test generation tools are more strongly connected, including stronger links between academic and industrial tools.

Verification of Security Properties

- Development compositional proof techniques for verifying services security properties, and for verifying group protocols.

Testing and Verification Platform for Embedded Systems

- Links to the tools developed and applied by the partners will be collected at a common web entry. Also, it will be analysed whether a common web interface can be provided for tool invocation in a trusted and controlled manner. This is a revision of the above milestone on providing a single powerful server for all tools.
- The ongoing work on tool evaluation through case studies will be continued and made accessible at the open repository. Also, links to mature version swill be provided via the Yahoda tool homepage. This is a revision of the above milestone on links to mature versions.
- Further experiments on exploiting contemporary technologies (GRID and PC clusters) will be made. This includes experiments on establishing tool access on available sites (e.g. NorduGrid) as well as further development of distributed model checkers.

Year4:

Quantitative Testing and Verification

- Development of generic framework using abstraction and compositionality for efficient analysis of quantitative models.
- Emergence of a range of new powerful debugging and analysis based on various combinations of testing and verification techniques.

Verification of Security Properties


- Design monitoring procedures for ensuring trust in services execution.


Testing and Verification Platform for Embedded Systems


- Integration of results from the related Joint Research Activities

5. Cluster Participants


5.1 Core Partners


Cluster Leader Activity Leader for “Testing and Verification Platform for Embedded Systems” Team Leader for Aalborg on the activities “Testing and Verification Platform for Embedded Systems” and “Quantitative Testing and Verification”	
	Professor, Director Kim G. Larsen (Aalborg) http://www.cs.aau.dk/~kgl/
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”.


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

Assistant for the Cluster Leader	
	Dr.Arne Skou (Aalborg) http://www.cs.aau.dk/~ask/
Technical role(s) within	Takes part in the cluster coordination; contributes with expertise on

Artist2	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) http://www.ulb.ac.be/di/ssd/jfr/
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) http://www.montefiore.ulg.ac.be/~pw/
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) http://mtc.epfl.ch/~tah/
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.
--	--


Team Leader for INRIA on the activities “Testing and Verification Platform for Embedded Systems” and “Quantitative Testing and Verification”	
	Scientific Leader Thierry Jeron (INRIA) http://www.irisa.fr/prive/jeron/
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.


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


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

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

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

Activity Leader for “Quantitative Testing and Verification” Team Leader for Twente on the activities “Testing and Verification Platform for Embedded Systems” and “Quantitative Testing and Verification”	
	Professor, Director Ed Brinksma (University of Twente/Embedded Systems Institute) http://wwwhome.cs.utwente.nl/~brinksma/
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.

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

Team Leader for Uppsala on the activities “Testing and Verification Platform for Embedded Systems” and “Quantitative Testing and Verification”	
	Professor Wang Yi (Uppsala) http://user.it.uu.se/~yi/
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.

Team Leader for Verimag on the activity “Verification of Security Properties”	
	Professor Yassine Lakhnech (Verimag) http://www-verimag.imag.fr/~lakhnech/
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.

5.2 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.

5.3 Affiliated Academic Partners

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

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