Network of Excellence

IST-004527 ARTIST2:
Embedded Systems Design

Activity Progress Report for Year 1

JPRA-Platform:

Testing and Verification Platform for Embedded Systems

Activity Leader:

Kim Larsen (Aalborg University)

Construction of powerful analysis tools by establishing a joint server platform providing extraordinary computational resources for conducting large-scale verification and testing efforts for embedded systems with respect to real-time requirements, quality-of-service guarantees as well as security properties.

The platform will provide a uniform, open and secure access and to all testing and verification tools of the academic as well as industrial partners of the consortium. The platform builds on existing works from the various partners and will also make available new powerful analysis tools developed within the network, in particular those from the related Joint Research Activities ("Quantitative Testing and Verification" and "Verification of Security Properties").

Table of Contents

1. Introduction

1.1 Activity Leader

Team Leader: Kim G. Larsen (BRICS/Aalborg)
Areas of his team's expertise: verification and testing of real-time systems.

1.2 Policy Objective

Construction of powerful analysis tools by establishing a joint server platform providing extraordinary computational resources for conducting large-scale verification and testing efforts for embedded systems with respect to real-time requirements, quality-of-service guarantees as well as security properties.

The platform will provide a uniform, open and secure access and to all testing and verification tools of the academic as well as industrial partners of the consortium. The platform builds on existing works from the various partners and will also make available new powerful analysis tools developed within the network, in particular those from the related Joint Research Activities ("Quantitative Testing and Verification" and "Verification of Security Properties").

1.3 Industrial Sectors

Immediate applications in aerospace, railway transport, automotive and telecommunication.

Long-term applications in virtually all industrial sectors.

2. Overview of the Activity

2.1 Artist Participants and roles

Team Leader: Ed Brinksma (University of Twente)
Areas of his team's expertise: verification and testing of reactive and stochastic systems.

Team Leader: Pierre Wolper (Centre Fédéré de Verification)
Areas of his team's expertise: model checking.

Team Leader: Philippe Schnoebelen (LSV)
Areas of his team's expertise: model checking.

Team Leader: Thierry Jeron (INRIA)
Areas of his team's expertise: testing theory and tools.

Team Leader: Yassine Lakhnech (Verimag)
Areas of his team's expertise: infinite state model checking.

Team Leader: Wang Yi (Uppsala)
Areas of his team's expertise: model checking for real-time systems.

2.2 Affiliated partners and Roles

Team Leader: Lubos Brim (University Brno)
Areas of his team's expertise: distributed model checking.

Team Leader: Henrik Leerberg (IAR Systems A/S)
Areas of his team's expertise: tool provider.

Team Leader: Tommy Ericsson (Telelogic)
Areas of his team's expertise: tool provider.
Team Leader:
Tom Henzinger (EPFL)
Areas of his team's expertise: model checking of embedded software and hybrid systems.

Team Leader: Sven H. Sørensen: (Siemens Mobile Phones A/S)
Areas of his team's expertise: end user.

Team Leader: Thomas Hune: (Terma A/S)
Areas of his team's expertise: end user.

2.3 Starting date, and expected ending date

September 1st, 2004 to September 1st 2005

2.4 Baseline

The teams collaborating on this activity are leading tool providers for testing and verification, with particular emphasis on real-time, hybrid and stochastic aspects.

Automatic analysis of such quantitative aspects are crucial in validating embedded systems, but are computationally significantly more difficult than validation of simple functional aspects.

Thus, to address industrial size models continued development of new algorithmic techniques and data structures should be combined with powerful computational resources. We seek to establish this by maximal use, coordination and extension of existing local resources (e.g. PC-clusters) and by exploiting on-going work on exchange between and combinations of tools.

2.5 Technical Description

Despite advances in algorithmic techniques verification and test case generation are computationally notoriously hard problems.

Consideration of quantitative phenomena (real-time, stochastic) adds to the complexity. Thus, to address industrial size models powerful computational resources are necessary for example by maximal coordination of existing local resources.

The computational resources of the platform will initially be provided by existing powerful stand-alone computers with the various verification and testing tools being made available via a common web-based interface. A procedure for controlling access in a flexible and secure (e.g. in accordance with the individual tools licence agreements) manner will be designed.

Among the tools that will be made available we mention: SPIN, SMV, UPPAAL, Kronos, Blast, TorX, TGV, FAST, CADP, IF; HyTech, visualSTATE, TAU, LASH, EMTCC and Rapture where the individual consortium member will have responsibility for integrating their tools into the platform.

The emerging advances in parallel and distributed model checking also motivate the development of a generally accessible server platform consisting of local clusters of (inexpensive) PCs.

Long term vision includes an experimental GRID infrastructure targeted specifically towards verification and testing.

3. Activity Progress Report

3.1 Work achieved in the first 6 months

The following work has been achieved during the first 6 months:

- Twente has made definite plans for establishing a verification cluster shared between three research groups at the University which can be part of a European grid.
- The Vertecs team ()IRISA) supports two test generation tools : TGV and STG. During the period, a new version of TGV (based on on-the-fly enumerative algorithms) linked to the IF toolbox (Verimag) has been developed using STL libraries (in place of CADP libraries).
- A general distributed verification environment (DiVinE, Brno) has been deployed. The environment supports the development of distributed enumerative model checking algorithms, enables unified and credible comparison of these algorithms, and makes the distributed verification available for public use in a form of a distributed verification tool.
- Results have been implemented in the TIMES tool for automated schedulability checking.
- A number of improvements have been made on the Uppaal real-time model checker (www.uppaal.com). This includes the possibility to enrich the timed automaton models with C code. This has given an important increase in the expressiveness of the modelling tool, e.g. the possibility to include advanced data types. During the period, the tool has been applied for off-line test generation on a connectivity testing framework.

3.2 Work achieved in months 6-12

The following work has been achieved during the first year period:

- Verimag develops the IF-tool set.
- A new version of STG (symbolic test generation and execution tool based on syntactic transformation guided by an approximate analysis) in OCAML is under development at IRISA.
- DiVinE (Brno) has been extended with a Promela front-end for SPIN compatible distributed model checking.
- CFV supports the verification tool LASH and hosts powerful servers dedicated to verification tools.
- An extension of Uppaal (Uppaal Cora), dedicated to solving optimal scheduling and planning problems, has been introduced. This version is based on a version of the classical timed automaton formalism extended with auxiliary cost variables and with a modified version of the Uppaal verification engine to take the accumulation of cost into account. During the period, several new algorithms have been designed, and they will be introduced in forthcoming versions of the tool.
- Recently, a version of Uppaal (Uppaal Tron), dedicated to online testing of real time systems, has been announced. By using Uppaal Tron, one can extend the testing power of traditional tools substantially, partly because one can run tests for a very long

time, and also because Uppaal Tron gives the possibility to build various stochastic criteria into the test selection algorithm. During the period, furhter tools improvements have been made, and also a first realistic industrial case study has been made. .

3.3 Recommendations

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)). A meeting in the autumn, 2005, will take place at INRIA Rhone-Alpes (host: Hubert Garavel) for taking steps towards such a coordinated initiative.

3.4 Milestones

It is difficult to point to just a single or few selected milestones achieved by the activity. Rather – as can be seen by the description of the work during the first year and the extensive list of publications – a large number of results has been obtained both on the significant improvement of individual tools and on making the tools generally accessible via a common web portal (the Yahooda web-page maintained by Brno).

3.5 Main Funding

Main sources of funding are

Funding from various national funding agencies and centres, such as:

- the Centre for Embedded Systems,
- CISS (http://ciss.auc.dk/),
- BRICS (http://www.brics.dk/),
- Dutch national projects STRESS, HaaST, IMPASSE, MC=MC, CASH (see http://fmt.cs.utwente.nl/),
- Swedish national projects SAVE, ASTEC,
- Czech project on distributed model checking: Paradise.

Funding from ongoing EU projects, in particular the AMETIST
IST-project 2001-35304 on Advanced Methods for Timed Systems
(http://ametist.cs.utwente.nl/).

Funding from the IST AGEDIS project – Automatic generation of test cases.

3.6 Indicators for Integration

The establishment of a joint server with access to all tools turned out to be too ambitious during the first 18 months. Instead, the partners have made information about their tools available on the Yahoda database (run by the affiliated partner at Brno). Also, the cluster has initiated European work on methods for Parallel and Distributed Model Checking jointly with research groups outside the cluster. Part of this work will include the definition of a coordination middleware layer to support tool development for distributed model checking.

3.7 Evolution

During the first 18 months, the partners have evaluated their tools thoroughly through a number of major industrial case studies. Also, a number of improvements have been implemented on the individual tools as mentioned above. It is planned that downloadable and stable versions will be made available through the Yahoda database.

4. Detailed Technical View

4.1 Brief State of the Art

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 first year the partners of the cluster have been active in developing, maintaining and disseminating of a number of testing and verification tools allowing for the analysis of quantitative models including real-time models, resource models, hybrid models and stochastic models:

Timing aspects:

- UPPAAL offers analysis and simulation of timed automata.
- IF allows for analysis of asynchronous timed and untimed systems and offers interface to other tools like UML tools and test generation tools.

Resources:

- UPPAAL Cora allows analysis and solution of optimal scheduling and planning problems given *priced* extended timed automata models.

Data & parameterised systems:

- LASH has focus on the (symbolic) analysis of systems with an infinite state space.

Schedulability analysis and schedulability synthesys:

- TIMES offers schedulability analysis and worst-case analysis.
- UPPAAL Tiga, has focus on time optimal controller synthesis
- Taxys combines the timed analysis facilities of Kronos with code generation from the Esterel tool

Hybrid phenonomas:

- The TreX has been applied for the study of hybrid automata and rectangular refinement of affine hybrid systems.

Stochastic phenomenas:

- The MODEST modelling formalism and the Moebius toolhas been applied for the analysis of stochastic phenonoma of an industrial case (self- configuring networks).

Testing:

- TGV offers the synthesis of test conformance test cases from automata specifications
- UPPAAL Tron and TorX offer on-line testing of reactive timed and untimed systems based on automata models.

Security aspects:

- The general approach so far for verifying security protocols, has been to apply existing model checking tools. A numbe rof case studies exist.

Verification is a computationally hard and memory intensisve activity in general. Verification and analysis of embedded systems models are computationally hard in particular as the underlying models contain quantitative aspects in order to enable reasoning about timeliness, expected resource consumption and performance of a given design. Therefore – to be successful and to fully realize the potential of a given verification technique – one must optimally utilize the architectural features of the platform on which the underlying algorithms are implemented. This includes e.g. memory size, communication delay, processor speed, etc. This has led to a new research discipline on distributed model checking, where the aim is to adapt existing model checking algorithms (and also to invent new distributed algorithms) to exploit modern architectures like grid systems in a dedicated manner. The partners are very active and collaborate on this subject.

4.2 Industrial Needs and Experience

Due to the growing complexity of modern embedded systems, the need for tools for automizing the generation and execution of test cases has become enormous. Although promising tools are emerging for testing purely functional properties, there is a total lack of tool support for the testing of quantitative aspects like e.g. real time properties. This means that testing now has become a bottleneck for most companies developing embedded systems, because it is precisely the quantitative aspects that characterise such systems. Often there has to be made a choice between releasing a poorly tested product (with the risk of bad reputation) or delaying the release date (risking loss of market shares).

4.3 Ongoing Work in the Partner Institutions

The group at CFV supports the verification tool LASH and hosts powerful servers dedicated to verification tools.

Verimag develops the IF-tool set.

The Vertecs team supports two test generation tools : TGV and STG. During the period, a new version of TGV (based on on-the-fly enumerative algorithms) linked to the IF toolbox (Verimag) has been developed using STL libraries (in place of CADP libraries). A new version of STG (symbolic test generation and execution tool based on syntactic transformation guided by an approximate analysis) in OCAML is under development.

OFFIS has performed the necessary integration work for various modelling tools, including the ASCET-SD tool from the company ETAS.

Uppsala has worked on algorithms for schedulability analysis and the results have been implemented in the TIMES tool for automated schedulability checking.

Aalborg has made a number of improvements on the Uppaal real-time model checker (www.uppaal.com) - most notably the possibility to enrich the timed automaton models with C code. Also, a version of Uppaal (Uppaal Tron), dedicated to online testing of real time systems, has been announced recently.

Aalborg has also implemented a distributed version of Uppaal, which can be executed on a local 50-node PC cluster (part of the Nordugrid facility). This enables fast verification of very large state spaces (up to 70GB of memory).

At Brno, a general distributed verification environment (DiVinE) has been deployed. It has also been extended by a Promela front-end for SPIN compatible distributed model checking.

Twente is working on the establishment of a verification cluster shared between three research groups at the University of Twente, which can form
part of a European grid.

4.4 Interaction, Building Excellence Between Partners

The regular interaction within the cluster makes it possible for each partner to focus on the special facilities and algorithms of his 'own' tool, while at the same time being kept up to date wrt. new ideas of the partners' tools. Also, it enables collaboration on common problems and algorithms of the tools, like e.g. how to efficiently support distributed model checking, how to efeciently represent symbolic data strucutes, etc.

The growing number of affordable, yet powerful, local PC-clusters has made parallel and distributed model checking a very active research area. Distributed versions of several tools for verification of untimed systems now exist with the partners of ARTIST2 T&V cluster making major contributions. It has therefore been decided to collaborate on the establishment of a joint distributed model checking facility.

4.5 Spreading Excellence

In the area of parallel and distributed model checking of embedded systems we are in close collaboration with other research teams in Europe (INRIA Rhtne-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.

The partners are all part of additional research networks outside Artist2, where the platform results are discussed and evaluated. Especially, there is a large world-wide research community working on (purely finctional) model checking and run-time verification, which can benefit from the results on tool support for quantitative testing and verification. Clearly, this also holds for tool developing companies.