Year 4 Review
Dresden, March 16th, 2012

Cluster

Achievements and Perspectives:

Modeling and Validation

Cluster Leaders:
Kim G. Larsen, Aalborg University
Susanne Graf, Verimag
Core Teams (Modeling & Validation)

- **Kim Larsen (Aalborg – Denmark)**
  - Timed automata based models. Performance analysis and synthesis.

- **Susanne Graf (VERIMAG – France)**
  - Component-based design. Extra-functional properties.

- **Tom Henzinger (IST - Austria)**
  - Rich Interfaces. Quantitative properties and resources.

- **Thierry Jéron (INRIA – France)**
  - Model-based testing, control synthesis

- **Martin Törngren (KTH - Sweden)**
  - Integrated models and validation.

- **Christoph Kirsch (Salzburg - Austria)**
  - Timing and reliability modeling.

- **Wang Yi (Uppsala - Sweden)**
  - Resource modeling and timing analysis.

- **Joseph Sifakis (VERIMAG - France)**
  - Component-based design. Structural verification

- **Sébastien Gérard, Christophe Gaston (CEA LIST - France)**
  - Model-based engineering, standard modeling.

- **Jozef Hooman (ESI - Netherlands)**
  - Quantitative modeling and testing.

- **Boudewijn Haverkort (ESI, Netherlands)**
  - Quantitative Modeling

- **Werner Damm (OFFIS - Germany)**
  - Component-based design and semantic foundation.

- **Alberto Sangiovanni-Vincentelli Roberto Passerone (Trento - Italy)**
  - Platform-based design.

- **Bengt Jonsson (Uppsala - Sweden)**
  - Component-based mod. & ver.
Affiliated Teams

- Henrik Lönn, Volvo Technology
- Jacques Pulou, France Telecom
- Roderick Bloem, TU Graz
- Koos Rooda, TU Eindhoven
- Paul van den Hof, TU Delft
- Tiziana Villa, Uni. Verona,
- Pierre Wolper, CFV, Belgium
- Yiannis Papadopolis, Uni. of Hull
- Ahmed Bouajjani, LIAFA
- Stavros Tripakis, University of California at Berkeley, USA
- Jean-Francois Raskin, CVF, Belgium
- Joost-Pieter Katoen, Aachen
- Holger Hermanns, U. of Saarland
- Christel Baier, Dresden
- Patricia Bouyer, Nicolas Markey, Philippe Schnoebelen, LSV Cachan
- Wil van der Aalst, TU Eindhoven
- Frits Vaandrager, Radboud U. Nijmegen
- Mehmet Aksit, Twente University

+ several industrial partners at national levels.
High-Level Objectives and Vision

- Establish a coherent **mathematically sound family** of design flows spanning the areas of computer science, control, and hardware based on model- and component-based theories, methods, and tools:
  - **model-based**, to achieve portability
  - **component-based**, to achieve scalability
  - **analyzable** (deterministic, ..), to achieve predictability
  - **tool-chains** cost-efficient development, early design-space exploration

- Requires a new scientific foundation
  - new **abstractions** for computing as a physical, imperfect act
  - from Boolean correctness to **quantitative robustness** measures: failure rate, life time, input tolerance, etc.

- Impact on **safety critical industries** (aerospace, automotive) as well as **high volume systems** (professional systems, consumer electronics).
Overview of Cluster Activities

MODELING
Susanne Graf (VERIMAG)

VALIDATION
Kim G. Larsen (Aalborg)

- Component Modeling
- Resource Modeling
- Quantitative Modeling
- Compositional Validation
- Quantitative Validation
- Cross-layer Validation
High-Level Objectives and Vision

MODELING

Susanne Graf (VERIMAG)

VALIDATION

Kim G. Larsen (Aalborg)

Robust
Probabilistic
Hybrid
Automata

pushing it further

Pareto frontier

Statistical MC
Compositionality
Efficiency
Integration achieved in Europe

- **Extensive collaboration** between partners of the cluster
- **Extensive collaboration** with leading research teams outside Europe.
- **Extensive interaction** with other communities

**Some Examples of collaborations:**
1. CEA+VOLVO+KTH: ATESST2 and its continuation MAENAD on MARTE, SysML & AutoSAR
2. CESAR partners work towards a common meta-model
3. COMBEST compositional verification
4. SPEEDS system level validation techniques
5. Uppsala & ETHZ on multi-core architecture
6. INRIA, Aachen, CISS work on compositional design methodologies for quantitative models.
7. CISS & Verimag on probabilistic duration automata.
8. IST and VERIMAG, CISS and LSV work on robustness
9. IST and CVF, LSV and CISS work on energy games!
10. ESI+TUB guest editors for special issue of ACM Trans. in Embedded Computing Systems
Integration achieved in Europe

- **National Centers and projects**
  - CISS, ESI, ...
  - DaNEx, DOTS, Testec, ICES, ...

- **Common FP7/ARTEMIS Projects**
  - Pro3D (STREP)
  - SMECY (ARTEMIS)
  - ACROSS (ARTEMIS)
  - SYMSMODEL (ARTEMIS)
  - VERDE (ITEA)
  - RECOMB (ARTEMIS)
  - MBAT (ARTEMIS)

  and others: QUASIMODO (STREP), MULTIFORM (STREP), COMBEST (STREP), GASICS, CESAR, GENESYS, ADAMS, ATTEST2, SPEEDS (IP), CREDO, ...

- **Tool Integration**
  Projects ATTEST, Combest, Multiform, Quasimodo lead to tool integration involving Uppaal, BIP, Forsyth, POOSL, MoDEST, CPNTools, METROPOLIS, Papyrus + Diversity ao. with usage in industry,
Building Excellence

- **155 publications (Y4)**
  (Y1 156, Y2 150, Y3 146)
- **50 joint publications (Y4)**
  (Y1 47, Y2 46, Y3 40)
- **3 Best Paper Awards Y4**
  FACS11, RTETAS11, FNRAE11
- High level of **dissemination**
  through PhD schools and industrial seminars (>40 keynote presentations).
- **Strong impact**
  on a number of important international **conferences**
  (CAV, TACAS, FORMATS, EMSOFT, CONCUR, ETAPS, HSCC, FMCAD)
- **Transfer to industry**
  long-term collaboration performed by individual partners.
  National centers and laboratories.
Conferences and Workshops Organized

- Special session on Robustness (with contributions from ARTIST Design partners)
- 2\textsuperscript{nd} QMC PhD school
- Yearly ESI Symposium (dissemination to industry)
- Workshop on Quantitative Models and Tools, DATE 2012
- The European Conference on Computer Systems (EuroSys 2011), University of Salzburg, Salzburg, Austria
- Green and Smart Embedded System Technology: Infrastructures, Methods and Tools at the Cyber-Physical System Week
- 9th International Conference on Formal Modeling and Analysis of Timed Systems, FORMATS 2011
- 3rd Workshop on Games for Design, Verification and Synthesis
Conferences and Workshops Organized (Cont)

- Special Session on Real-Time and Networked Embedded Systems, IEEE Transactions on Industrial Informatics (to be published in May 2012)
- ACM/IEEE Ninth International Conference on Formal Methods and Models for Codesign (Memodode 2011)
- EUROSYS 2011 (ARTIST workshop Axel)
- Special session on virtualisation of embedded systems at DAC 2011 and for probabilistic embedded systems at DAC 2012
- INRIA Rennes Gipsy Workshop on Games, Logic and Security

Grants & Awards

- ERC grants: J-F Raskin, K Chatterjee, Tom Henzinger
- NSF grant with Berkeley: Chistoff Kirsch
- Pressburger Award 2011: Patricia Bouyer
Achievements Y4

**Modeling**

- Component Modeling & Compositional Validation
  - Component-based design frameworks (functional, timing and stochastic aspects)
  - Component adaptation
  - Coordination Languages
  - Tool Integration (meta-models and model-transform.)

- Resource Modeling
  - Multi-core scheduling
  - Design-space Expl.
  - Dist. Impl from global spec.

- Quantitative Modeling
  - Weighted automata
  - Priced TA
  - Quantitative communication models.
  - Quantitive properties for non-quantitative models.

**Validation**

- Quantitative Validation
  - WCET analysis and Schedulability analysis
    - Digraphs
  - Combinations of AI and MC
  - Analysis of parametric models
  - Statistical model checking
  - Metrics

- Cross-layer Validation
  - Model-based testing
  - From models to code
  - Learning.
Scientific Highlight Y4
Model-Based Testing

Model-Based Testing

SUT conf model

exhaustive sound

SUT passes tests

model-based test generation

system model

conf

test execution

SUT

pass fail

pass fail
Model-Based Testing: A Wireless Sensor Network Node

MYRIANED “GOSSIP”
Medium Access Protocol: gMAC
Model-Based Testing:

A Wireless Sensor Network Node

SUT

Test cases

Model-based test generation

MBT tool: Uppaal-Tron, TorXakis, JTorX

test adapter

pass

fail

test runs

WSN software on PC

(vague)
descriptions

guru

ad-hoc model learning

• long test runs: > 100,000 test events

• many discrepancies between spec and SUT detected

• incremental development of model
Scientific Highlight Y4

Digraphs

- Branching, cycles (loops), ...
- Allow *arbitrary directed graphs*
  - Vertices $J$: jobs to be released (with WCET and deadline)
  - Edges $(J_i, J_j)$: minimum inter-release delays $p(J_i, J_j)$

- Test *more challenging*, but also efficient:

**Theorem (Our technical result)**

For DRT task systems $\tau$ with a utilization bounded by any $c < 1$, feasibility can be decided in *pseudo-polynomial time.*
Digraphs: The Big Picture

- Task Automata
- DRT
- non-cyclic RRT
- RRT
- non-cyclic GMF
- GMF
- MF
- L&L
- sporadic

- Expressiveness: high
- Expressiveness: low
- Feasibility test: efficient
- Feasibility test: difficult

- Strongly (co)NP-hard
- Pseudo-Polynomial
Digraphs: The Demand Bound Function

- General tool/technique for schedulability analysis: dbf(t)
- Intuition:
  - Given a time interval length $t$
  - $dbf(t)$ bounds the *demand* for processor time within *any* $t$ interval

$$dbf(t) = e_1 + e_3$$
Feasibility Test Using `dbf()`

**Theorem**

A task system $\tau$ is preemptive uniprocessor feasible iff:

$$\forall t \geq 0 : \sum_{T \in \tau} dbf_T(t) \leq t$$

**Challenges:**

1. How to calculate $dbf_T()$?
2. How to check existence of a violating $t$?
Highlight: The BIP Toolbox for rigorous component-based design in practice

Integration of verification and design taking into account heterogeneity of models

http://www.bip-components.com
Refactoring of Software to make it component-based

Functional Layer

Hierarchical decomposition into components

Composition of atomic components using only glue

Description of the behavior of atomic components

B₁, B₂, …, Bₙ-₁, Bₙ

efficient C++ code generation

scalable analysis with D-Finder
Highlight: The BIP Toolbox - Componentization

GenoM/BIP Toolchain

Applied to the DALA Robot

GenoM Models

Codels

BIP Models

D-Finder

BIP Engine
Highlight: The BIP Toolbox – Distributed Implementation

Distributed Mutual Exclusion Protocol

Interaction Protocol for I1
Interaction Protocol for I2
Interaction Protocol for I3

Interface Interface Interface Interface Interface

Distributed Execution Engine

Distributed Implementation
Main Scientific Highlights and Insights Gained

Quantitative Modelling and Validation
- Probabilistic, Timed, Energy Automata and Games

Contracts and Interfaces
- General Contract theory
- Probabilistic contracts
- Real-time modal transition systems.

Model-Based Testing:
- On-line test generation / monitoring, execution and conf. check.
- Compositional approach for RT systems
- Automatic selecting off-the-shelf components
- Randomized emulation of environment model!

Controller and Code Synthesis
- Tool-chain commercial /academic UPPAAL/PHAVer / SIMULINK & BIP w Lustre, Simulink, ..
- Important improvement of existing solutions
IMPACT

Several ARTEMIS projects: ACROSS, CESAR, MBAT, RECOMB, SMECY, ...

Impact on industry in France (Renault, Alstom, Esterelle, Thales, Denmark, (Terma, Novo Nordisk, Danish Industry), Sweden, The Netherlands (Philips Healthcare, OCEASML, Thales,...), Italy ( ), Germany (Daimler, Siemens, ..), ..

High impact tools and platforms: BIP, Forsyth, UML MARTE, UPPAAL

Advances on formalisms and theory for contracts & quantitative modeling
Tools & Platforms

Individual tools (and links)

Scientific Highlight: Component-Based Design

COMBEST & SPEEDS
Tool-chain:
- integration of state-of-the-art tools
- application to case studies

Tool integration
Main Scientific Highlights: Position Papers


G.M. Bonnema, P.D. Borches, *Design with Overview - how to survive in complex organizations*, INCOSE. 2008

G. Muller, *When and What to Standardize; An Architecture Perspective*. INCOSE 2008


Main Scientific Highlights: Position Papers


Ch. Kirsch. *What are visionary and futuristic domains where advances in CPS will have broad impact?* Invited Panelist CPSWEEK 2009, San Francisco


Main Scientific Highlights: Position Papers


J. Sifakis A vision for computer science - the system perspective. – Central Europ. J. Computer Science


Joseph Sifakis Methods and tools for component-based system design. DATE 2011


Lasting Impacts
Future interaction beyond the end of the NoE

Research will be continued within a (large) number or newly funded European projects:

- MBAT (ARTEMIS), ENCOURAGE (Smart Houses & Grid), RECOM (ARTEMIS), DANSE (FP7, IP), OpenETCs (ITEA)
- Dali (Devices for Assisted Living) (FP7, Strep), SCUBA (Energy Aware Buildings), SAFE (Safety standard in automotive industry)

The QMC (Quantitative Model Checking) PhD School will be continued by MT-LAB (DK)

Continued dissemination to industry will (also) be continued at national levels:

- The Netherlands Allegio, Octoplus, Italia (test-based modeling)
- Denmark: CISS / DTU with Danish Industry
- Germany: software platform form embedded systems (continuation in May)
Funding (now and future) is becoming increasingly application driven!

- Increased dynamicity (Cyberphysical, SoS, Complex Adaptive Systems, ..)
- Optimality → Equilibria
- Correctness → Synthesis
Final Overall Assessment

- Integration and networking between research teams with multiple exchange visits.
- Numerous connections between tools
- Dissemination to Industry at several levels
- Awareness of necessity of model-based development (e.g. MBAT, RECOMB)
- Model-Based Testing is really on its way of taking off
END