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).

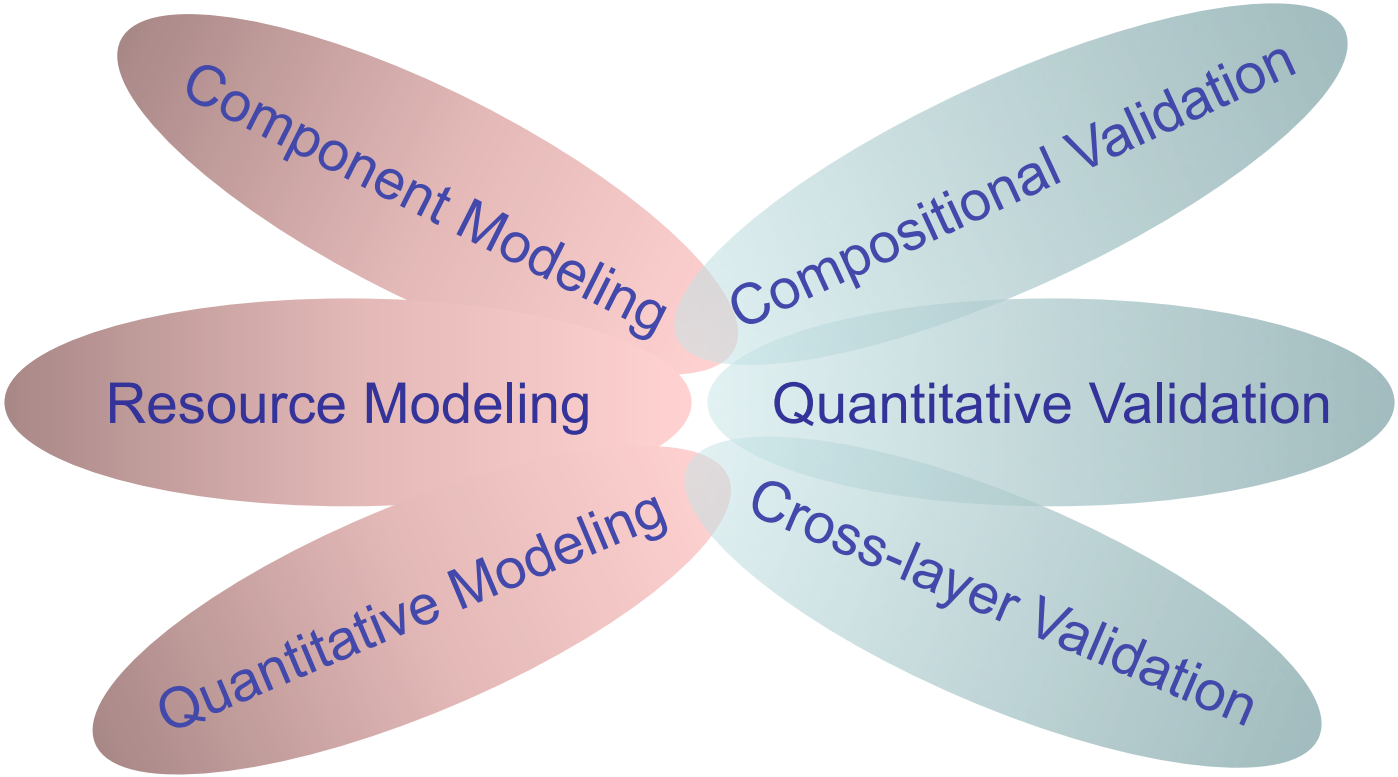
Overview of Cluster Activities

MODELING

Susanne Graf (VERIMAG)

VALIDATION

Kim G. Larsen (Aalborg)



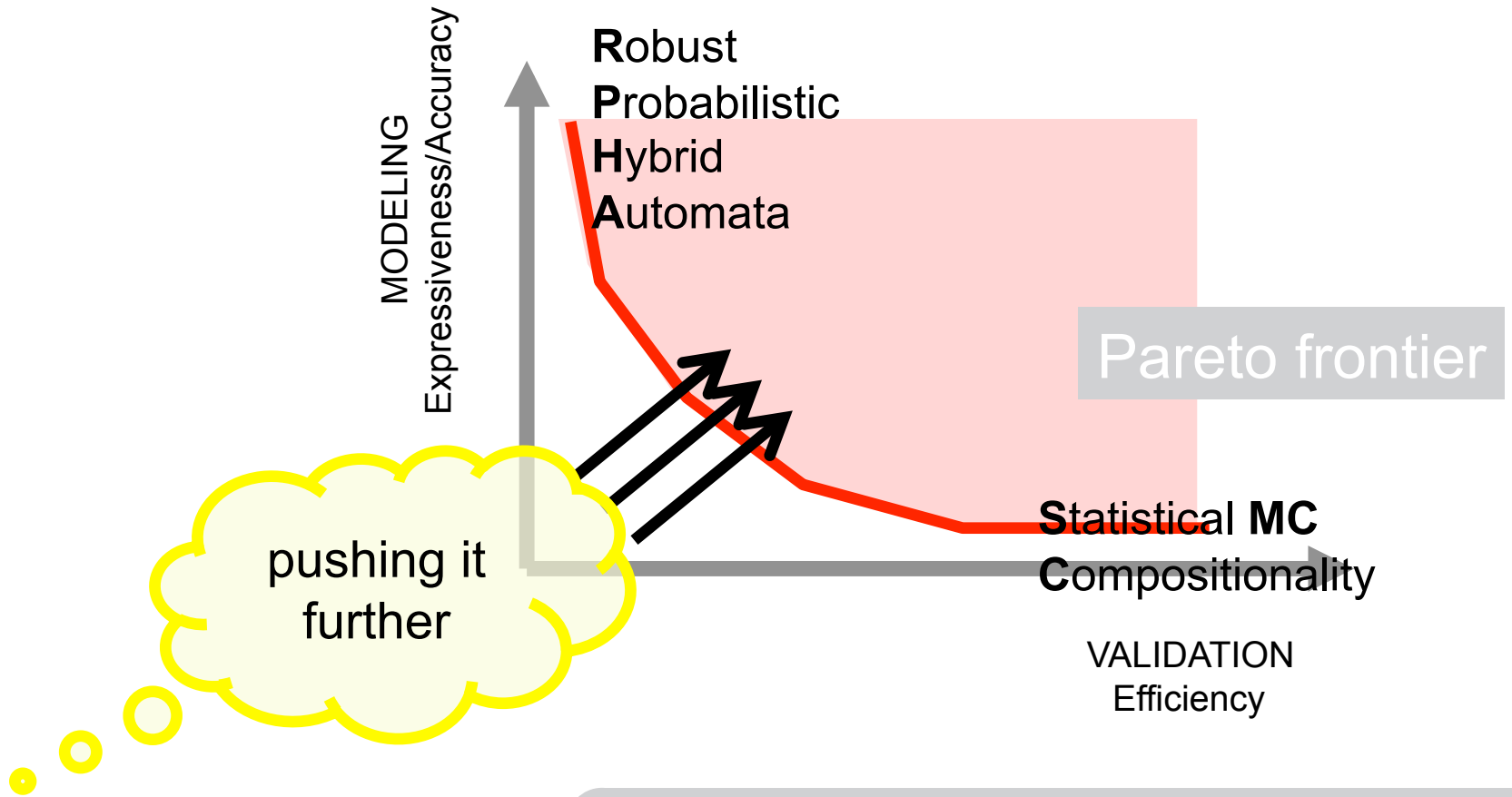
High-Level Objectives and Vision

MODELING

Susanne Graf (VERIMAG)

VALIDATION

Kim G. Larsen (Aalborg)

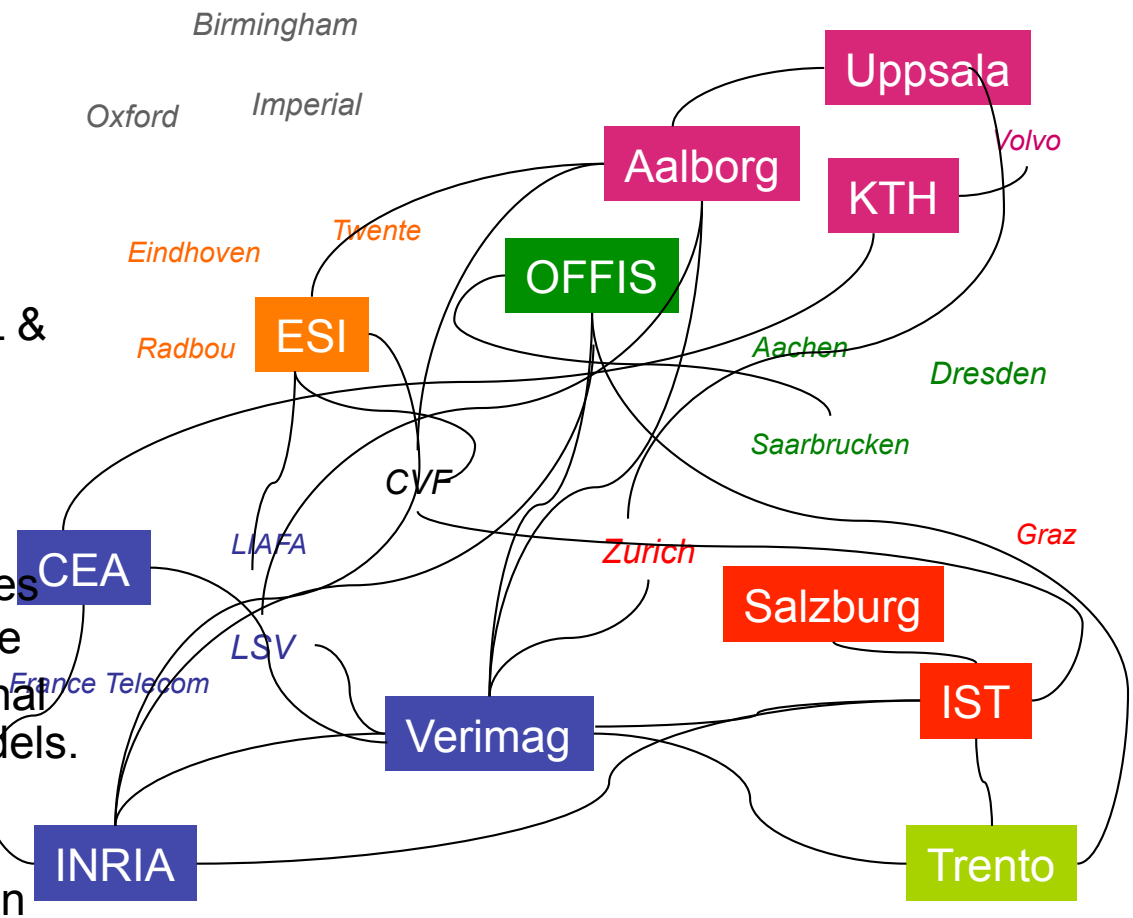


Integration achieved in Europe

- **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

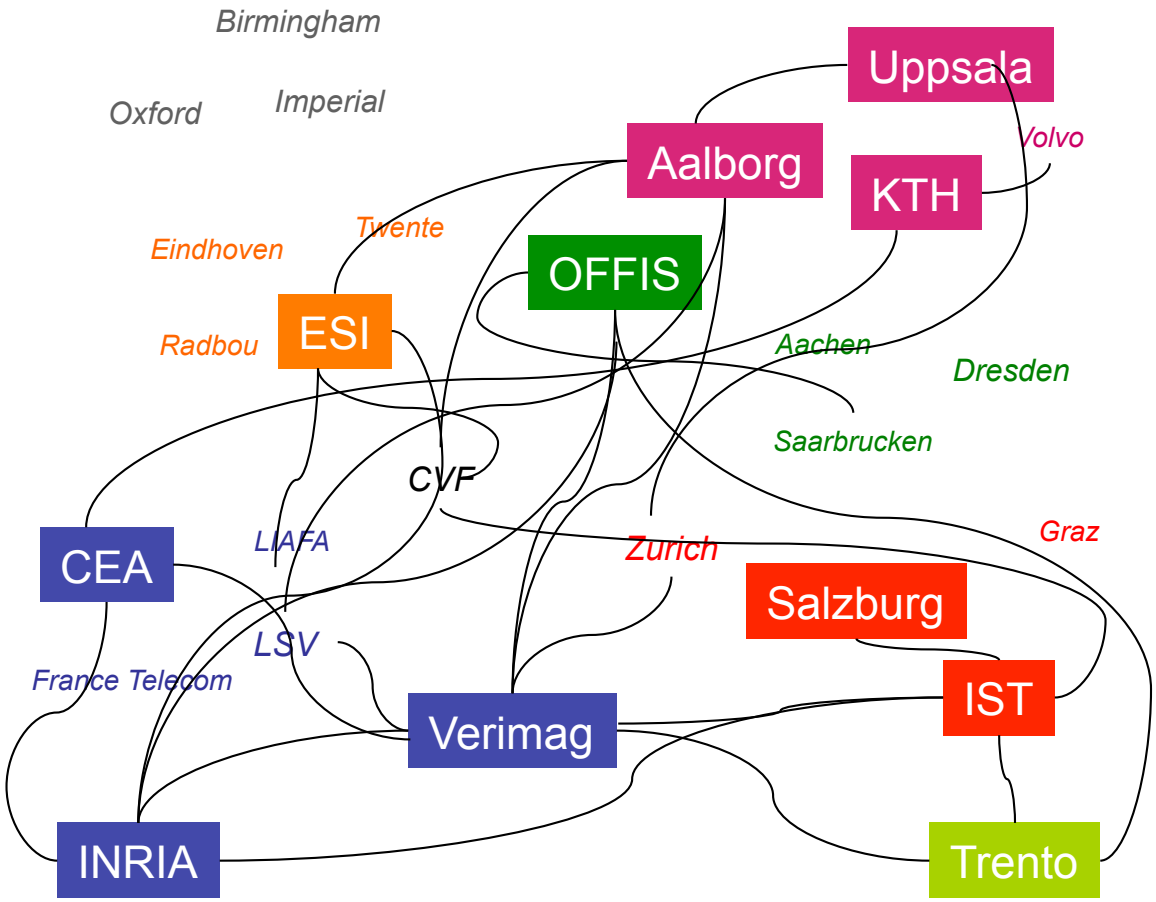


Integration achieved in Europe

- **National Centers and projects**
  - CISS, ESI, …
  - DaNES, DOTS, Testec, ICES, ...
- **Common FP7/ARTEMIS Projects**
  - Pro3D (STREP)
  - SMECY (ARTEMIS)
  - ACROSS (ARTEMIS)
  - SYSMODEL (ARTEMIS)
  - VERDE (ITEA)
  - RECOMB (ARTEMIS)
  - MBAT (ARTEMIS)

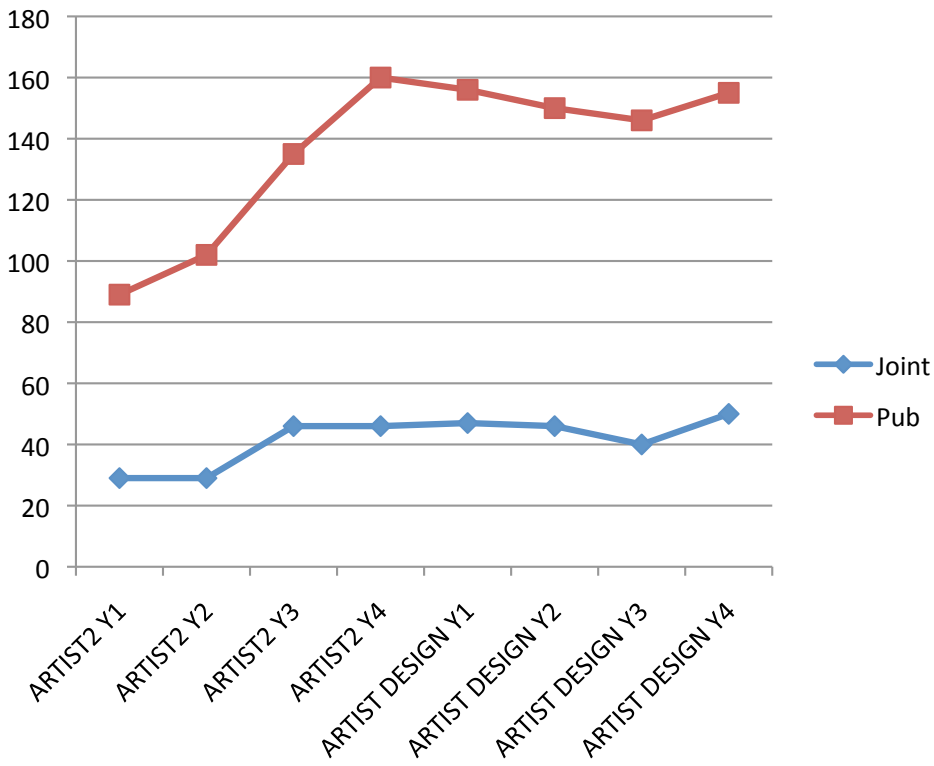
  and others: QUASIMODO (STREP), MULTIFORM (STREP), COMBEST (STREP), GASICS, CESAR, GENESYS, ADAMS, ATTEST2, SPEEDS (IP), CREDO, ...
- **Tool Integration**

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



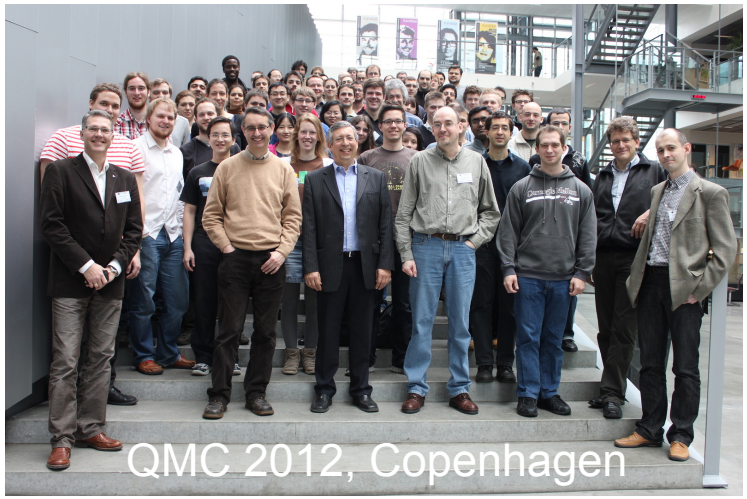
Building Excellence

- **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.



Building Excellence

Conferences and Workshops Organized


QMC 2012, Copenhagen

- The 6th IEEE International Symposium on Industrial Embedded Systems (SIES 2011), SIES Symposium on Industrial Embedded Systems), Västerås, Sweden, June 2011.
- Special session on Robustness (with contributions from ARTIST Design partners)
- 2nd 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

Building Excellence

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

Validation

- 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.

- 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.

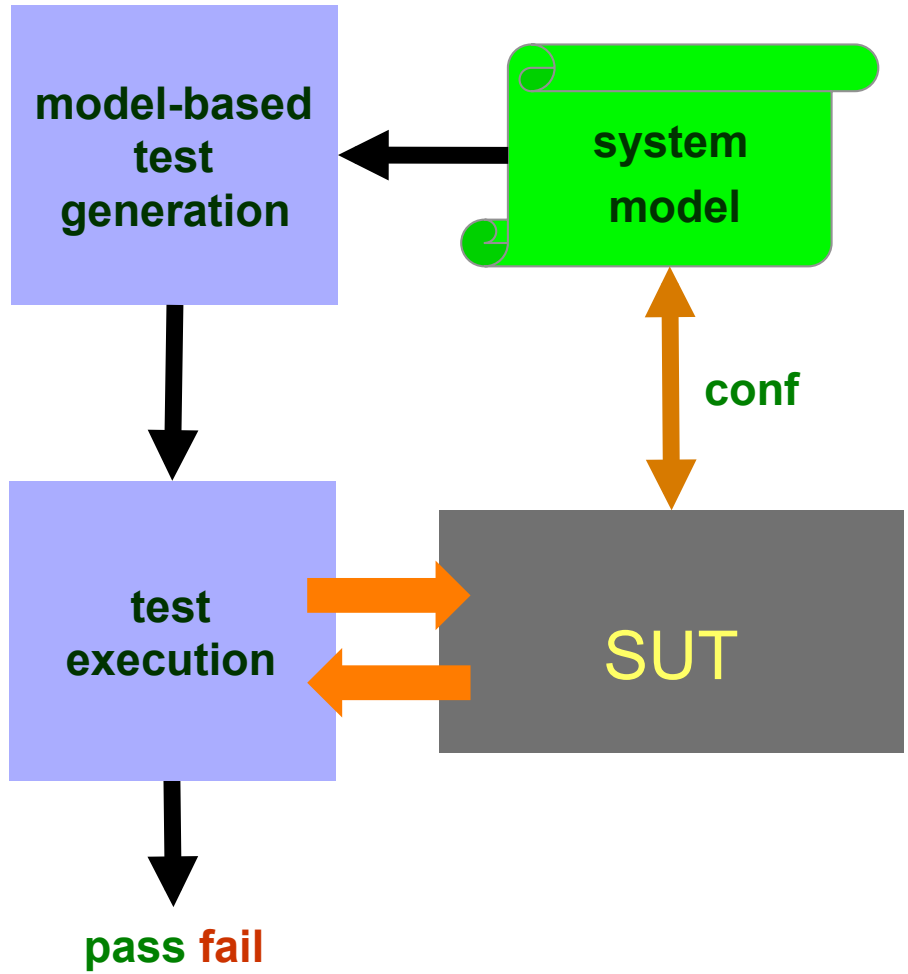
Scientific Highlight Y4
Model-Based Testing

Model-Based Testing

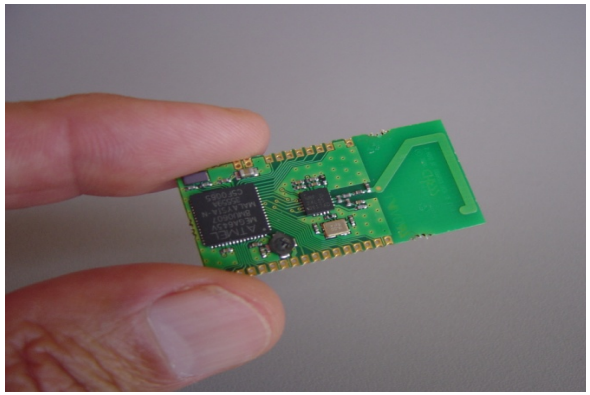
SUT conf model

exhaustive ⇑ ⇓ sound

SUT passes tests

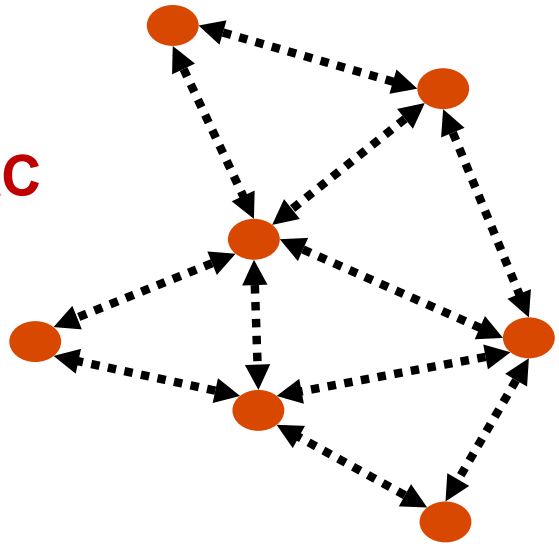


Model-Based Testing : A Wireless Sensor Network Node



MYRIANED “GOSSIP”

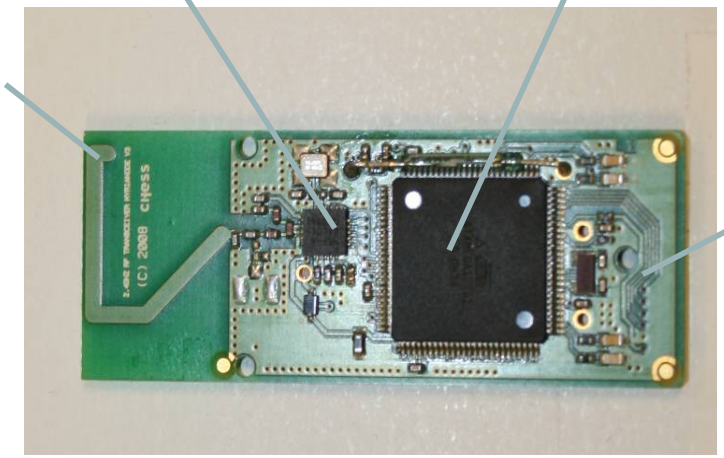
Medium Access Protocol: gMAC



RF TRANCEIVER (NORDIC SEMI)

CPU (ATMEL XMEGA128)

RF ANTENNA



I/O INTERFACES

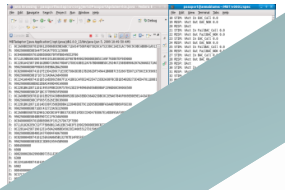
Model-Based Testing
A Wireless Sensor Network

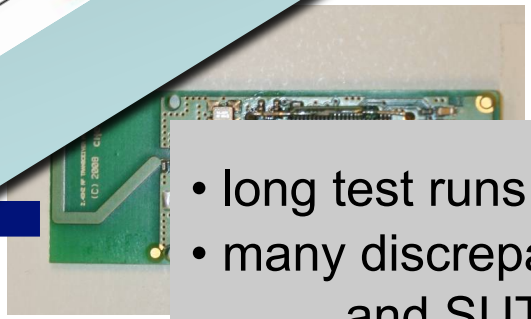
MBT tool:

Uppaal-T

T

test runs





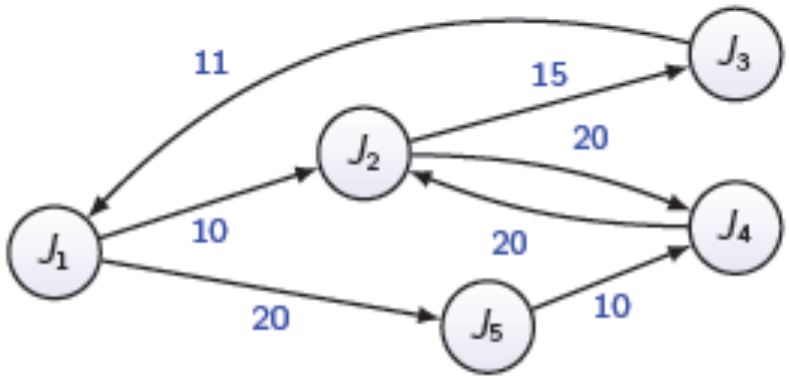
- long test runs: > 100.000 test events
- many discrepancies between spec and SUT detected
- incremental development of model

Scientific Highlight Y4

Martin Stigge, Pontus Ekberg, Nan Guan and Wang Yi.
IEEE RTETAS. Best Paper Nomination.

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 $p(J_i, J_j)$

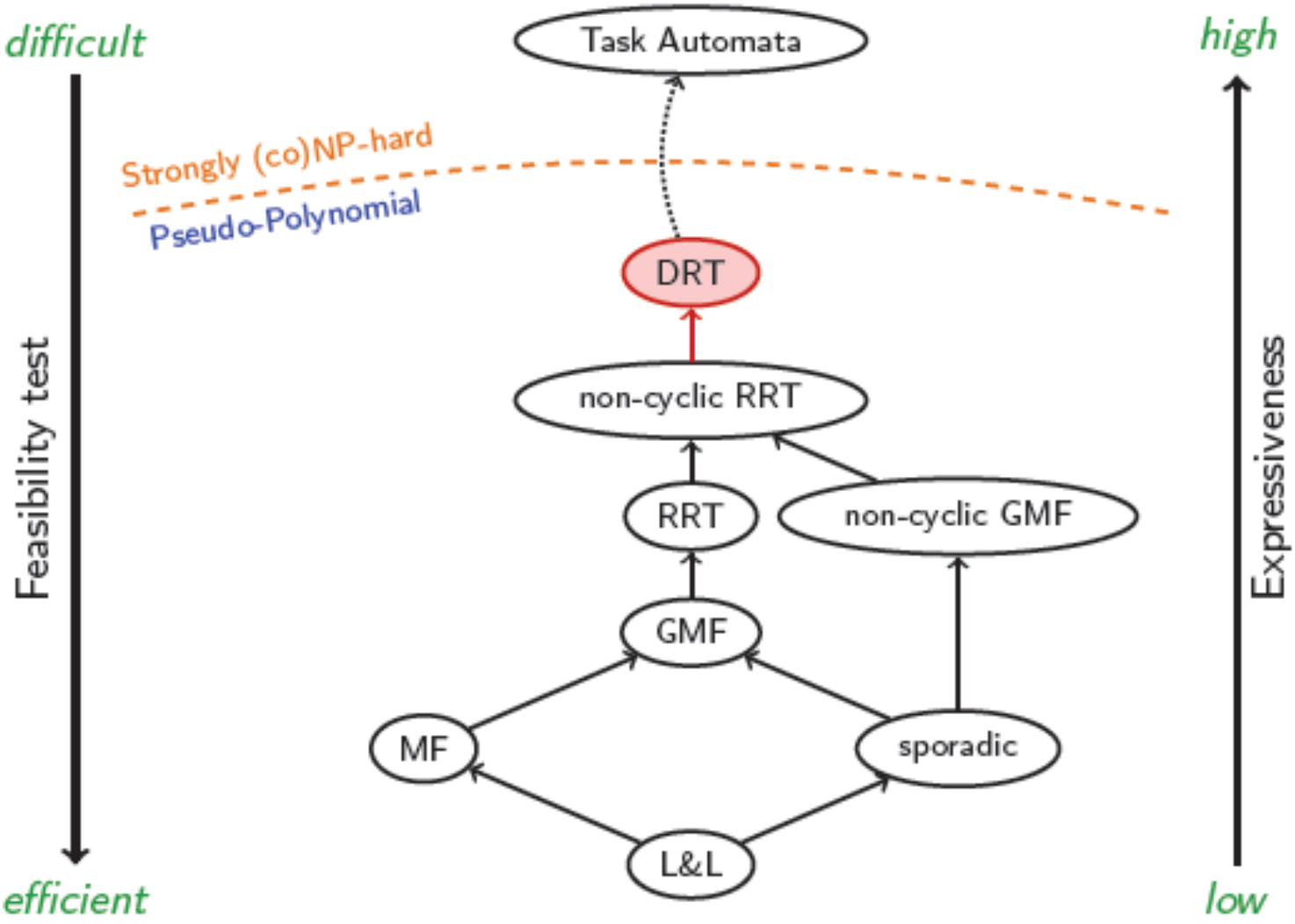


- Test *more challenging*, but also efficient:

Theorem (Our technical result)

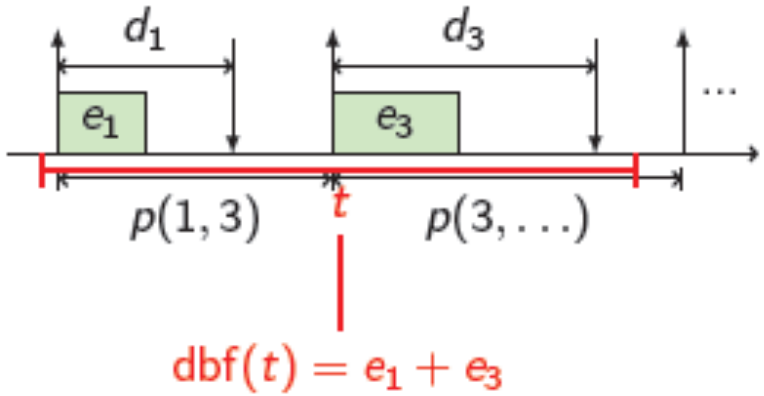
For DRT task systems τ with a utilization bounded by any $c < 1$, feasibility can be decided in pseudo-polynomial time.

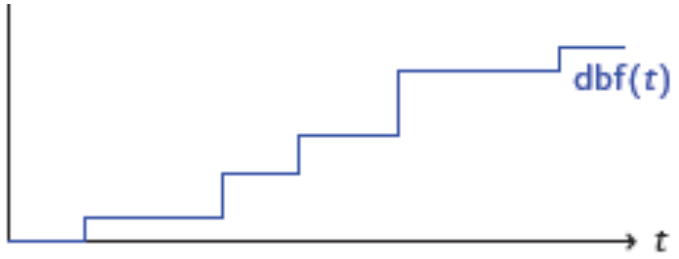
Digraphs: The Big Picture



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





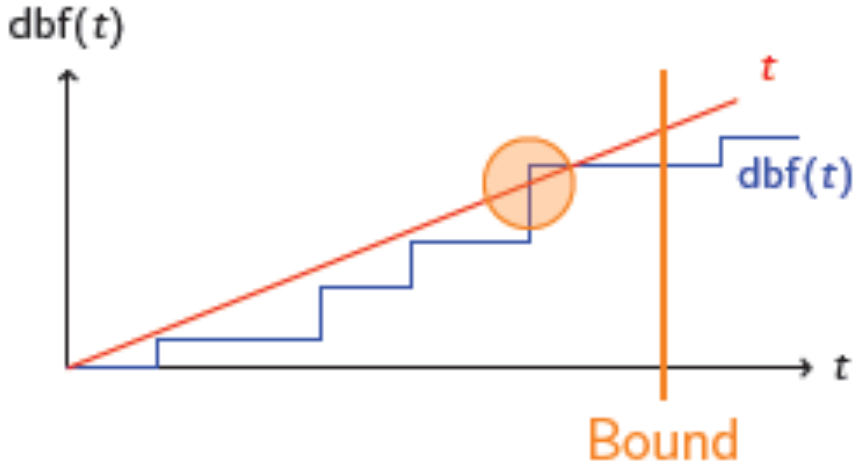
- Challenges:

Feasibility Test Using dbf()

Theorem

A task system τ is preemptive uniprocessor feasible iff:

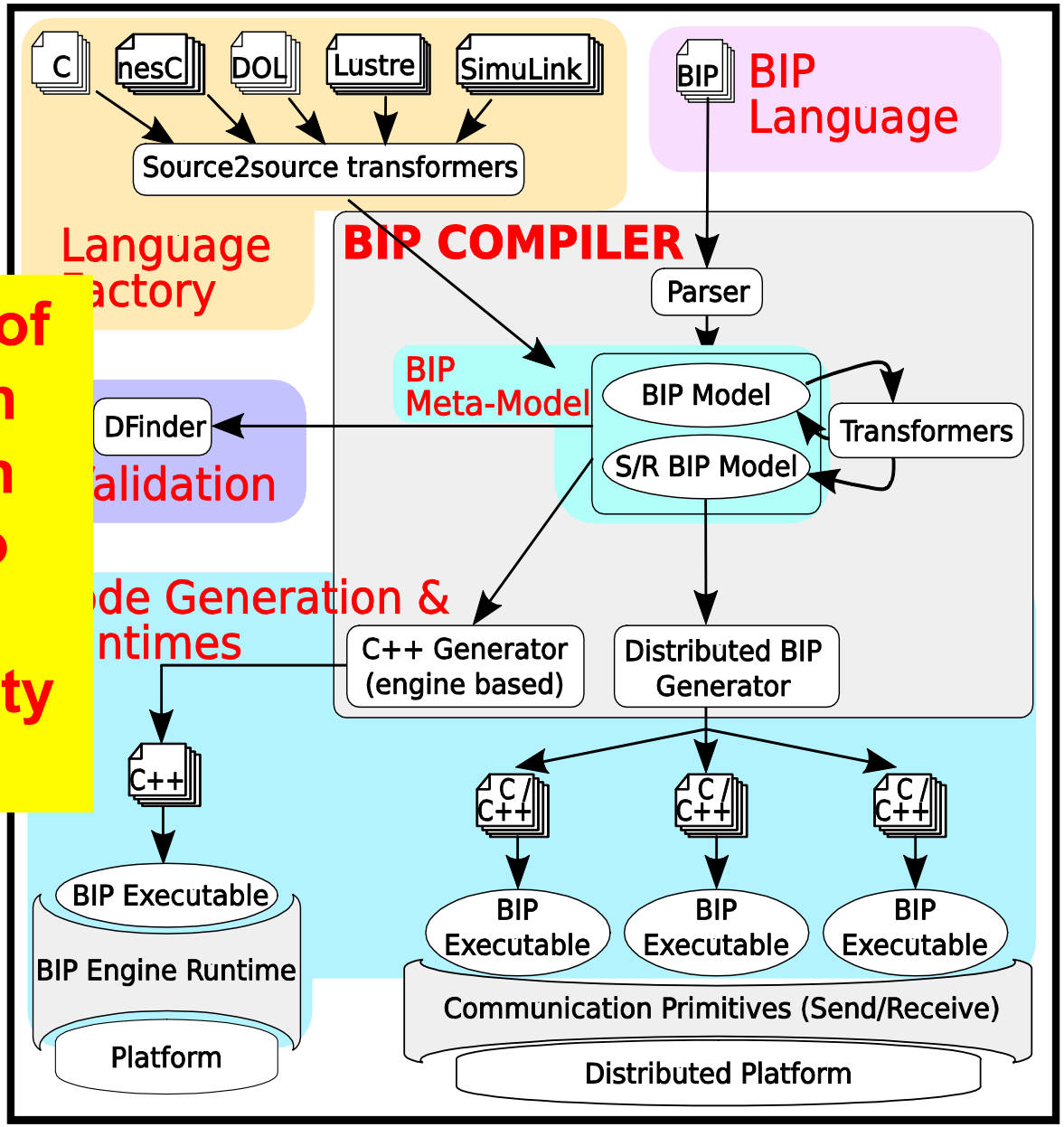
$$\forall t \geqslant 0 : \sum_{T \in \tau} \mathrm{dbf}_T(t) \leqslant t$$



- Challenges:
  1. How to calculate $\mathrm{dbf}_T()$?
  2. How to check existence of a violating t?

Highlight : The BIP Toolbox for rigorous component-based design in practice

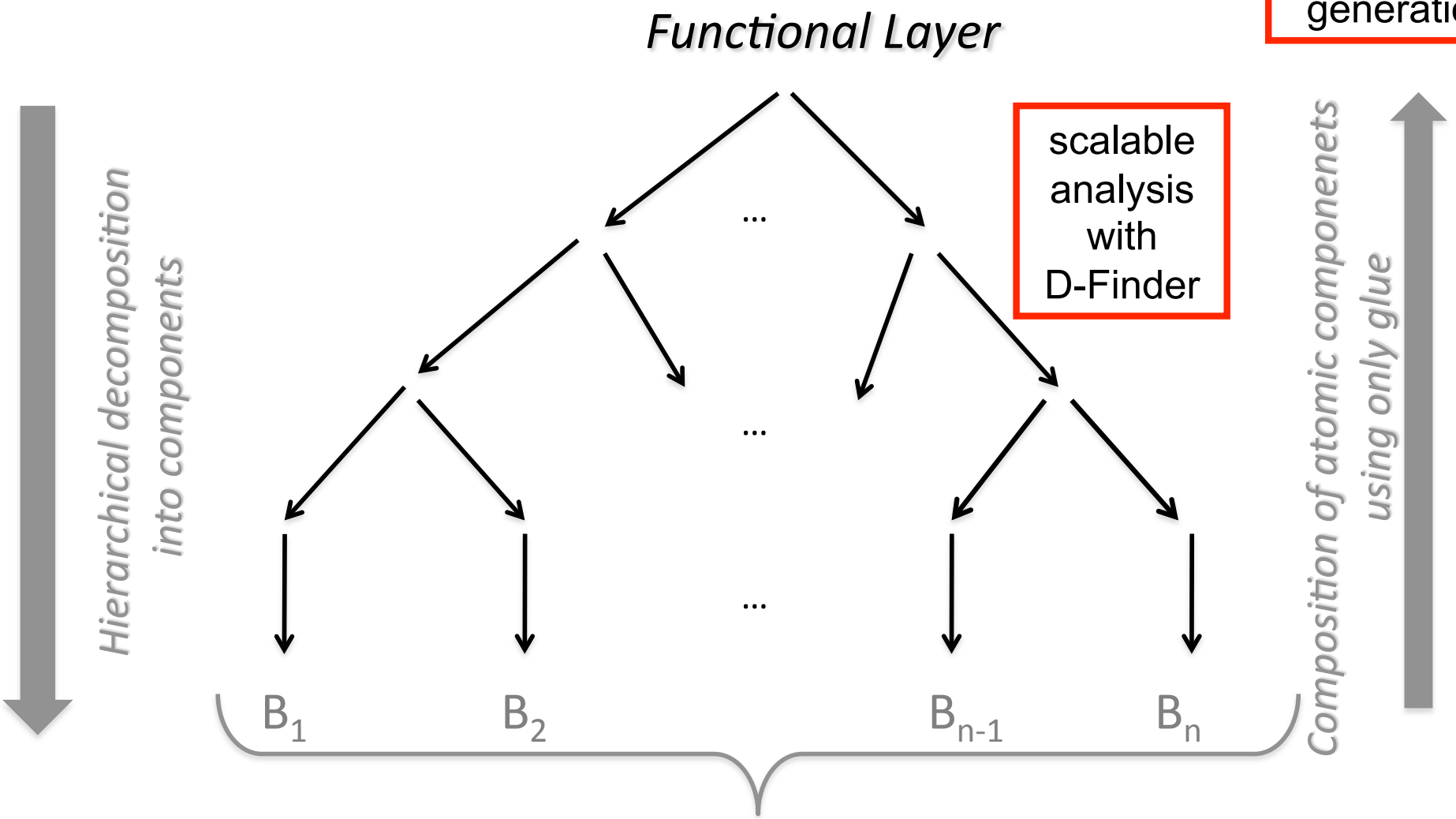
Integration of verification and design taking into account heterogeneity of models



Highlight : The BIP Toolbox - componentisation

Refactoring of Software to make it component-based

efficient C++ code generation



Highlight : The BIP Toolbox - componentization

GenoM/BIP Toolchain

Applied to the DALA Robot

GenoM

Models

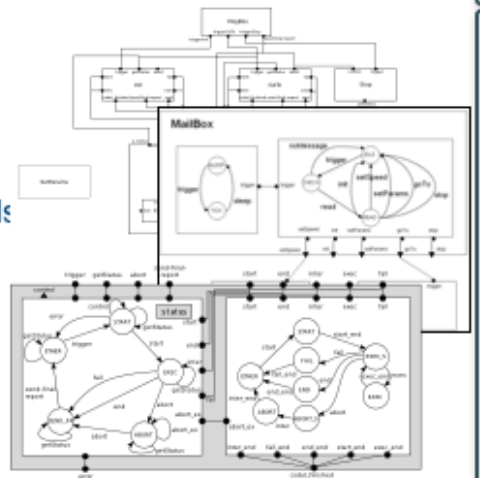
```
module Motion {
  number:  9600;
  SDI:     MOTION_DATA;
}
request SetPos {
  type:    control;
  input:   pos::pos;
  control: controlPos;
  report:  BAD_PARAM;
}
task Move {
  period:   25;
  priority: 15;
}
```

+

Codels

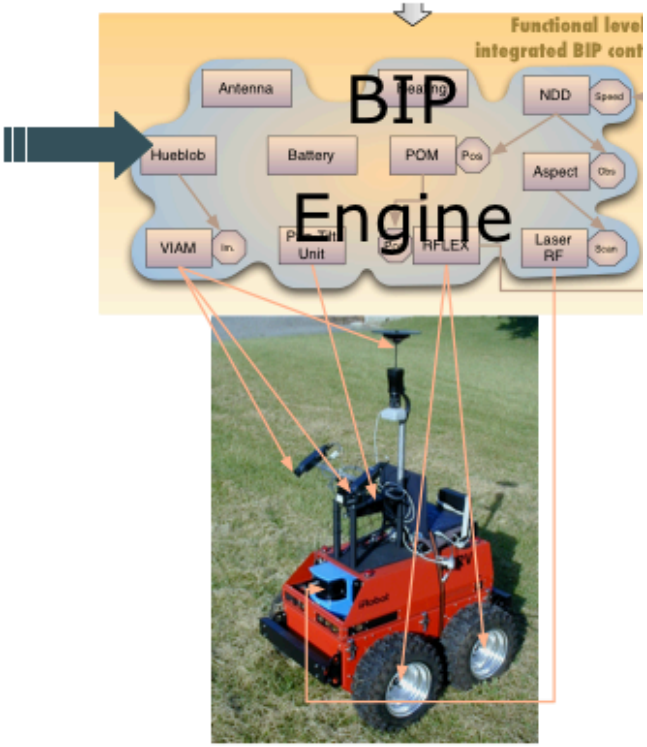
+

BIP Models

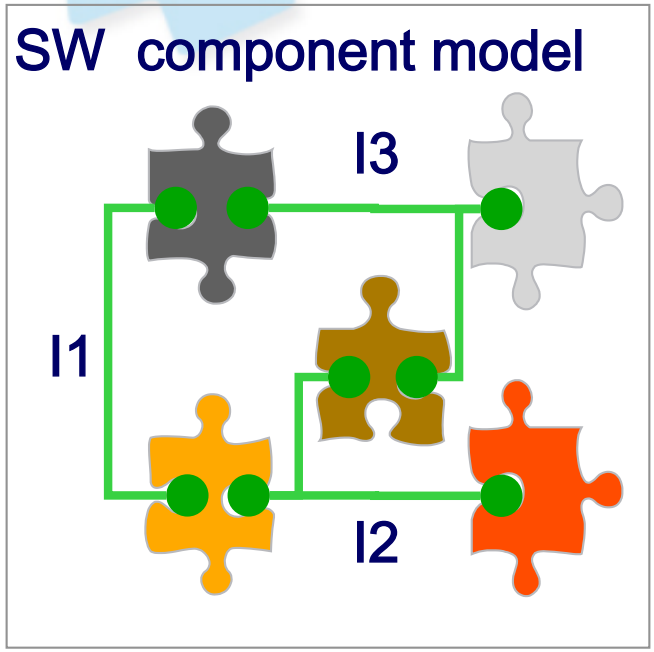


BIP

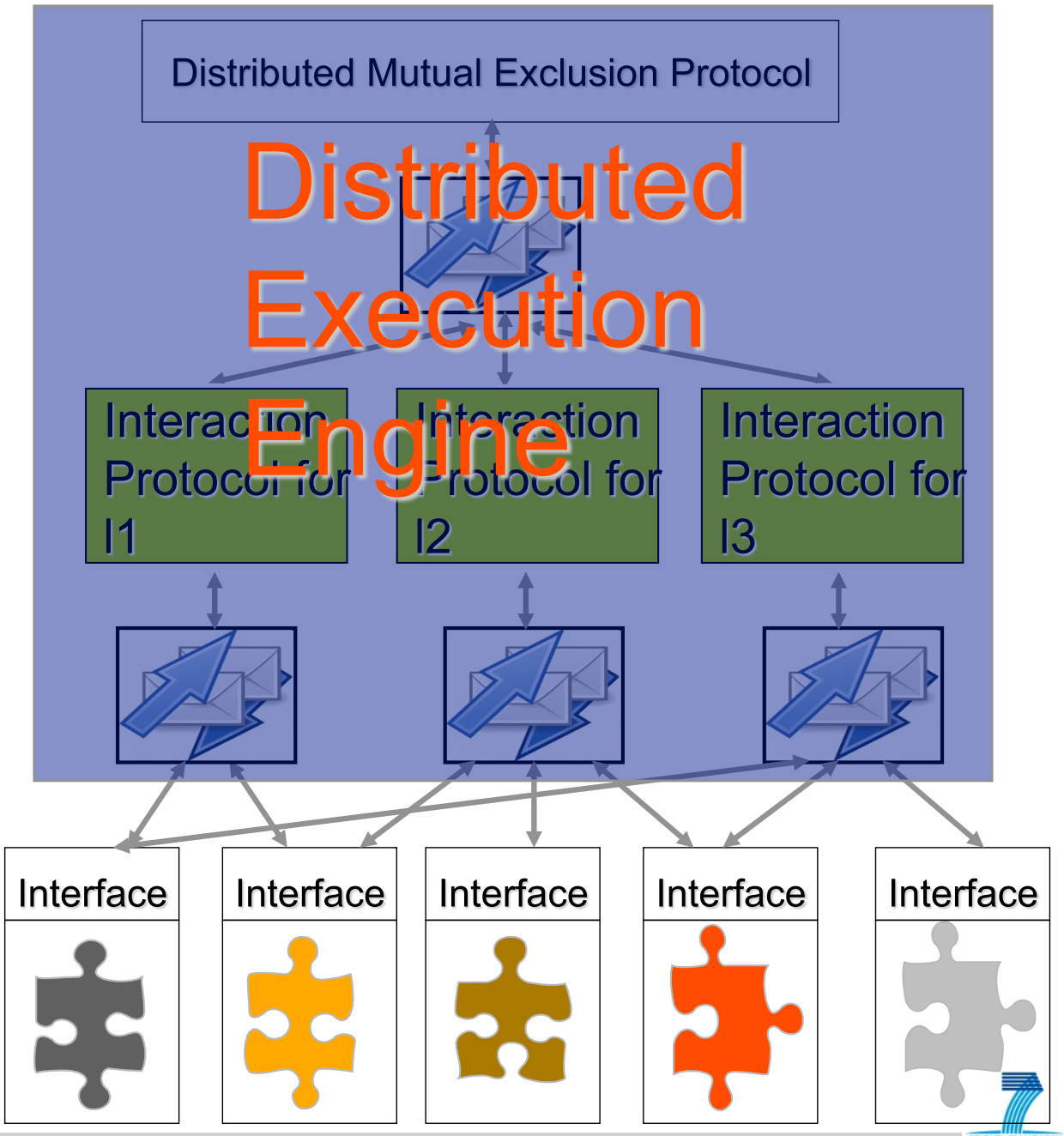
D-Finder



Highlight : The BIP Toolbox – Distributed Implementation



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.
- Compostional 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

INDUSTRIAL IMPACT

Test effort reduced by a factor of 10.

Building Excellence

in the area, in Europe

IMPACT

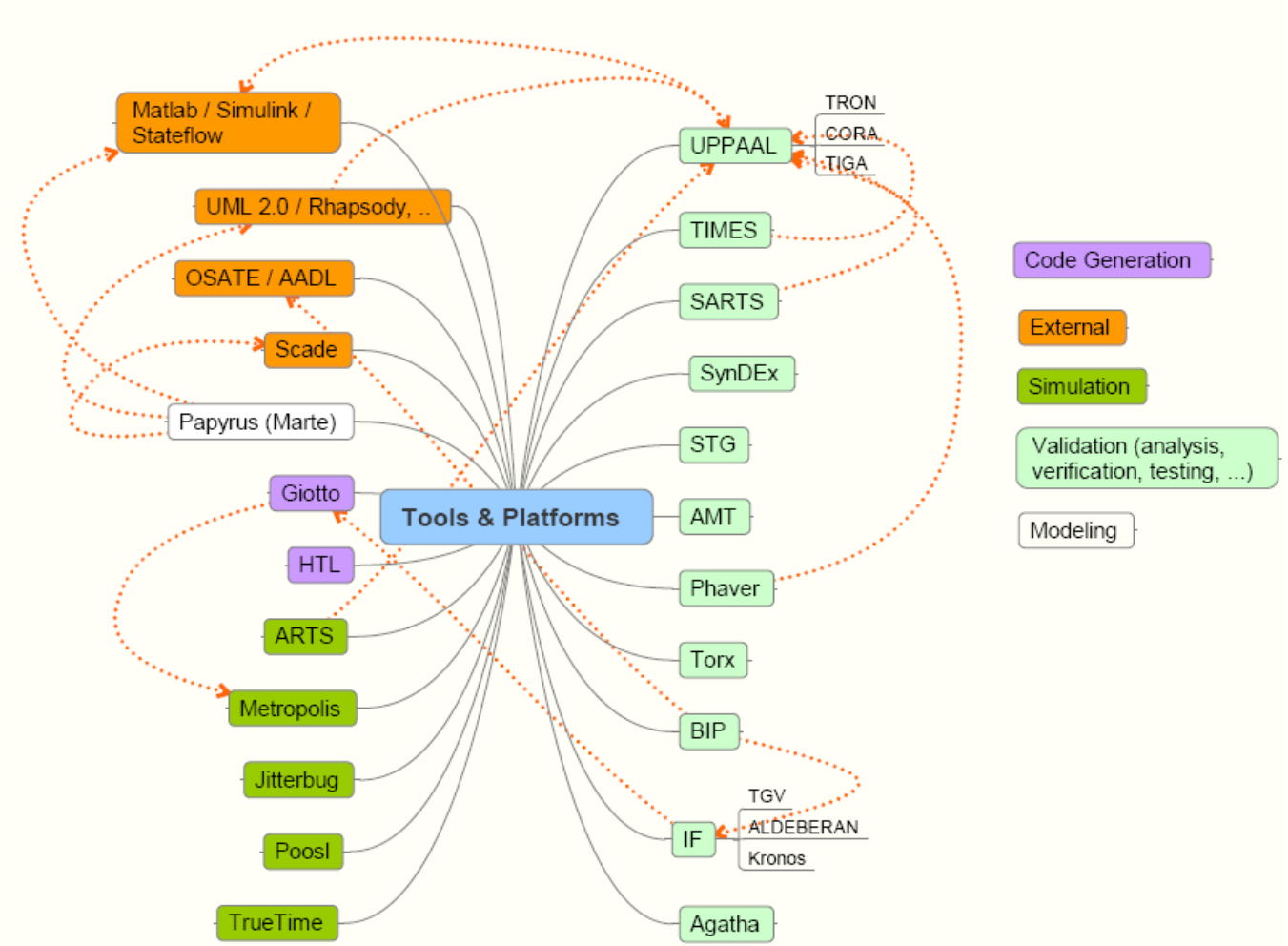
Several ARTEMIS projects:
ACROSS, CESAR, MBAT, RECOMB, SMECY, ...

Impact on industry in Franc
(Renault, Alstom, Esterelle, Thales, Denmark, (Terma, Novc
Nordisk, Danish Industr
Sweden, The Netherlan
(Philips Healthcare, OC
ASML, Thales,..), Italy
( ), Germany (Daimler, Siemens, ..), ..

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

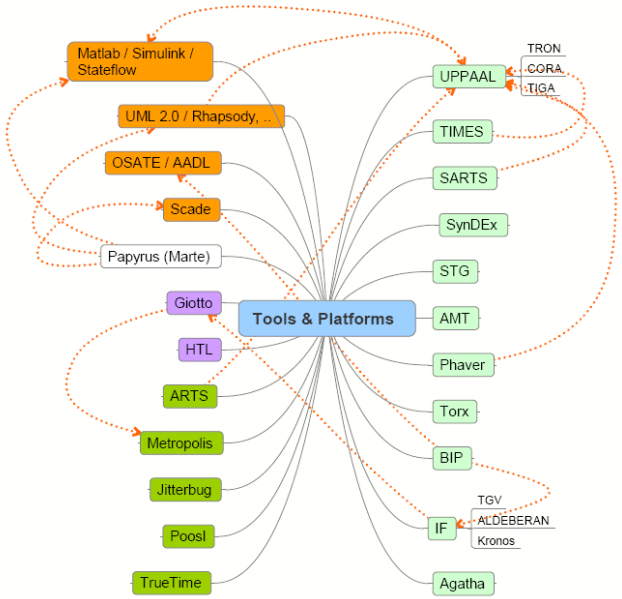
Advances on formalisms ar
theory for contracts & quantitative modeling

Tool Integration



Tools & Platforms

Tools & Platforms

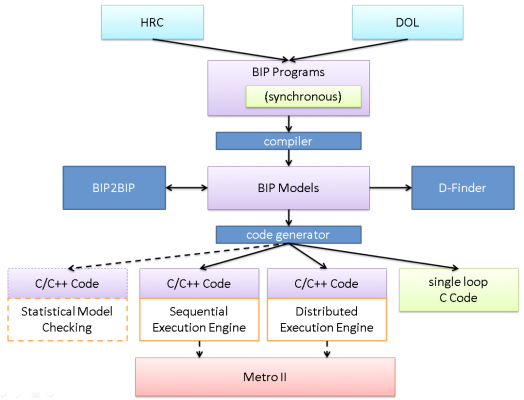


Code Generation
External
Simulation
Validation (a verification, t
Modeling

Individual tools (and links)

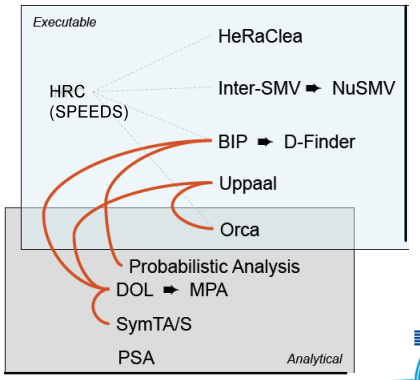
Scientific Highlight: Component-Based Design

COMBEST & SPEEDS



Tool-chain:

- integration of state-of-the-art tools
- application to case studies



Tool integration

Tool Integration

Main Scientific Highlights : Position Papers

T. Henzinger. *Two challenges in embedded systems design: predictability and robustness*. Phil. Trans. of the Royal Society, 2008

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

A. Sangiovanni-Vincentelli. *Is a Unified Methodology for System-Level Design Possible?* IEEE Design and Test of Computers, Special Issue, 2008.

S. Graf. *Special issue on "Omega -- Correct development of Real Time Embedded Systems".* In SoSyM Journal, vol. 7(2), 2008

W. Damm, B. Josko, A. Metzner, M. Di Natale, H. Kopetz, A. Sangiovanni Vincentelli. *Software Components for Reliable Automotive Systems*. In DATE 2008.

T. Henzinger *Grand Challenges for Real-Time Systems*. 20th ECRTS, Prague, 2008

T. Henzinger. "Challenges in Embedded Systems Design: Predictability and Robustness. Invited lecture, Royal Society Meeting, 2008

J. Sifakis. Embedded Systems Challenges and Research Directions. Onassis Foundation, The 2008 Lectures in Computer 2008, Heraklion Greece

K. Chatterjee, L. Doyen, T. Henzinger. *Quantitative Languages*, in Computer Science Logic (CSL'08), 2008.

M. Törngren, D. Chen, D. Malvius, J. Axelsson. Chapter on *Model-Based Development of Automotive Embedded Systems Model-Based Development of Middleware for Self-Configurable Embedded Real-TimeSystems: Experiences from the DySCAS Project*.

Main Scientific Highlights : Position Papers

T. N. Qureshi, M. Persson, D. Chen, M. Törngren and L. Feng. *Model-Driven Development for Distributed Real-Time Embedded Systems* Summer School MDD4DRES, Aussois, France, 2009

R. Passerone, I. Ben Hafaiedh, A. Benveniste, D. Cancila, A. Cuccuru, W. Damm, A. Ferrari, S. Gérard, S. Graf, B. Josko, L. Mangeruca, T. Peikenkamp, A. Sangiovanni-Vincentelli, F. Terrier, Meta-models in Europe: Languages, Tools and Applications, IEEE Design & Test of Computers, Special Issue, Vol 26 (3), 2009.

Ph. Cuenot, P. Frey, R. Johansson, H. Lönn, Y. Papadopoulos, M.-O. Reiser, A. Sandberg, D. Servat, R. Tavakoli Kolagari, M. Törngren, M. Weber. *The EAST-ADL Architecture Description Language for Automotive Embedded Software*. Invited chapter in "Model-Based Engineering of Embedded Real-Time Systems", 2009

R. Wilhelm, D. Grund, J. Reineke, M. Schlickling, M. Pister, and Ch. Ferdinand, *Memory Hierarchies, Pipelines, and Buses for Future Architectures in Time-Critical Embedded Systems*. Systems IEEE Transactions on CAD, Special Issue DATE 08

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

A. David, K.G. Larsen, U. Nyman, A. Legay, and A. Wasowski. Methodologies for specification of real-time systems using timed I/O automata. FMCO 2009

M. Di Natale and A. Sangiovanni-Vincentelli, *Moving From Federated to Integrated Architectures in Automotive: The Role of Standards, Methods and Tools*, IEEE, 2010

Main Scientific Highlights : Position Papers

P. Bouyer, U. Fahrenberg, K. G. Larsen, N. Markey. Quantitative modelling and analysis of embedded systems. Communications of the ACM, 2011. Invited paper.

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

Gerd Behrmann, Alexandre David, Kim Guldstrand Larsen, Paul Pettersson, Wang Yi: Developing UPPAAL over 15 years. Softw., Pract. Exper. 41(2): 133-142 (2011)

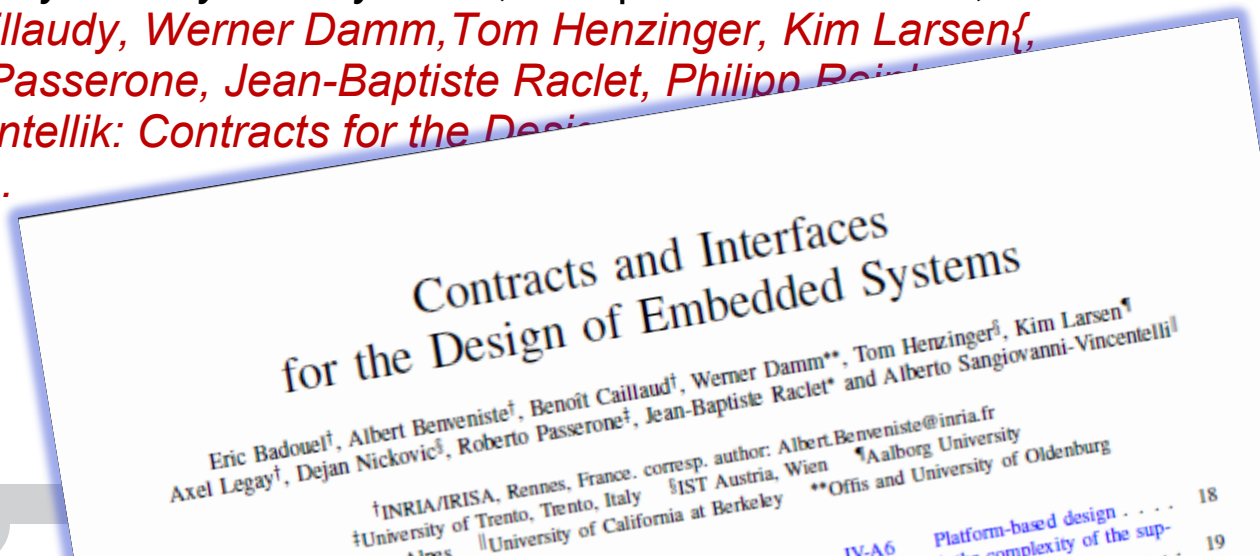
Joseph Sifakis *Methods and tools for component-based system design*. DATE 2011

P. Derler, Ed Lee and A. Sangiovanni Vincentelli, Modeling Cyber–Physical Systems, IEEE, Vol. 100, n.1, January 2012, invited paper

P. Nuzzo, A. Sangiovanni Vincentelli, X. Sun, A. Puggelli, *A Methodology for theDesign of Analog Integrated Interfaces Using Contracts*, IEEE Sensors Journal, 2012, invited

Sangiovanni-Vincentelli, W. Damm, and R. Passerone. *Taming Dr. Frankenstein: Contract-Based Design for Cyber-Physical Systems*, European J. of Control, 2012

Albert Benvenistey, Benoît Caillaudy, Werner Damm,Tom Henzinger, Kim Larsen{, Dejan Nickovicx, Roberto Passerone, Jean-Baptiste Raclet, Philipp Rei... Alberto Sangiovanni-Vincentellik: Contracts for the Desi... Submitted to Proc of IEEE..



Contracts and Interfaces
for the Design of Embedded Systems

Eric Badouel†, Albert Benveniste†, Benoît Caillaud†, Werner Damm**, Tom Henzinger§, Kim Larsen¶
Axel Legay†, Dejan Nickovic§, Roberto Passerone‡, Jean-Baptiste Raclet* and Alberto Sangiovanni-Vincentelli‖

†INRIA/IRISA, Rennes, France. corresp. author: Albert.Benveniste@inria.fr
‡University of Trento, Trento, Italy §IST Austria, Wien ¶Aalborg University
‖University of California at Berkeley **Offis and University of Oldenburg

Lasting Impacts

Future interaction beyond the end of the NoE

Research wil 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)

Lasting Impacts

Future interaction beyond the end of the NoE

BUT

Funding (now and future) is becoming increasingly application driven!

➔

Less funding for foundational research on challenges, e.g.:

- 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