Year 3 Review
Brussels, December 14th, 2007

Achievements and Perspectives :

Testing and Verification

Cluster leader : Kim Guldstrand Larsen

CISS, Aalborg University, Denmark

Core Partners of the Cluster

- CISS, Aalborg University
  (real-time verification and testing, controller synthesis, security)
- University of Twente
  (verification and testing of hybrid and stochastic systems, security)
- Verimag
  (real-time verification and testing, security protocols analysis)
- CFV / Centre Fédéré de Verification
  (model checking and robustness of hybrid and real-time systems)
- LSV / CNRS
  (model checking, security protocols and logics)
- INRIA / Rennes
  (symbolic testing, security, controller synthesis)
- Uppsala University
  (real-time verification, testing and schedulability)
- OFFIS, Oldenborg
  (UML-based verification and testing)

Affiliated partners:
5 industrial
6 academic

Cluster Activities

- JPRA-Cluster Integration
  Quantitative Testing and Verification
  (Ed Brinksma)

- JPIA-Platform:
  Testing and Verification Platform
  (Kim G. Larsen)

- JPRA-Cluster Integration
  Verification of Security Properties
  (Sandro Etalle)

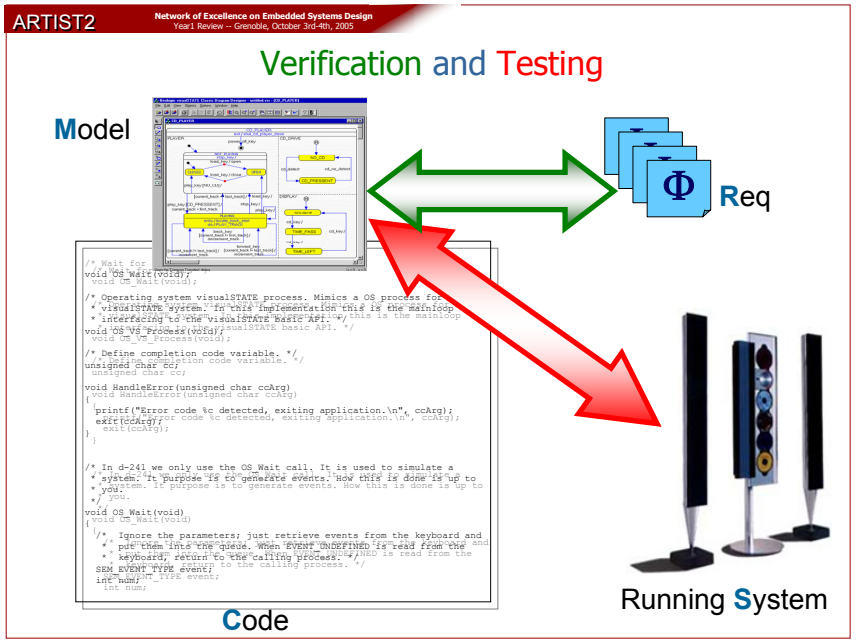
Outline

- Overall Aims and Achievements
- Scientific Highlights during Y3
- Work planned for Y4
- Scientific Highlights within Security (Sandro Etalle)
- Discussion

Overall Aims and Achievements

Vision & Long Term Goals

- 30-70% of production time is currently spend on elaborate, ad-hoc testing
- Gap between industrial practice and academic state-of-the-art
- Time-to-market may be shortened considerable by verification and performance analyses of early design models
- Models must deal with quantitative information (real-time, memory, bandwidth, energy) and security.



High-Level Objectives

Improve current industrial practice for validating embedded systems applications by continuous dissemination and improvement of existing powerful testing and verification techniques and tools.

Effort on making state-of-the-art verification and testing technology *visible* and *easily accessible* for industry with long term vision of integration in tool chains applied in industry.

Testing and Verification Platform

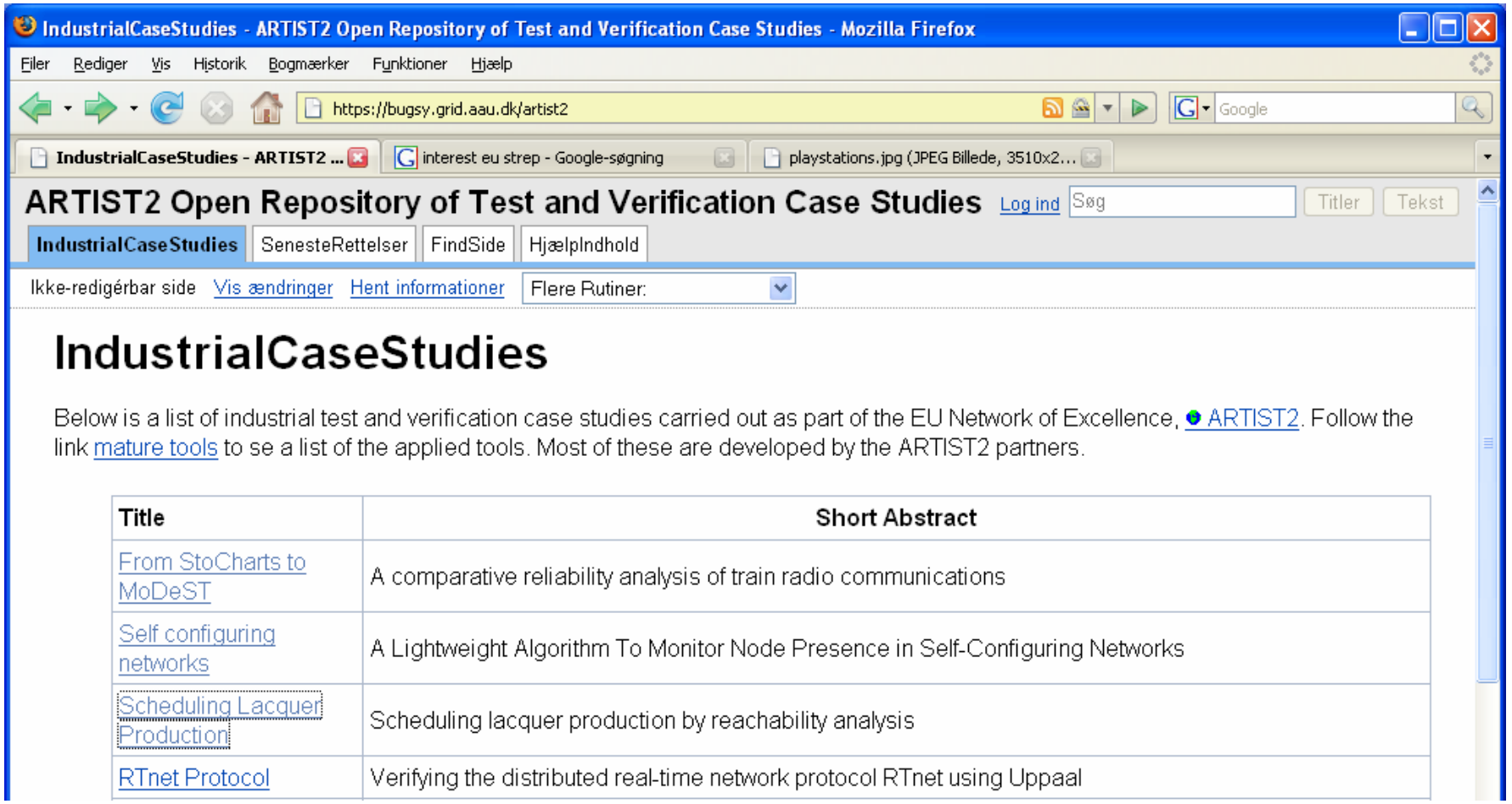
- Highlevel Objectives
  - Individual tools
  - Dissemination through industrial case studies (web)
  - Verification Server and Grid
- Milestones Y3
  - Tool evaluation through industrial case studies; reported on web repository (done)
  - Installation and links to stable version of individual tools (done)
  - Exploitation of local PC-clusters and NorduGrid (done)
  - Mutual exploitation of European Grid resources for model checking (postponed)

Testing and Verification Platform

- Advances on Individual Tools
  - Improved versions of UPPAAL (verification), TRON (testing) and TIGA (synthesis) (Aalborg)
  - Improved STG tool (test generation) (IRISA)
  - CATS: compositional timing and performance analysis using timed automata and real time calculus (Uppsala)
  - Open source DBM library (Aalborg);
  - DeadlockFinder, generating BIP models (VERIMAG)
  - DeVinE parallel multicore verifier for Promela models (Brno)

Testing and Verification Platform

Verification Case Studies (OFFIS, Twente, Aalborg, Uppsala)



Quantitative Testing and Verification

- Highlevel Objectives Y3
  - Metrics for testing coverage
  - Abstraction methods and compositional techniques
  - Optimal scheduling & controller synthesis
  - Robustness and implementability
  - Stochastic, timed and hybrid models
- Milestones Y3
  - Optimal controller synthesis (done)
  - Robust model checking (done)
  - Coverage-based test selection (done)
  - Code generation (postponed)
  - Connection between academic and industrial tools (demonstrated; UPPAAL→Simulink)

Quantitative Testing and Verification

problems dealt with

- Verification Heuristic search Algorithms
- Testing Games; conformance for hybrid systems
- Compositionality Modal Transition Systems
- Abstraction and Approximate Analysis
  Event stream abstraction from TA
  CEGAR for TA
  Iteration and convex hull for inf. state
- Robustness and Implementability
- Controller Synthesis and Optimal Scheduling
- Priced Timed Automata & Quantitative Models
  > 3 clocks: undec; 1 clock: dec; 2 clocks ?

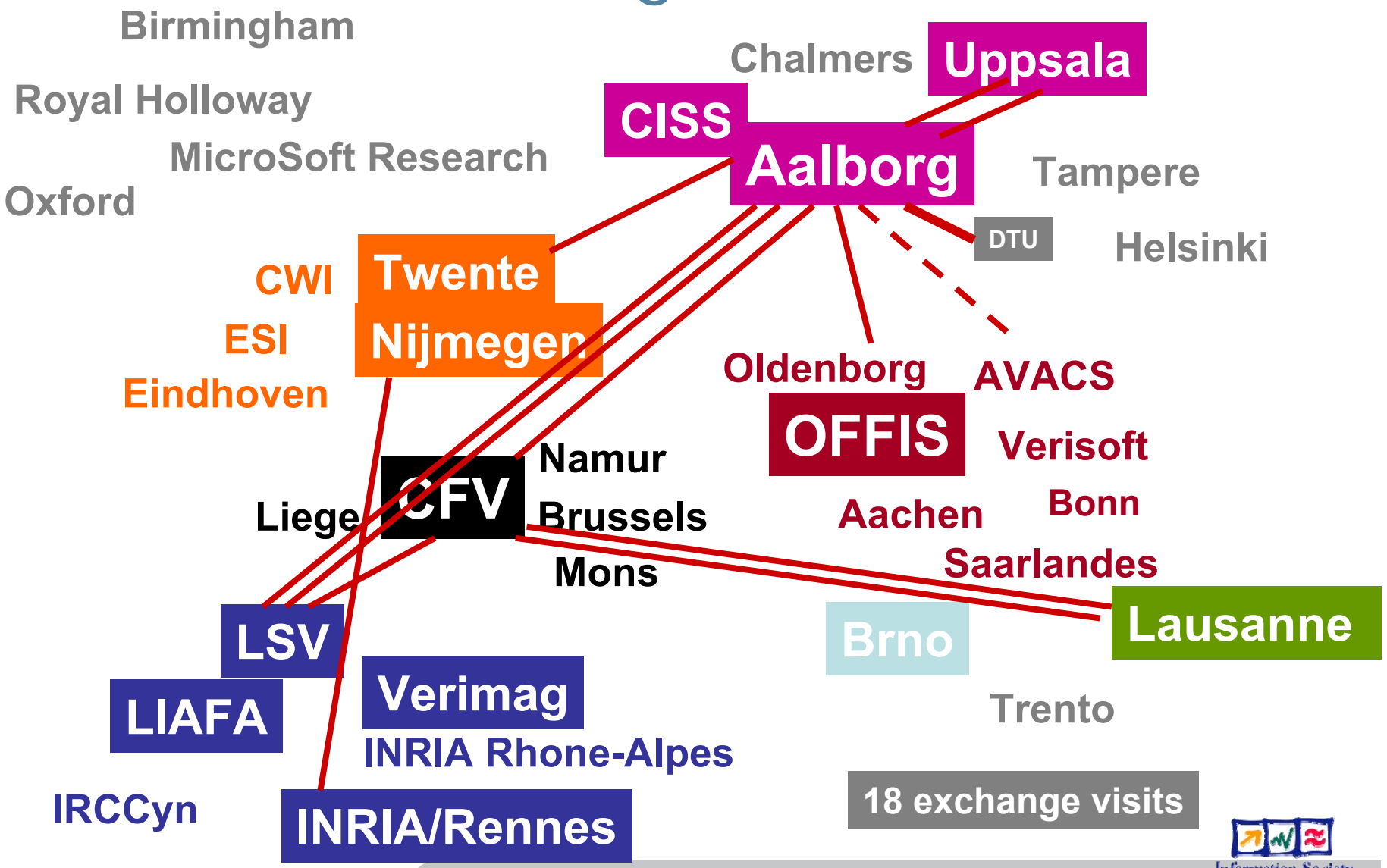
Spreading of Excellence

- Organization and contributions to the ARTIST2 winter school MOTIVES in Trento, February 2007.
- Cluster meeting in Trento, February 2007.
- Organization and contributions to the ARTIST2 workshop at DATE, Nice, April, 2007.
- Organization and contributions to the ARTIST2 workshop at CAV, Berlin, July 2007.
- Organization and hosting of the International Workshop FORMATS in Paris, October, 2006.
- Organization and hosting of the International Workshop FORMATS in Saltzburg (in connection with the ES Week), October 2007.

Spreading of Excellence

- 86 publications
- 19 joint publications
- 40 invited keynotes, workshops or tutorials
- CNRS Bronze Medal (Patricia Bouyer)
- ENS Cachan Honary Doctorate (Kim G. Larsen)

Exchange Visits



Overall Assessment

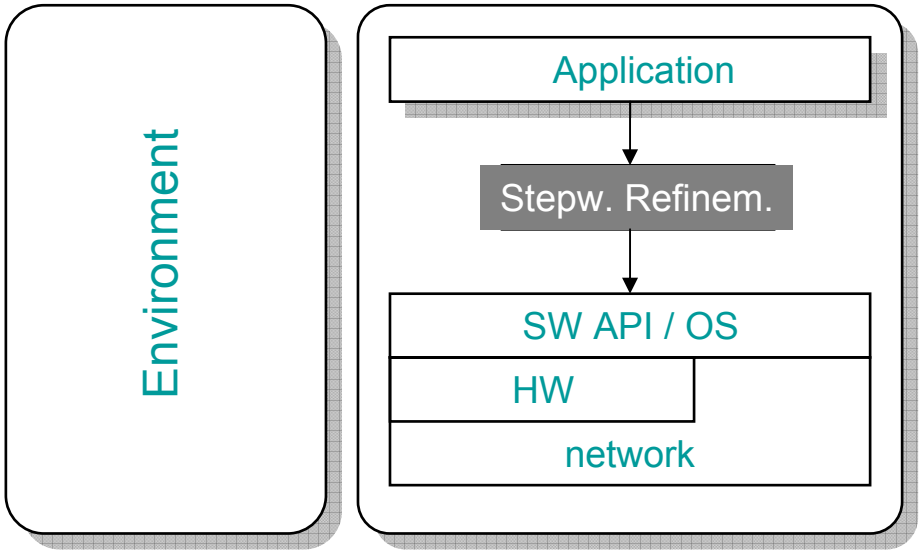
- As last year *Quantitative Testing and Verification* and *Verification of Security Properties* have been particular successful.
- Extensive list of publications, invited and keynote lectures, etc witnesses *true excellence* within the area.
- *Quantitative Testing and Verification* and *Testing and Verification Platform* are tightly connected.
- The objective of joint infra-structure for *European Verification Grid not* pursued during Y3.
- Substantial effort has been put by individual partners in *dissemination* to research and industry.

Scientific Highlights Y3

3 examples

DaNES

Danish Network for Embedded Systems

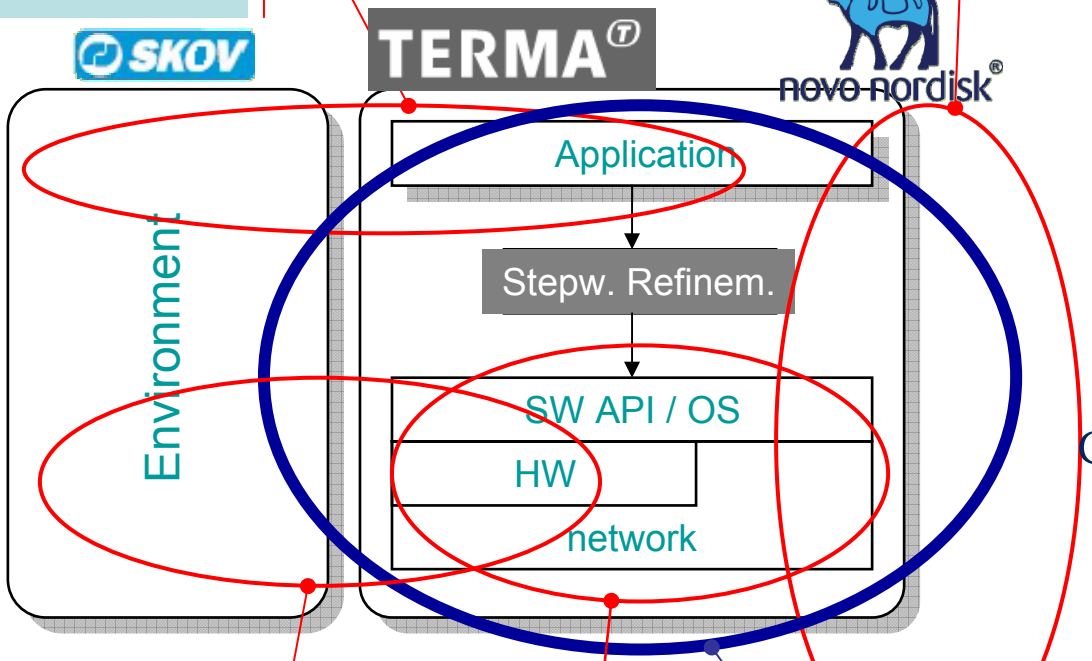


DaNES

Danish Network for Embedded Systems

Selfdiagnosic & -repair

Test & Verificaiton



Højteknologifonden

2007-2011: 9MEuro

Embedded & Distributed Control

Development

Informatik og Matematisk Modellering

IO TECHNOLOGIES

CENTER FOR INDLEJREDE SOFTWARE SYSTEMER

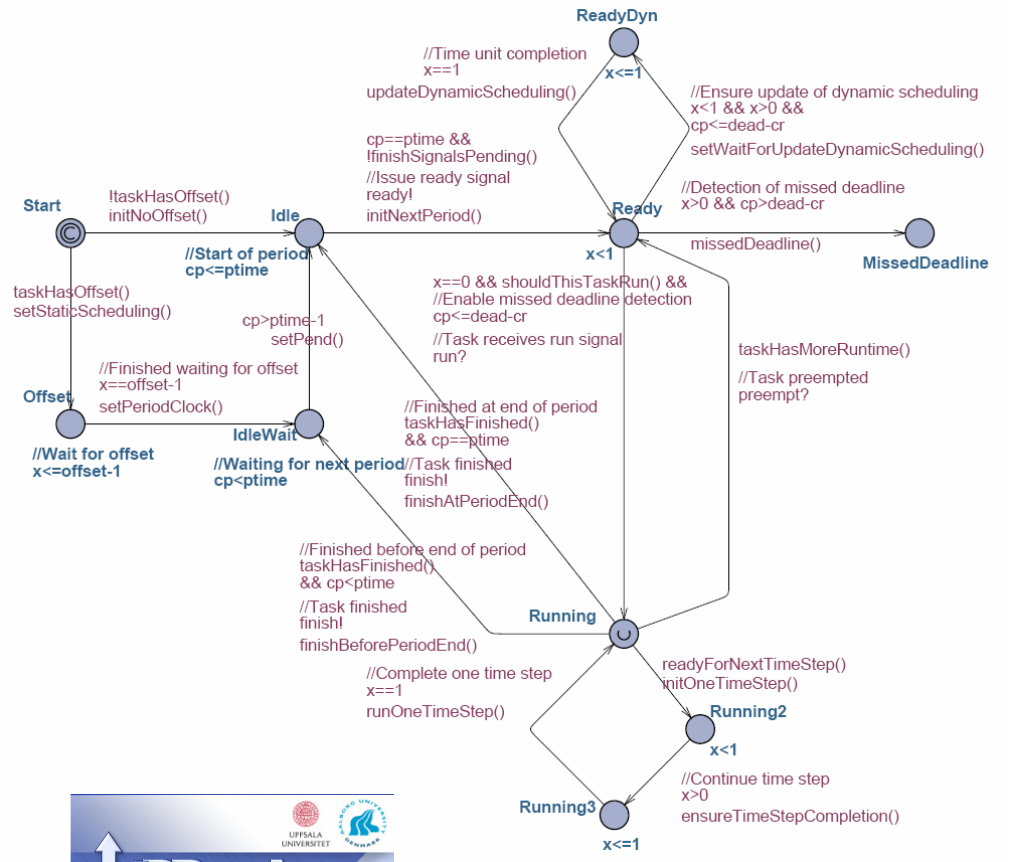
GATEHOUSE

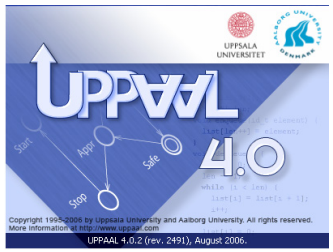
ice power

PAJ SYSTEMTEKNIK

Information Society

ARTS MPSoC Model in UPPAAL





A Timed Automata Model for a Task

DTU, Aalborg

Aske Brekling, Jens Ellebæk,
Kristian S. Knudsen,
Jan Madsen,
Michael R. Hansen,
Jacob Illum Rasmussen

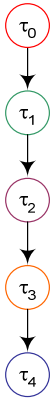
DaNES

Similar models for
- dependencies, scheduling principle
- execution platform
  (multi-processor)
- network

Handling realistic applications?

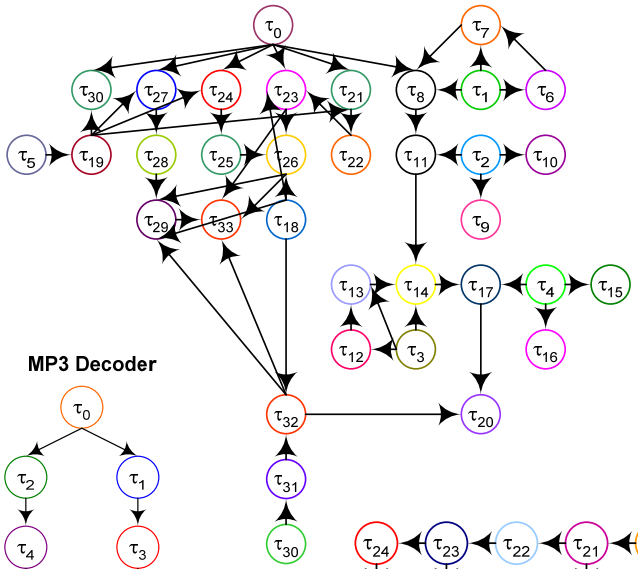
Smart phone:

JPEG Encoder

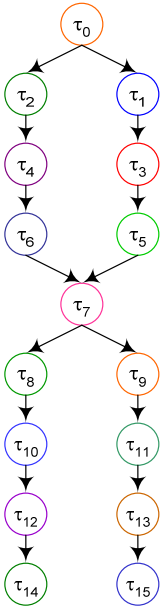


JPEG Decoder

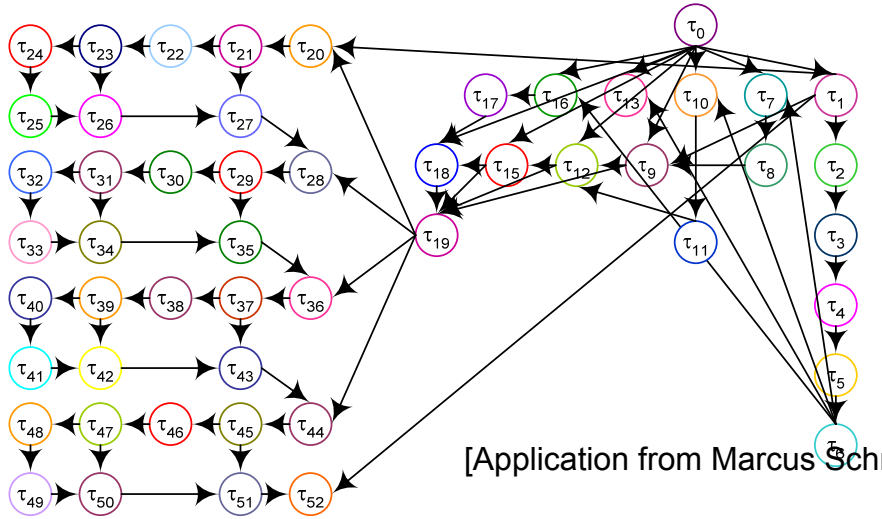
GSM Decoder



MP3 Decoder



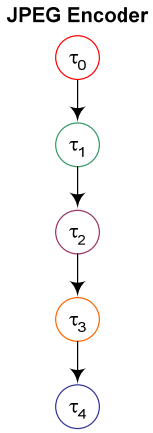
GSM Encoder

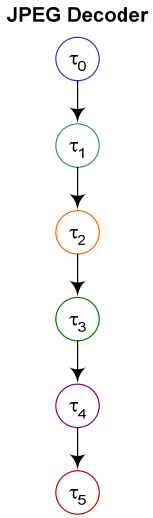


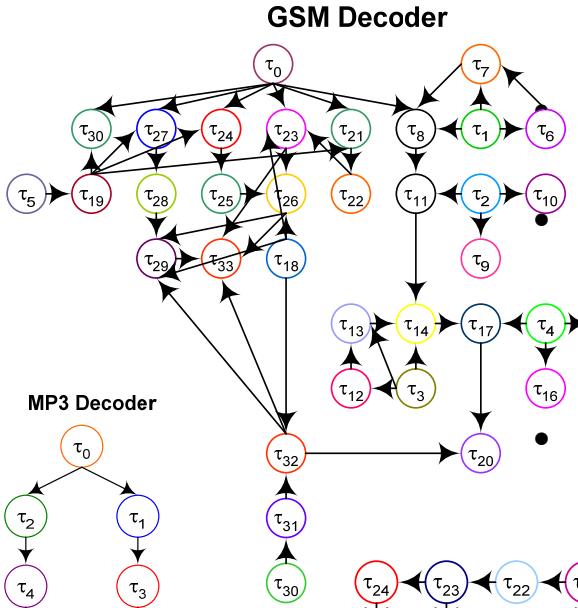
DaNES

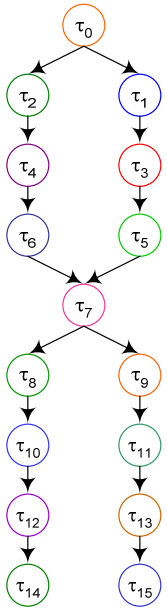
[Application from Marcus Schmitz, TU Linkoping]

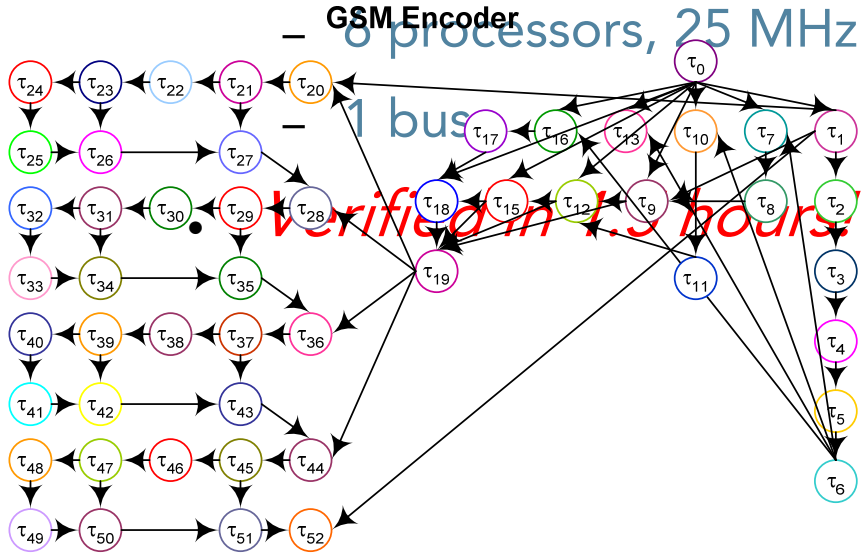
Smart phone











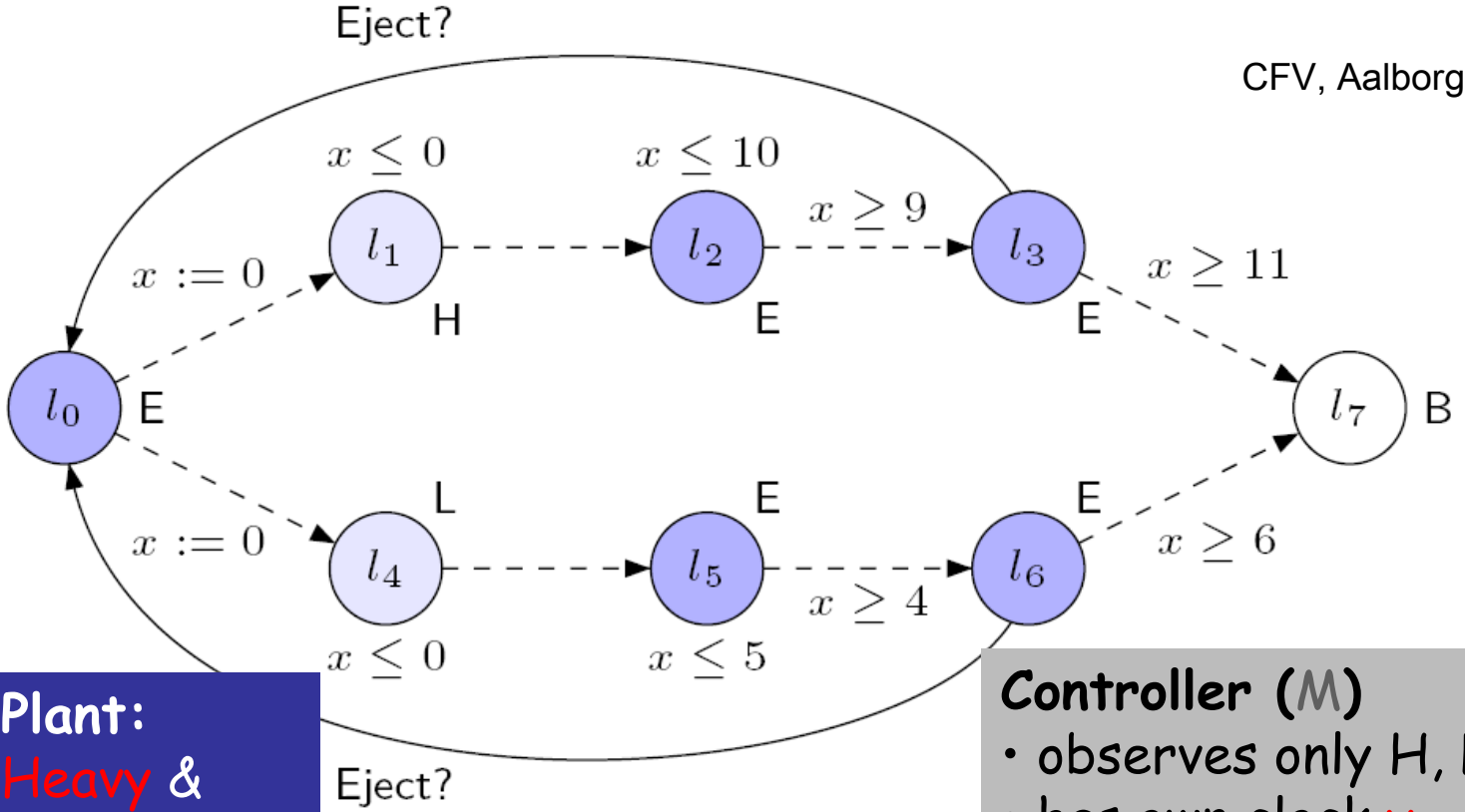
- Tasks: 114
- Deadlines: [0.02: 0.5] sec
- Execution: [52 : 266.687] cycles
- Platform:
  - 8 processors, 25 MHz
  - 1 bus

Verified in 1.3 hours!

DaNES

Timed Games w Partial Observability

CFV, Aalborg, LSV, Nantes



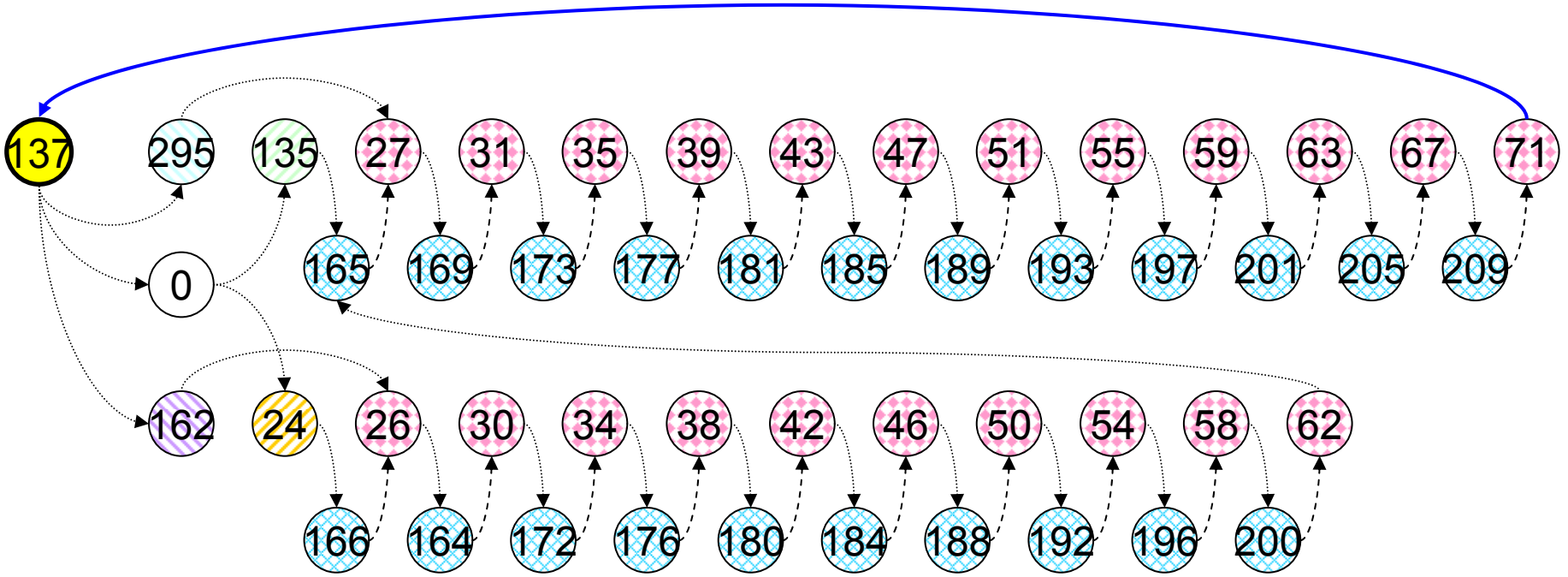
Plant:
Heavy & Light Bricks

Objective:
A[] : B

Controller (M)
- observes only H, L, E or B
- has own clock y
- can test (y < M) or (y ¸ M)
- can always reset y

+ MEMORY

Memory-full Strategy



Partition:

Actions:

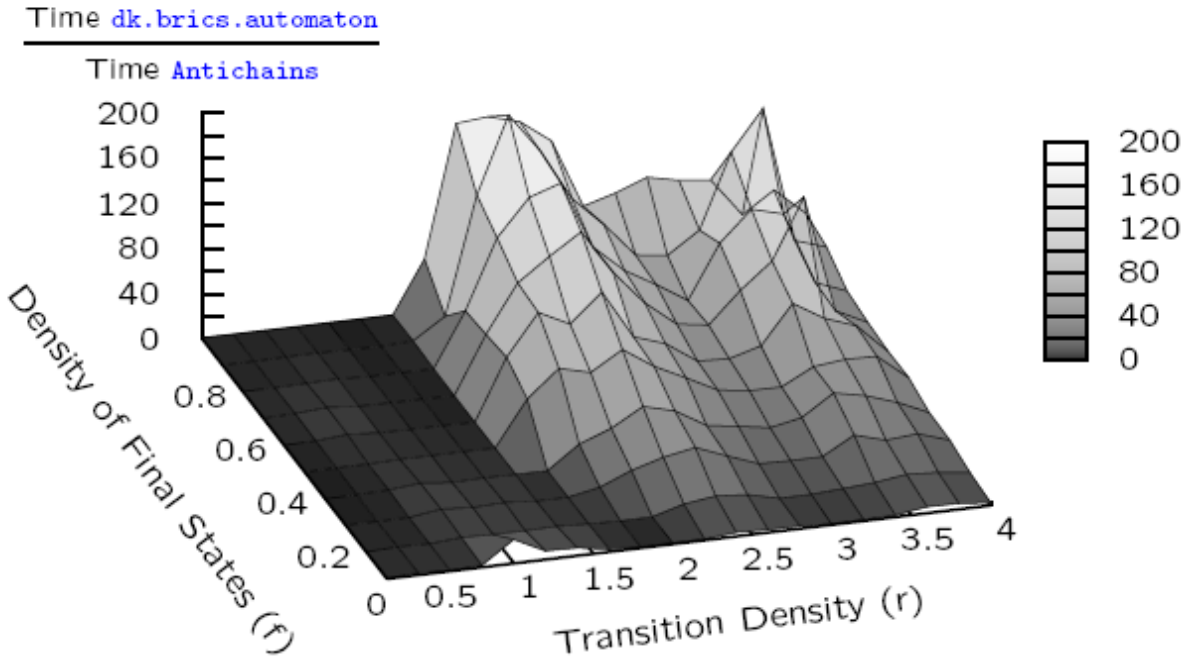
delay

y=0

eject!

LTL Model Checking

- Martin De Wulf, Laurent Doyen, Thomas A. Henzinger, Jean-François Raskin, Nicolas Maquet CAV2006, TACAS2007, TACAS2008.



Each sample point: 100 automata with $|\mathrm{Loc}| = 175$, $\Sigma = \{0, 1\}$.

Work Planned in Y4

Testing and Verification Platform

- Milestones Y3
  - Tool evaluation through industrial case studies; reported on web repository (done)
  - Installation and links to stable version of individual tools (done)
  - Mutual exploitation of European Grid resources for model checking (postponed)
  - Exploitation of local PC-clusters and NorduGrid (done)
- Future milestones Y4
  - Case tool repository updated.
  - 3 candidates for high-performance verification (SPIN, UPPAAL, DiVine) tested on the new cluster in Aalborg.
  - Maintain links to existing activities on high performance verfication

Fyrkat & PS3

Fyrkat: new PC cluster: 84 servers w 672 processor kernels.
1.3 terabyte ram; 4.8 terabyte memory; 6,2 teraflops.

30 PS3 Cell processor; highly parallel programming

Quantitative Testing and Verification

- Milestones Y3
  - Optimal controller synthesis (done)
  - Robust model checking (done)
  - Coverage-based test selection (done)
  - Code generation (postponed)
  - Connection between academic and industrial tools (demonstrated; UPPAAL→Simulink)
- Future milestones Y4
  - Efficient tool component for controller synthesis under partial observability
  - Property-preserving code generation.
  - Generic framework for abstraction and compositionality for efficient analysis of quantitative models.

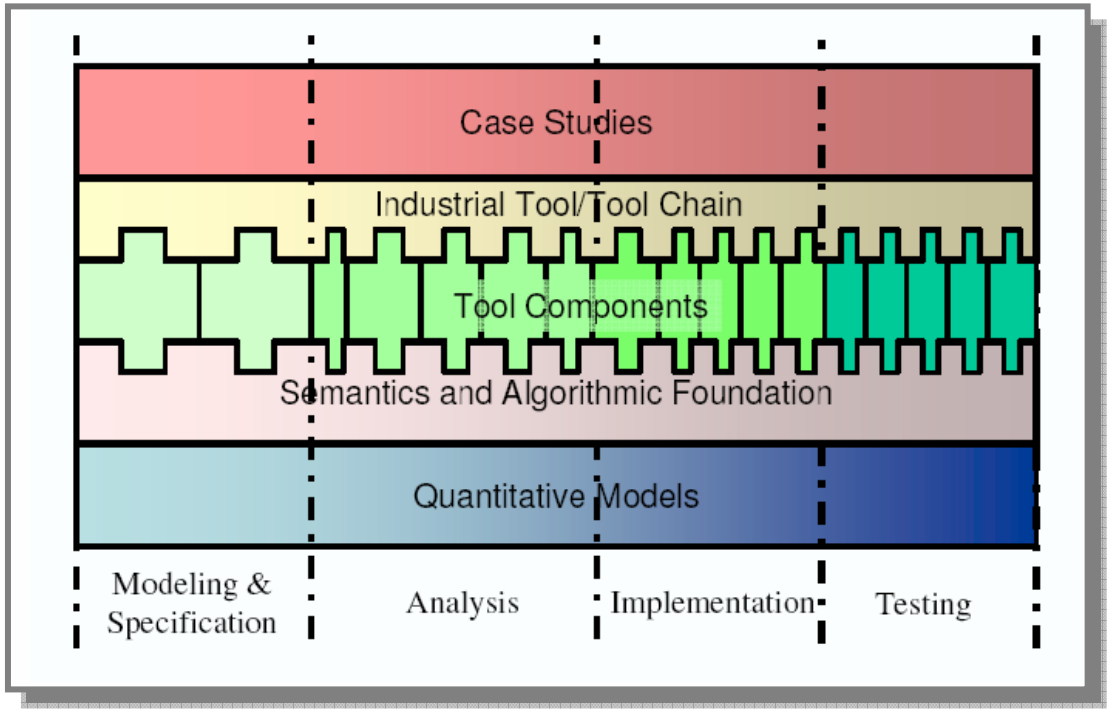
Quantitative Testing and Verification
problems to be dealt with

- Verification
  - Efficient tool for LTL model-checking
- Testing
  - Semantic framework test coverage (secco).
  - Testing and learning
- Abstraction and Approximate Analysis
- Robustness and Quantitative Analysis
  - Metrics on stochastic games
- Controller Synthesis and Optimal Scheduling
  - Priced timed games and robustness

Quasimodo (FP7 STREP)

Quantitative System Properties in Model-Driven Design of ES

- AAU, DK
- ESI, NL
- CNRS, F
- Aachen, D
- Saarland, D
- Brussels, B
- Terma, DK
- Chess, NL
- Hydac, D



"The Quasimodo project will research and develop methods and tools that can be used to design reliable embedded systems that meet their requirements in a controlled and resource-efficient way using a model-based approach. This means that design decisions, analysis, simulation, testing, code generation, etc. are always based upon models that reflect the relevant aspects of the design. This requires methods to maintain, manipulate, analyse and transform models in a coherent and meaningful way."

Year 3 Review
Brussels, December 14, 2007

Verification of Security Protocols

Cluster Testing and Verification

Sandro Etalle

University of Twente & University of Eindhoven

Goal of the Activity

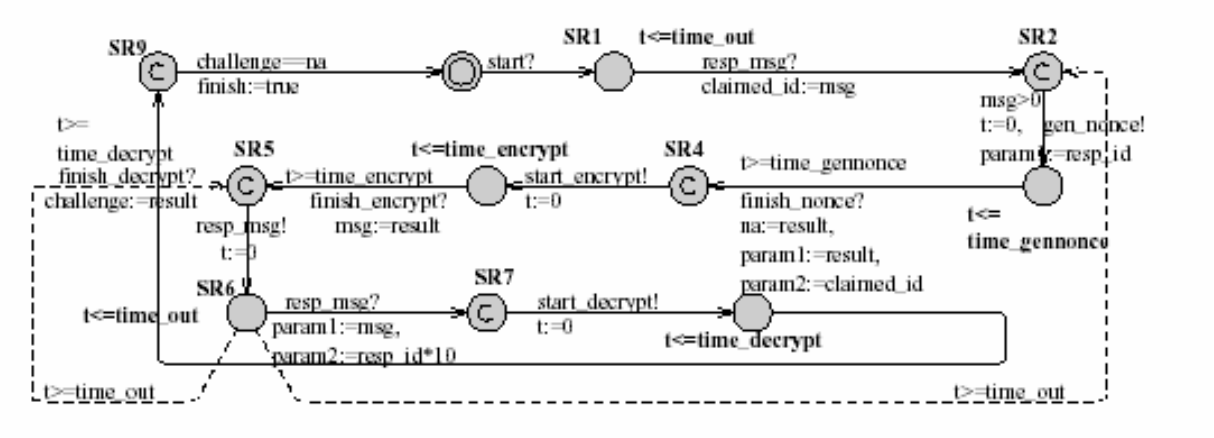
- Security of the Interaction
- In presence of malicious behaving peers

Aims

- Achieving security using simple tools
  - Embedded systems are resource-constrained
  - Bridge the gap between **formal and computational view** of security protocols
- Achieving security in complex systems
  - Think of e-payment
  - Integration of embedded systems in larger infrastructures
  - Main problems: **usage control and trust management**

A Couple of Highlights

- Common Criteria evaluation of Javacard product.
  - First time that a smart card at Evaluation Assurance Level 7
- An equational theory for electronic money
  - Modular exponentiation
  - Lead to a new project
- Verification of timed systems



Integration and Building Excellence

- Projects, e.g.
  - PRIAM (INRIA-Twente)
  - E-voting poject (VERIMAG, LSV, FT, LORIA)
  - Computer-Aided security (Verimag & INRIA)
- Dagstuhl Seminar (LSV, with Twente and many others)
- ARTIST + FOSAD summer school
- Regular visits
  - LSV-INRIA-Verimag
  - Inria-Twente
  - CNR-Twente
- Several publications with 2 or more partners involved.

Future Work

- *Practical* tools for protocol verification which take into consideration the weaknesses of the underlying crypto

- High level protocols for modelling and enforcing trust (i.e. Complex usage control policies) in services execution.

Thanks for your attention!

Main Aims for Integration

through Artist2

- **MAIN AIM:**
  Concerted effort on making state-of-the-art verification and testing technology *visible* and *easily accessible* for industry with long term vision of integration in tool chains applied in industry.

- **MEANS:**
  - Widespread industrial dissemination (*e.g.* work-based learning courses).
  - Continuous take-up of techniques in commercial tools, e.g. Esterel, Rhapsody, visualSTATE, Simulink, Trusted Tools, Object Geode.
  - Easy (=web) accessible repository of *mature tools* and *case studies.*
  - Scalability: European Verification Grid

Spreading of Excellence

Spreading of Excellence

TO OTHER RESEARCH COMMUNITIES

Model checking increasingly used in other areas. Invited talks and papers at:

- ICAPS: International Conf. on AI, Planning and Scheduling
- European Journal of Control
- IFAC Annual Reviews in Control
- ACM Performance Evaluation Review

CONFERENCES (Initiator, SC, Chair)

CAV, TACAS, FORMATS, EMSOFT, CONCUR, ETAPS, PSTV/FORTE, PAPM, HSCC, ARTS, PDMC, FTRTFT, FATES, TESTCOM, ..

Publications

During first year approximately 100 publications covering areas as

1. *Optimal scheduling and schedulability analysis*
2. *Monitoring, fault-diagnosis and controller synthesis*
3. *Robustness and implementability of quantitative models*
4. *Real-time testing and verification*
5. *Expressiveness and Decidability Results*
6. *Probabilistic Model Checking*
7. *Modelling and Verification of Security Properties*
8. *Distributed Model Checking*
9. *Case Studies, Methodologies and Tools*

13 papers are joint publications between two or more cluster partners.

High-Level Objectives

- **Quantitative Testing and Verification:**
  - Test case generation
  - Testing theories and analysis techniques for quantitative aspects;
  - Metrics for testing coverage;
  - Robustness and implementability;
  - Stochastic analysis;
    Optimal scheduling and Controller Synthesis.
- **Verification of Security Properties:**
  - Tools for security and communication protocols;
  - Security and trust management; security of services;
  - Bridging the gap between computational and formal aspects of cryptography.

Objectives and Industrial Impact

- Testing and Verification Platform for Embedded Systems
  - Improvement and availability of individual tools; Web-pages for tools (Yahooda) and case-studies; distributed analysis tools; common coordination layer for European verification Grid.

- Strong ties with ARTEMIS SRA:
  (Design Methods and Tools)
  - …methods and tools for simulation, validation and proving, …,and verification and validation….reduce cost by 50%; …50% reduction in development time. …manage 100% increase in complexity with 20% , etc.

- Number of industrial collaborations:
  - Danfoss, Ericisson Telebit, Ericsson Felix Ingrat, Skov, Océ, ASML, Philips,..

State of the Art - Research Trends

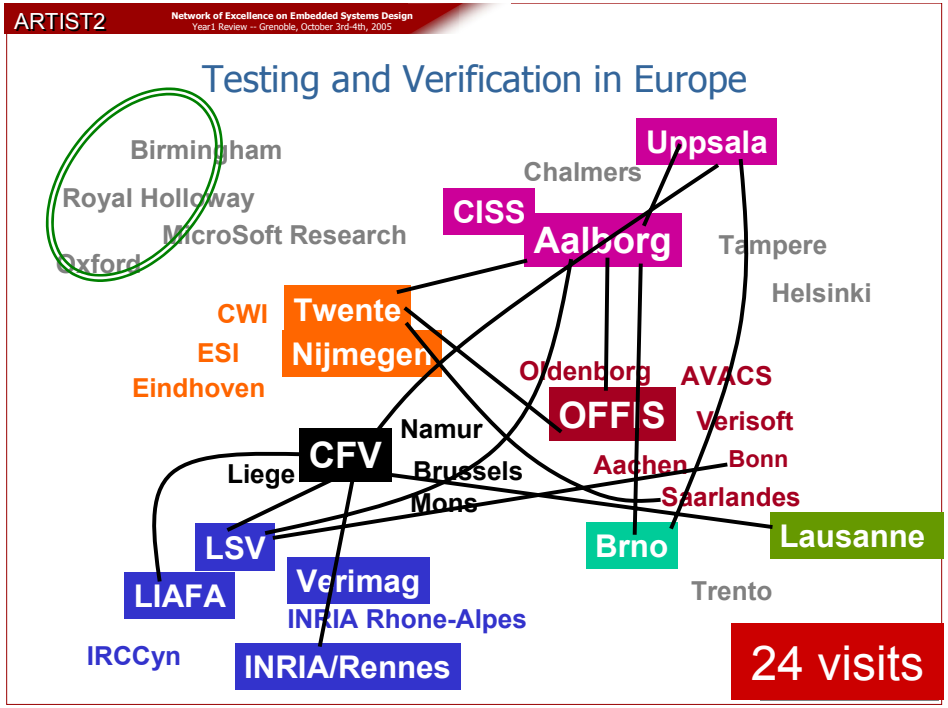
- **Software validation**
  - SLAM, Blast, Verisoft, Bandera, Java Pathfinder
  - Abstraction-refinement, static analysis, model checking
- **Modelling and validation of non-functional properties**
  - Data-intensive systems
  - Time, hybrid and resource/cost phenomena
  - Stochastic phenomena
- **Modelling and validation of security properties**
  - Specification and checking of richer security properties.
  - bridging the gap between the formal and the computational and views of security protocols modelling cryptographic aspects and algebraic properties

State of the Art - Research Trends

- **Bounded model-checking**
  - Exploitation of advances in SAT-solving
- **Extended scope of verification technology**
  - model-based testing, monitoring
  - scheduling and planning
  - controller synthesis
- **Robustness and Implementability**
  - of quantitative models
- **Extending the scope for distributed model checking**
  - safety properties → liveness properties
  - finite state models → quantitative models

Integration and Building Excellence

- **Extensive collaboration** with leading research teams outside Europe.
- **Strong impact** on a number of important international **conferences** (CAV, TACAS, FORMATS, EMSOFT, CONCUR, ETAPS, HSCC,..)
- High level of **dissemination** through PhD schools and industrial seminars (>30 keynote presentations).
- **ARTIST2 PhD schools** (Nässlingen, Xian, Trento, Suzhou).
- **PhD schools** organized by ARTIST2 partners: MOVEP, ARTES, FOSAD.
- **Transfer to industry** through long-term collaboration performed by individual partners. National centers and laboratories.
- **Additional European funding**
  - Prototype tools→ ARTIST2 platforms→ HRC→ Industrial tool chains;
  - European verification GRID.



Microsoft Research
Rice, Texas
NASA Ames
Kansas
Bangalore
Kestrel Technologies
Cadence
TCS
Weizmann
Haifa
Hebrew University

Assessment at Y0+2

- **Quantitative Testing and Verification** and **Verification of Security Properties** have been particularly active pursuing challenges ahead of plan, with very promising results.
- Prestigious awards, extensive list of publications (>120), key-note presentations, organization of workshops and conferences witness true excellence within the area. Joint proposals. Impact on EU/US collaboration.
- **Testing and Verification Platform**:
  - Advancement and dissemination of individual tools. Installation on common (powerful) server.
  - European T&V GRID common infrastructure:
    - Participation in two European meetings
    - A number of ongoing European projects wrt usage of HP and GRID for model checking.
    - Dependencies on design decisions still to be made by the GRID-computing community at large.
    - Exploitation of immediately available resources (NORDUGrid).
- **Dissemination** to industry has been done extensively during the second year by individual partners.

Coming Events

- ARTIST2 Winterschool Motives
  Trento, Italy, February 19-23.
- T&V Cluster Workshop, Trento, Italy, February 20.
- ARTIST2 Platform Workshop, DATE07, April 16-20, Nice: aiming at users.
- ARTIST2 Platform Workshop, CAV07, July 3-7, Berlin: aiming at verification community.
- ARTIST2 Platform Workshop, Embedded Systems Week.
- T&V Cluster Workshop, EPFL, Lausanne, Spring 2007.
- FORMATS07: workshop on Formalisms for Modeling and Analysis of Timed Systems.
- FOSAD07: school on Foundations of Security Analysis and Design.
- Participate in the ARTIST2 China Workshop.
- Initiate/participate in Inter-Cluster Activities on Security and Predictability.

Future Work

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

Future Work

- **Verification of Security Properties:**
  - Link between security and trust management.
  - Verification of more realistic protocols (e.g. group protocols, protocols for ad-hoc networks)
  - Verification of more realistic security properties (e.g. anonymity, stronger versions of secrecy).
  - Continue effort on bridging gap between computational and formal view of cryptography
  - Initiate Inter-Cluster activities on security issues.

Future Work

- **Testing & Verification Platform:**
  - Continued development of Web-repository for tools and case-studies.
  - Contributions to GRID infra-structure at large!
    Postpone development of infrastructure for dedicated verification GRID.
  - Links to platforms of other clusters, in particular Execution Platforms, Control, Real Time Components.
  - Interaction with SPEED on HRC profiles for quantitative verification.
- **Continued dissemination to industry**
  - Based on collaborations by individual partners and laboratories.

Outline

- Kim G. Larsen:
  Overview of Activities within the Cluster

- Ed Brinksma:
  Coverage Metrics for Testing
- Jean-Francois Raskin
  Controllers: Robustness and Synthesis
- Kim G. Larsen:
  Real-Time Validation Tools
- Sandro Etalle:
  Verification of Security Protocols

Highlevel objectives Y3

- Quantitatative Testing and Verification
  - Metrics for testing coverage
  - Abstraction methods and compositional techniques
  - Optimal scheduling & controller synthesis
  - Robustness and implementability
  - Stochastic, timed and hybrid models
- Testing and Verification Platform
  - Individual tools
  - Dissemination through industrial case studies (web)
  - Verification Server and Grid
- Verification of Security Properties
  - Bridge gap between formal and computational schools
  - Verification of voting and e-payment protocols
  - New trust model

Quantitative Testing and Verification
problems to be dealt with

- Verification
  - Efficient tool for LTL model-checking exploiting the research done for synthesis for partial observability
  - Abstraction / refinement
  - Efficient automata-based symbolic representations of sets of integers
- Testing
  - Monte Carlo simulation techniques for DFT (dynamic fault trees)
  - Semantic framework test coverage (secco).
  - Testing and learning

Quantitative Testing and Verification
problems to be dealt with

- Abstraction and Approximate Analysis
  - Suitable abstractions between (priced) timed games preserving winning strategies.
- Robustness and Quantitative Analysis
  - Metrics on stochastic games
  - Qualitative and quantitative verification on probabilistic models
- Controller Synthesis and Optimal Scheduling
  - Synthesis of robust controllers (under partial observability)
  - Implementation of on-the-fly algorithms for priced timed games; Undecidability 😐 Zones → Polyhedra ☺
  - Priced timed games under partial observability (decidability?)