Year 2 Review
Paris, November 8th and 9th, 2006

Achievements and Perspectives :

Testing and Verification

Cluster leader : Kim Guldstrand Larsen

CISS, Aalborg University, Denmark

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

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.

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

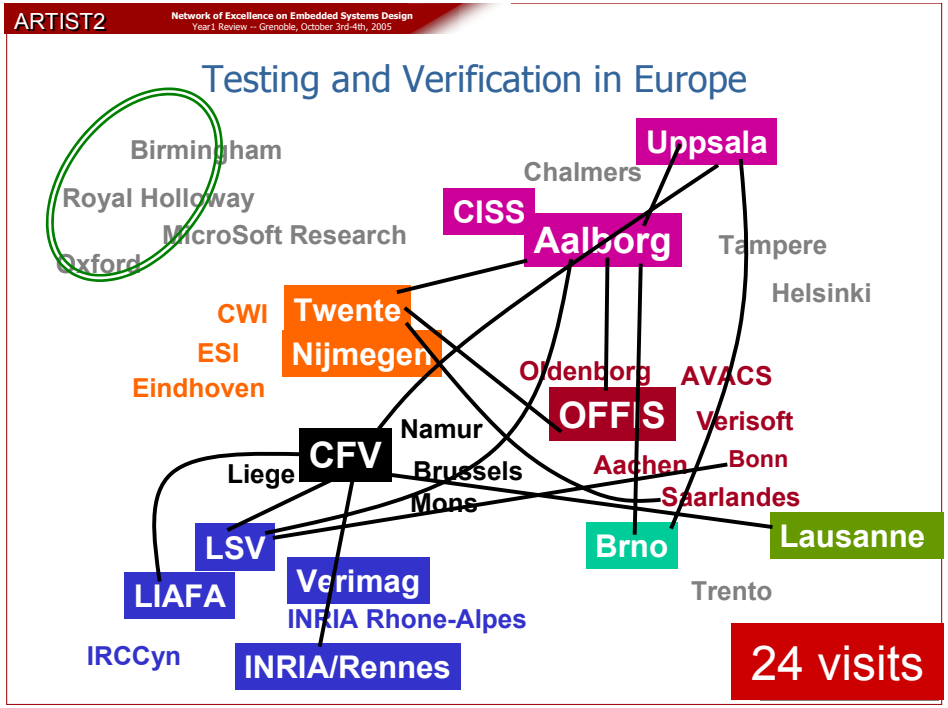
- **Software validation**
  - SLAM, Blast, Verisoft, Bandera, Java Pathfinder
  - Abstraction-refinement, static analysis, model checking
- **Modelling and validation of non-functional properties**
  - Data-intensive systems
  - Time, hybrid and resource/cost phenomena
  - Stochastic phenomena
- **Modelling 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