ARTIST2 – Year 1 Review

Grenoble, October 3rd-4th, 2005

Cluster Presentation:
Testing and Verification

Kim G. Larsen: Cluster Leader
CISS, Aalborg U, DK

Ed Brinksma: Activity Leader
Twente U, NL

Yassine Lakhnech: Activity Leader
Verimag, F

Outline of the Presentation

Presentation of the Cluster

- Core and Affiliated Partners, Competencies and Roles
- Research Activities & Platform

Description of the Area

- Main Research Trends
- Industrial Applications

State of Integration in Europe

- European Research Teams
- Main Aims for Integration through Artist2
- Spreading Excellence & Mobility

Overall Aims and Vision for the Cluster

- Overall Assessment
- Recommendations and Visions

Presentation of the Cluster ?

❖ Core Partners

- ➢ CISS, Aalborg University
  (real-time verification and testing toos, controller synthesis, security and mobility)
- ➢ 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)

Presentation of the Cluster ?

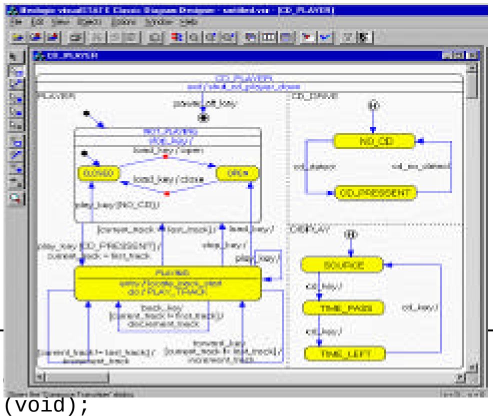
- **Affiliated Partners**
  - Masaryk University in Brno
    (distributed model checking)
  - EPFL,Lausanne
    (model checking embedded
  - and hybrid systems)
  - Nijmegen
    (Testing data-dependent systems)
  - LIAFA, Paris
    (Real-time and hybrid model checking)
  - University of Firenze
    (Competency)
  - INRIA
    (Proofs and Protocols)
  - FTR&D
    (security protocols)
  - Telelogic
    (Tool provider)
  - IAR Systems A/S
    (Tool providcer)
  - Siemens Mobile Phones A/S
    (End-user of model-driven methodology)
  - ABB Automation
    (Validation of industrial robots)
  - EneaEDF
    (RTOS and testing)
  - Terma
    (Hardware verification)
  - SchlumbergerSema
    (Smart card verification)
  - Trusted Logics
    (Secure components and Smart Cards)

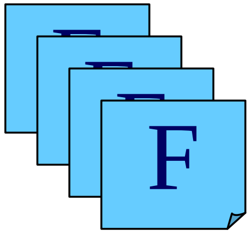
Cluster Activities

- ❖ JPRA-Cluster Integration
  Quantitative Testing and Verification (Ed Brinksma)
- ❖ JPRA-Cluster Integration
  Verification of Security Properties (Yassine Lakhnech)
- ❖ JPIA-Platform:
  Testing and Verification Platform (Kim G. Larsen)

Verification and Testing

Model





Req

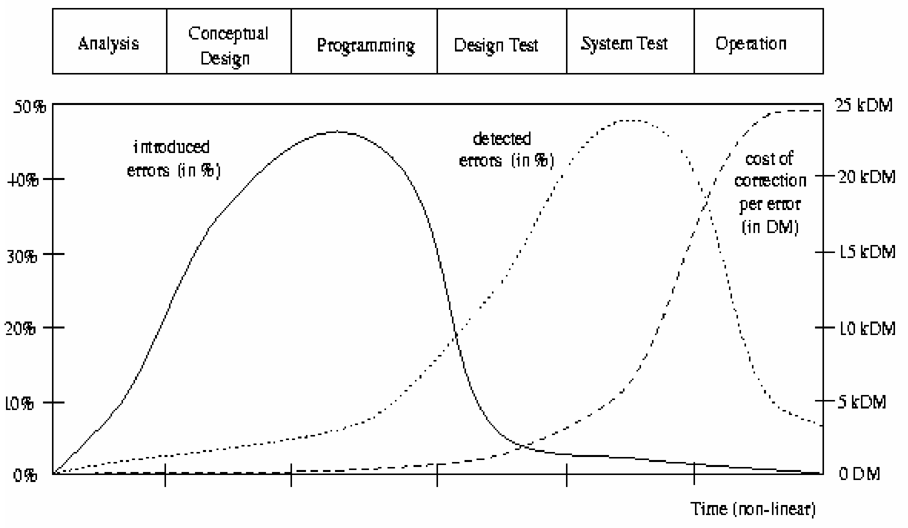
```
/* Wait for
void OS_Wait(void);

/* Operating system visualSTATE process. Mimics a OS p
 * visualSTATE system. In this implementati
 * interfacing to the visualSTATE
void OS_VS_Process(void);

/* Define completion code v
unsigned char cc;

void HandleError(unsigned ch
{
  printf("Error code %c detec
  exit(ccArg);
}


/* In d-241 we only use the OS_V      call. It is used to simulate a
 * system. It purpose is to generate events. How this is done is up to
 * you.
 */
void OS_Wait(void)
{
  /*  Ignore the parameters; just retrieve events from the keyboard and
   *  put them into the queue. When EVENT_UNDEFINED is read from the
   *  keyboard, return to the calling process. */
  SEM_EVENT_TYPE event;
  int num;
```

Code

- Verification
  Code/Model wrt Req
- Testing
  System wrt Model/Req

Running System

Why Testing and Verification



❖ **POTENTIAL**:

30-40% of production time is currently spend on elaborate, ad-hoc testing

- ➢ The potential of existing/improved testing methods and tools is enormous
- ➢ Time-to-market may be shortened considerable by verification and performance analyses of early designs

❖ **COMMONALITY**:

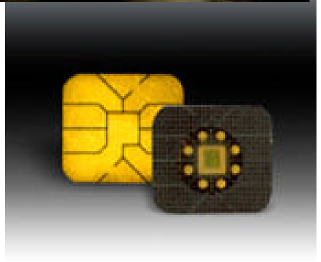
Transversal topic, interacts with all other topics in embedded systems design:

- ➢ Modelling and Components (verification, model-based testing)
- ➢ Hard and adaptive real time (optimal scheduling & schedulability analysis)
- ➢ Execution platform (performance analysis, security)
- ➢ Compilers and timing analysis (WCET and compact code-generation)

Why Testing and Verification

❖ IMPORTANCE for EMBEDDED SYSTEMS

- ➢ Often safety critical
- ➢ Often economical critical
- ➢ Hard to patch



❖ CHALLENGES for EMBEDDED SYSTEMS

- ➢ Correctness of embedded systems depend crucially on use of *resources* (real-time, memory, bandwidth, energy).
  Need for verification of and conformance testing with respect to quantitative models.
- ➢ Participation in mobile ad-hoc networks require particular attention to security aspects.

Main Research Trends

- **Software validation**
  - SLAM, Blast, Verisoft, Bandera, Java Pathfinder
  - Abstraction-refinement, static analysis, model checking
- **Bounded model-checking**
  - Exploitation of advances in SAT-solving
- **Modelling and validation of non-functional properties**
  - time, hybrid, resource/cost, stochastic phenomena
- **Modelling and validation of security properties**
- **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

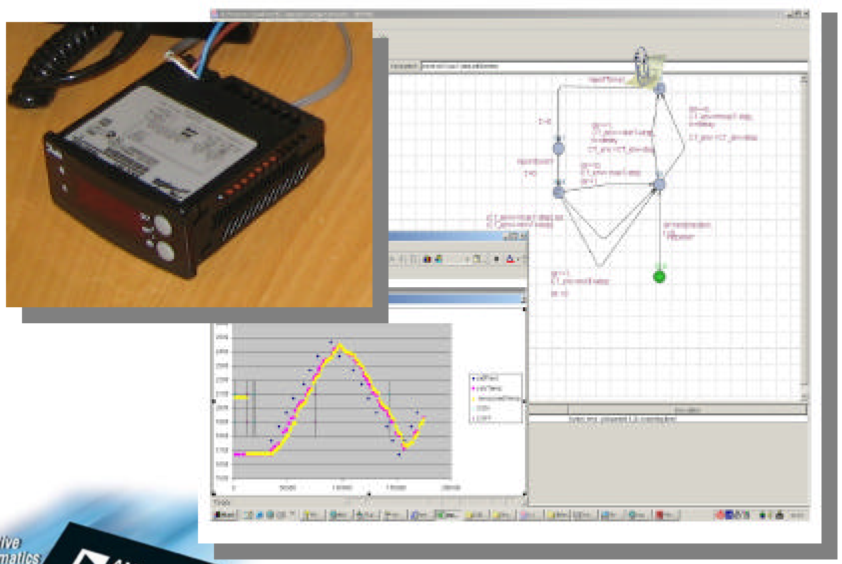
Industrial Applications

❖A large collection of ongoing industrial projects carried out by individual partners:

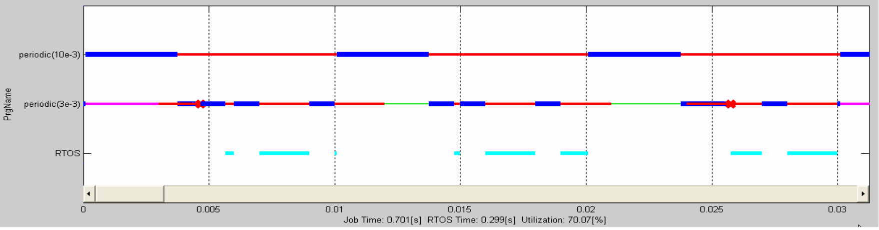
❖Representative samples:

- ➢ ***France Telecom***: formal validation of vocal phone services.
- ➢ ***CEA***: verification and validation process of programs with floating-point numbers
- ➢ ***BMW***: test the efficiency of the formal verification techniques based on the active front steering (AFS) developed for the 5-Series BMW
- ➢ ***Danfoss***: model-based code-generation and testing of a refrigeration controller
- ➢ ***Terma***: modelling and verification of memory interface of a radar system
- ➢ ***Ericsson Telebit***: domain-specific methodology for off- and on-line test-case generation from so-called RFC
- ➢ ***Analoge Devices:*** Synthesis of energy optimal schedule for DVS processor

Danfoss Electronic Cooling Controller (16K)



Analoge Devices Blackfin DVS Processor



❖ Work towards a repository of case-studies.

Testing and Verification in Europe

Birmingham

Royal Holloway

MicroSoft Research

Oxford

Uppsala

Chalmers

CISS

Aalborg

Tampere

Helsinki

CWI

Twente

ESI

Nijmegen

Eindhoven

Oldenborg

AVACS

OFFIS

Verisoft

Namur

Liege

CFV

Brussels

Mons

Aachen

Bonn

Saarlandes

LSV

LIAFA

Verimag

INRIA Rhone-Alpes

IRCCyn

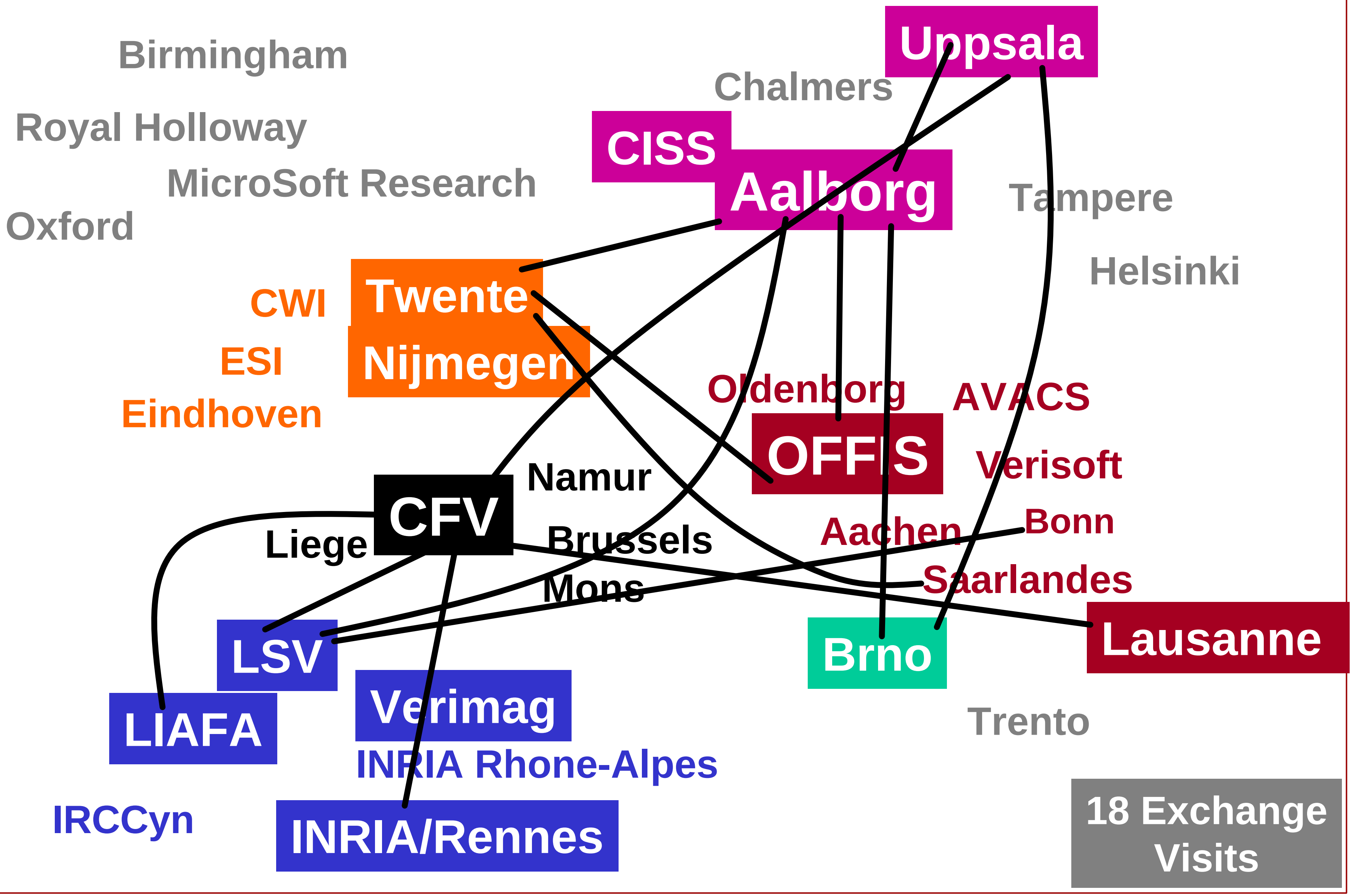
INRIA/Rennes

Brno

Lausanne

Trento

Testing and Verification in Europe



Birmingham
Royal Holloway
MicroSoft Research
Oxford
Chalmers
Uppsala
CISS
Aalborg
Tampere
Helsinki
CWI
Twente
ESI
Nijmegen
Eindhoven
Oldenborg
AVACS
OFFIS
Verisoft
Namur
CFV
Liege
Brussels
Mons
Aachen
Bonn
Saarlandes
Lausanne
LSV
Brno
LIAFA
Verimag
INRIA Rhone-Alpes
Trento
IRCCyn
INRIA/Rennes
18 Exchange Visits

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.*
- ➢ Ultimate means: European Verification Grid

Spreading of Excellence

TO INDUSTRY & PhD STUDENTS

- Dagstuhl Meeting on Testing, September 5-10, 2004
- Formal Methods and Components and Objects, Eindhoven, Nov, 2004
- Embedded Systems Testing – Trends and Vision, Aalborg, Dec 1, 2004
- MOVEP04, Brussels, 13-17 December 2004
- Embedded World, Nürnberg, February 22-24, 2005
- German Verification Day, Oldenborg, March 3, 2005
- Security Spring School, Marseille, April 25-29, 2005
- Workshop on the Links between Formal and Computational Models for Security Protocols, Paris, June 23-24, 2005.
- ARTIST2 Summerschool on
  Modelling and Components, Testing and Verification,
  Static Analysis
  Nässlingen, Sweden, September 29 – October 2 , 2005
- TECS, Pune, India, January 3-7, 2006.

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.

Overall Assessment

- ❖ Each research activity has demonstrated a high level of convergence in goals pursued.
- ❖ Extensive list of publications witnesses true excellence within the area.

- ❖ *Quantitative Testing and Verification* and *Verification of Security Properties* are largely carried out by disjoint groups of people (but highly overlapping teams).
- ❖ *Quantitative Testing and Verification* and *Testing and Verification Platform* are tightly connected with overlapping groups of people.

- ❖ Substantial effort has been put by individual partners in bridging the gap between current industrial practice and existing academic state-of-the-art technology.

Recommendations and Vision

- ❖ High demand and interest from industry
  →
  more disseminating activities for industry should be organized. In particular we suggest a school on:

  "Testing, Verification and Security of Embedded Systems"

- ❖ Establish cross-cluster activities with other clusters
  - in particular Models and Components.

- ❖ It is necessary to involve research teams outside the cluster working on parallel and distributed model checking in pursuing the vision of a European Verification Grid.

- ❖ **OVERALL VISION**: to provide domain-specific testing and verification methodologies for embedded systems well-integrated with the complete chain of tools applied by industry.

Schedule & Milestones

Joint Cluster Meeting (w. parallel sessions) medio December

Quantitative Testing & Verification

A. Foundation for black-box testing of real-time systems established

T0+6:
a. Soundness and limit-completeness
b. Metric for coverage.
T0+18:
a. Computability and Complexity of learnability.

B. Improved tools for quantitative analysis with experimental evaluation

T0+6:
a. Improved symbolic datastructures
b. Heuristics for efficient guiding
T0+18:
a. Abstraction methods
b. Comparison with (MI)LP and OR

C. Industrial case studies.

T0+6:
Collection of case studies on web.
T0+18:
Classification of case studies

Verification of Security Properties

A: Cryptographic protocols

T0+6:
a. A common language for security protocols
b. A publicly available data base of security protocols and their analysis (attacks, proofs, assumptions/properties,...)
T0+18:
a. A validation tool set that is accessible via the web.
b. Two industrial case studies that are already available.

B: Certification technology and virtual machine validation

T0+6:
A methodology for certification of the levels EAL6 and EAL7 of the common criteria.
T0+18:
A tool set for certification of the levels EAL6 and EAL7 of the common criteria.

Testing & Verification Platform

A. Testing and Verification Server:

T0+06:
Evaluation of main testing and verification tools wrt maturity for integration.
T0+18:
Installed and configured (virtual) server

B. Parallel and Distribution Model Checking (PDMC):

T0+6:
Evaluation of tools currently supporting PDMC on local PC-clusters.
T0+18:
Design of coordination layer for integrating PDMC methods.

C. European Test and Verification GRID

T0+6:
Preevaluation of UPPAAL running on NORDUGRID
T0+18:
Design of GRID infrastructure

END

☺☺☺

Schedule & Milestones

Joint Cluster Meeting (w. parallel sessions) medio December

Quantitative Testing & Verification

A. Foundation for black-box testing of real-time systems established

T0+6:
a. Soundness and limit-completeness
b. Metric for coverage.
T0+18:
a. ~~Computability and Complexity of learnability~~.
b. Robustness and Implementability

B. Improved tools for quantitative analysis with experimental evaluation

T0+6:
a. Improved symbolic datastructures
b. Heuristics for efficient guiding
T0+18:
a. Abstraction methods
b. Comparison with (MI)LP and OR
c. Stochastic Model Checking
d. Controller Synthesis

C. Industrial case studies.

T0+6:
Collection of case studies on web.
T0+18:
Classification of case studies

Verification of Security Properties

A: Cryptographic protocols

T0+6:
a. A common language for security protocols
b. A publicly available data base of security protocols and their analysis (attacks, proofs, assumptions/properties,...)
T0+18:
a. A validation tool set that is accessible via the web.
b. Two industrial case studies that are already available.

B: Certification technology and virtual machine validation

T0+6:
A methodology for certification of the levels EAL6 and EAL7 of the common criteria.
T0+18:
A (prototype) tool set for certification of the levels EAL6 and EAL7 of the common criteria.

Testing & Verification Platform

A. Testing and Verification Server:

T0+06:
Evaluation of main testing and verification tools wrt maturity for integration.
T0+18:
~~Installed and configured (virtual) server~~
Links to mature/stable versions

B. Parallel and Distribution Model Checking (PDMC):

T0+6:
Evaluation of tools currently supporting PDMC on local PC-clusters.
T0+18:
(Initiate) design of coordination layer for integrating PDMC methods.

C. European Test and Verification GRID

T0+6:
Preevaluation of UPPAAL running on NORDUGRID
T0+18:
Design of GRID infrastructure