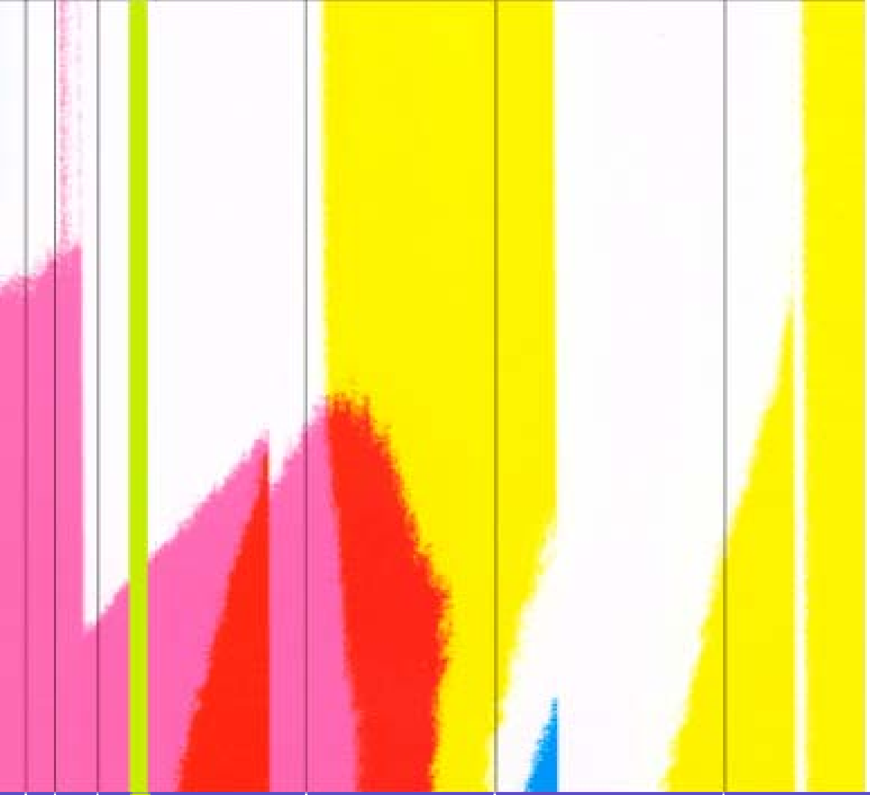


Evaluation INRIA ComC
The VASY Project-Team

April 24-25, 2007

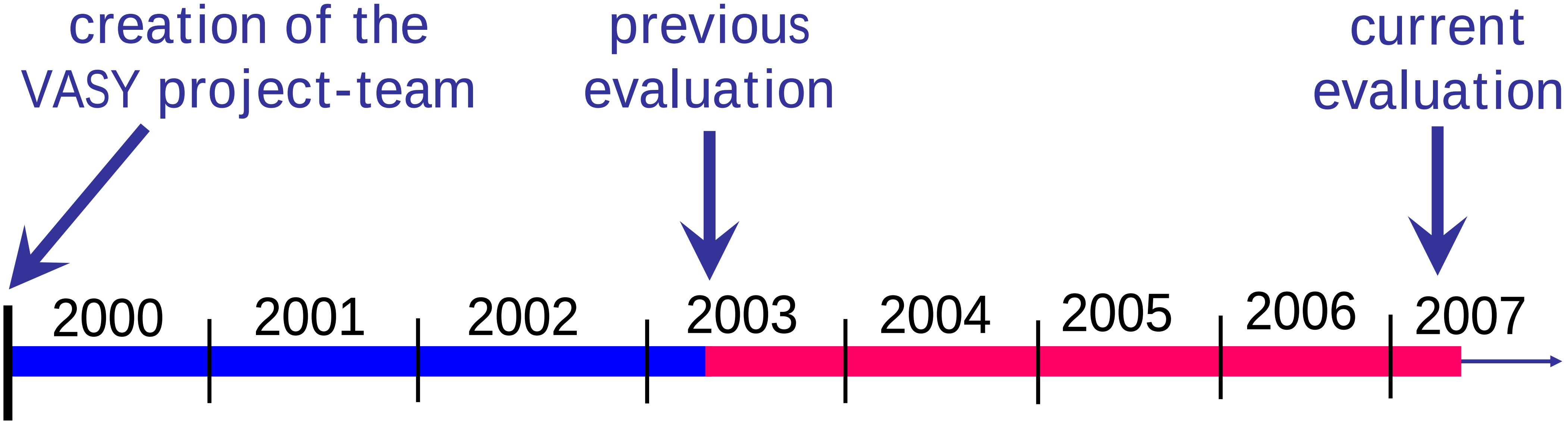
40 ans
la révolution de l'information

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA
RHÔNE-ALPES

Hubert Garavel
Centre de recherche INRIA de Grenoble Rhône-Alpes

A note about timing



Scientific topics of VASY

Motivations

Design of reliable computer systems

Focus on asynchronous concurrency

- Distributed processes
- Message-passing communications

Various application domains

- telecommunications
- software
- hardware

Promotion of formal approaches

Development of software tools

‘Transfer theoretical concurrency results into robust tools for research, education, and industry’

Three scientific directions

1. Languages and compiling techniques

- Formal specification of concurrent systems
- Langages supporting asynchronous concurrency
- Process algebras and functional / imperative languages
- Standards: LOTOS [ISO 8807], E-LOTOS [ISO 15437]
- Compiling techniques, code generation, static analysis
- Simulation, rapid prototyping

2. Models and verification techniques

- Formal models for asynchronous concurrency
  - Petri Nets extended with data
  - Communicating automata extended with data and time
  - Boolean equation systems
  - Probabilistic/stochastic models

Three scientific directions

2. Models and verification techniques (cont'd)

- ‘Explicit-state’ methods
  - Reachability analysis
  - On-the-fly verification
  - Compositional verification
  - Distributed verification
- Logical properties (*model checking*)
  - Modal mu-calculus extended with data
- Behavioural properties (*equivalence checking*)
  - Bisimulations
- Performance properties
- Generic software components for verification

3. Industrial applications

- Embedded systems
- Circuits and hardware architectures

Scientific work done by VASY since the previous evaluation (March 2003-April 2007)

40 ans
la révolution de l'information

INRIA
RHÔNE-ALPES

VASY staff (Jan. 2003 – Dec. 2006): 25 persons

4 INRIA scientists: Hubert Garavel, Radu Mateescu (including 18 months in Lyon at LIP-ENSL), Frédéric Lang, Wendelin Serwe (since Sep. 2004)

1 Bull engineer: Solofo Ramangalahy (17 months)

3 post-docs: Aurore Collomb (18 months), Gwen Salaün (25 months), Olivier Ponsini (3 months)

2 PhD students: Christophe Joubert (39 months), Jan Stöcker (4 months)

1 MSc student: Abdul-Malik Khan (6 months)

5 expert engineers: Damien Bergamini (24 months), David Champelovier (48 months), Nicolas Descoubes (24 months), Frédéric Tronel (6 months), Marie Vidal (6 months)

5 computer-science students: Alban Catry (7 months), Damien Thivolle (9 months), Jérôme Fereyre (12 months), Nathalie Lépy (10 months), Guillaume Schaeffer (6 months)

1/3 assistant : Valérie Gardès (15 months), Catherine Magnin (9 months), Elodie Toihein (24 months)

VASY external funding (contracts) : 2003 – 2006

ARC Modocop	2002 - 2003
RNTL Parfums	2001 - 2003
ACI Fiacre	2004 - 2007
RNTL OpenEmbedd	2006 - 2009
IST6 Archware	2002 - 2005
Associated team SENVA	2004 - 2007
Bull FormalFame	2003 - 2004
Bull FormalFame Plus	2004 - 2007

Software: the CADP toolbox

A verification toolbox for asynchronous systems

Modular, extensible architecture (APIs)

Generic software components for verification

Main functionalities:

- Several input languages
- Step-by-step simulation
- Rapid prototyping
- Model checking
- Equivalence checking
- Test generation
- Performance evaluation

#1: Next generation specification languages

- Enhanced CAESAR compilers for LOTOS (time, memory, user-friendliness)
- Optimized TRAIAN compiler for LOTOS NT (memory) (55,000 loc)
- LNT2LOTOS translator (18,600 loc)
- CHP2LOTOS translator (19,500 loc)
- FSP2LOTOS translator (25,500 loc)
- NTIF intermediate semantic model (13,300 loc)
- FIACRE intermediate model = NTIF + VCOTRE

#2: Fight against state explosion

- CAESAR 7.0: static analysis to reduce state spaces by several orders of magnitude, still preserving strong bisimulation
- Tools for on-the-fly verification (see later)
- Tools for compositional verification:
  - 4 tools completed
  - automatic interface generation
- Tools for distributed verification

#3: Temporal logic extended with data

- AAL (*Architecture Analysis Language*) (7,500 loc)
  - model checker for software architectures and architectural styles
  - developed in the IST6 Archware project
- EVALUATOR 3.5 (10,700 loc)
  - on-the-fly model checker for μ-calculus with regular expressions
  - diagnostic generation (counterexamples)
  - used in 28 industrial case-studies
- EVALUATOR 4.0 (48,700 loc)
  - model checker for the new MCL language
  - MCL = value-passing modal μ-calculus with data types
  - under intensive test campaign

#4: Generic software components

- Several new OPEN/CAESAR libraries
- CAESAR_SOLVE library for solving Boolean equation systems on-the-fly (12,200 loc)
- Tools for equivalence checking based on CAESAR_SOLVE:
  - BISIMULATOR : comparison for 7 equivalences (16,000 loc)
  - REDUCTOR : minimization for 8 equivalences (2,000 loc)
- Tools for compositional performance evaluation
  - discrete-time and continuous-time Markov chains
  - numerical solvers for transient and steady-state analysis
  - stochastic minimization tool

Release of CADP 2006 "Edinburgh" (Dec. 2006)

15 new tools and software libraries

- Explicit state space generation

  CAESAR 7.0, CAESAR.BDD

- Compositional verification

  BCG_GRAPH, EXP.OPEN 2.0, PROJECTOR 2.0

- On-the-fly verification

  CAESAR_SOLVE, BISIMULATOR , EVALUATOR 3.5, REDUCTOR 5.0

- Distributed verification

  BCG_MERGE, DISTRIBUTOR

- Performance evaluation

  BCG_STEADY, BCG_TRANSIENT, DETERMINATOR

- Trace-based verification

  SEQ.OPEN

Some figures about CADP 2006

42 tools

17 software libraries

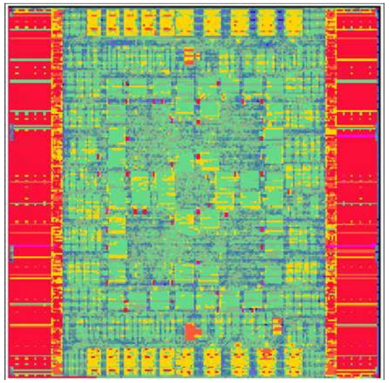
4 computing platforms supported

- Sun/Solaris, PC/Linux, PC/Windows, MacOS

International dissemination

- license agreements signed with 372 organizations
- licenses granted for 822 machines in 2006
- 94 case-studies accomplished using CADP
- 29 research tools connected to CADP
- 28 university lectures based on CADP (since 2002)

Two significant applications



FSS chip of FAME1
(60 million gates)

FAME1 multiprocessor architecture (Bull)

- CADP discovered issues in the FSS, a critical circuit of Bull's NovaScale servers (at the core of the Tera10 supercomputer)
- CADP tools became part of Bull's validation methodology

FAUST1 network-on-chip (CEA/Leti)

- formal verification of the FAUST1 input stage using CADP and CHP2LOTOS
- recent publication at ASYNC'07 (Berkeley, CA, USA)

Overall assessment

Work done is in line with the initial goals defined in the VASY workplan (2003)

New research directions have emerged or developed:

- Hardware verification (in collaboration with CEA/Leti and STMicroelectronics)
- Semantic translations from various languages (CHP, FDR2, FSP, SystemC/TLM) to LOTOS
- Bio-informatics (in connection with the HELIX project-team)

Former recommendations have been addressed

1. Over-emphasis on E-LOTOS draining resources from CADP
   ⇒ Bull has funded the development of the LNT2LOTOS translator, which should eventually become part of CADP
   ⇒ STMicroelectronics is planning to experiment LNT2LOTOS
2. Lack of industrial interest in formal methods (in favour of semi-formal methods)
   ⇒ Hardware designers (Bull, CEA, STM) already use LOTOS
   ⇒ Aerospace companies (Airbus, Astrium, Thales, etc.) plan to introduce formal verification (including a connection to CADP) in their tool chains
3. Team instability, with a negative impact on tool development
   ⇒ Radu Mateescu remained a member of Vasy (Lyon, then Dijon)
   ⇒ David Champelovier (expert engineer) contract was extended to 6 years
4. Lack of students to develop the next generation of Vasy members
   ⇒ Vasy became associated with Grenoble Universities (LIG laboratory)
   ⇒ Three new VASY PhD students hired directly by Bull, INRIA, and STM
5. Overdependence on Bull for industrial funding
   ⇒ We diversified funding by cooperating with Airbus, CEA/Leti, and STM

Goals of VASY for the next 4-year period

Two scientific opportunities for VASY

Motivation: transfer concurrency theory results to industry

- Asynchrony everywhere in circuits and hardware architectures

  asynchronous logic, multi-core processors, network-on-chip, system-on-chip, multiprocessor architectures (CC-NUMA)

  ⇒ VASY is part of *pôle de compétitivité* **Minalogic** (Grenoble)

- Models everywhere in software and system engineering

  move from merely syntactic models to semantic models for real-time and asynchronous behaviours (Marte, Fiacre, etc.)

  ⇒ VASY is part of *pôle de compétitivité* **AESE** (Toulouse)

External funding (contracts) : 2007 – 2010

Software development requires strategy and manpower:

- VASY established strong collaborations with Airbus, Bull, CEA/Léti, and STMicroelectrics
- VASY has a clear budget visibility for the next period

RNTL OpenEmbedd	2006 - 2009
AESE Topcased	2006 - 2010
Minalogic Multival	2006 - 2009
IST6 EC-MOAN	2007 - 2009

1. Specification and modelling languages

- Maintain activity on LOTOS
  - support to users in hardware industry
  - more state space reductions using static analysis
- Develop / finish translators for other languages
  - CHP2LOTOS (with CEA/Leti and TIMA)
  - FDR2LOTOS
  - FSP2LOTOS (with Imperial College)
  - TLM2LOTOS (with STMicroelectronics)
- Provide next generation languages
  - LNT2LOTOS translator (with Bull)
  - TRAIAN native compiler for LOTOS NT
  - NTIF / FIACRE intermediate models (with LAAS-CNRS)

2. Verification and performance evaluation

- On-the-fly model and equivalence checking
  - EVALUATOR 4.0 (model checking with data)
  - new algorithms for solving Boolean equation systems
  - on-the-fly state space reductors
- Distributed verification using clusters and grids
  - distributed solver for Boolean equation systems
  - distributed equivalence checking
  - distributed model checking
- Combining verification and performance evaluation
  - new stochastic bisimulations
  - on-the-fly simulation methods

3. Well-chosen, challenging case-studies

- Avionics embedded software (Airbus, Thales)
- Complex hardware architectures
  - FAME2 CC-NUMA architecture (Bull)
  - xSTream system-on-chip (STMicroelectronics)
  - FAUST2 network-on-chip (CEA/Leti)
  - embedded BLITTER block (STMicroelectronics)
- Bio-informatics (EC-MOAN partners)

4. High quality software tools

- Integration of prototype tools in next CADP releases
- Porting all the CADP tools to 64-bit architectures
- Connection of the CADP tools to the Eclipse platform
- Building of large non-regression testing data bases
- Semantics-aware testing to ensure quality

Planned growth of the VASY project-team

- Currently: 19 persons in April 2007
- Objective: 24 persons
- Based in Grenoble (19 persons) with research offices in Dijon (4-5 persons)
- Strong collaboration with industry (1 Bull employee and 2 STMicroelectronics employees in VASY)
- Connections with local universities in Dijon (LE2I laboratory) and Grenoble (LIG laboratory)
- Invited professor: Holger Hermanns (Saarland University)

More information…

http://www.inrialpes.fr/vasy

VASY