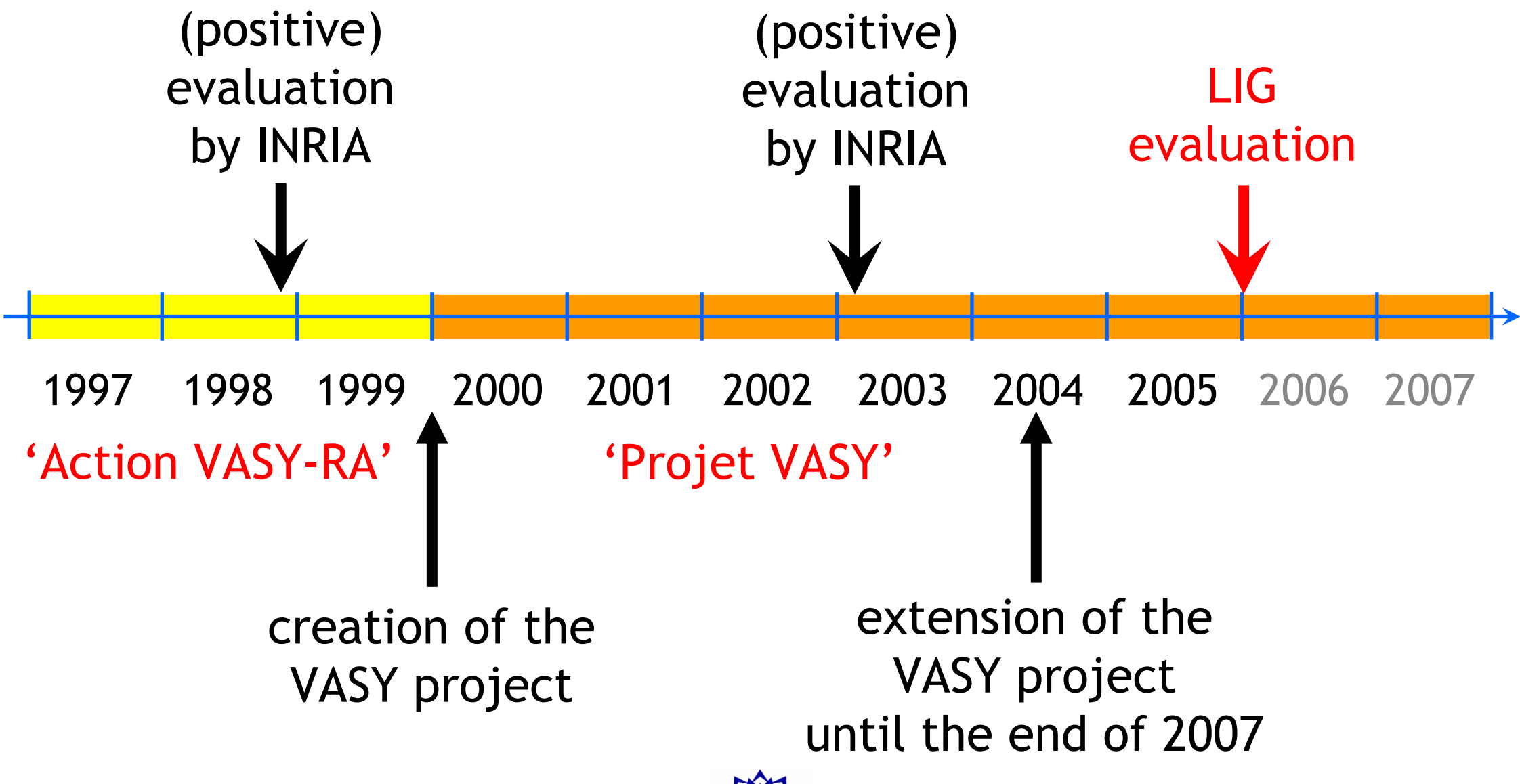
The VASY Team
Validation of Systems

Hubert Garavel

INRIA Rhône-Alpes
655, avenue de l'Europe
38330 Montbonnot Saint Martin
France

History of the VASY team



The VASY team staff

(January 2006)

The Vasy team: 11 persons

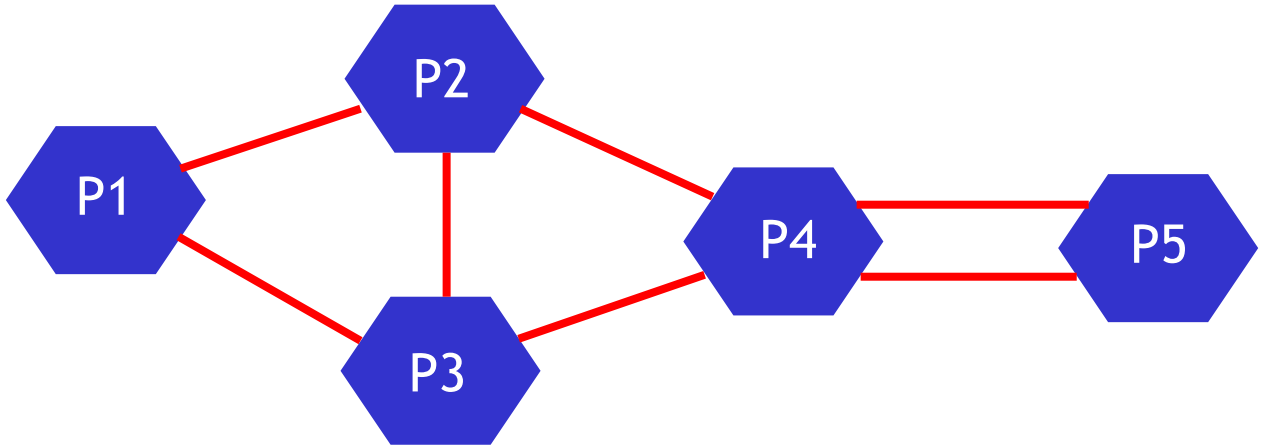
- INRIA scientists: 4
  - Hubert Garavel (DR2)
  - Radu Mateescu (CR1) since oct. 1998
  - Frédéric Lang (CR1) since sep. 2001
  - Wendelin Serwe (CR2) since sep. 2004
- Assistant: 1 Elodie Toihen
- Post-docs: 1 Gwen Salaün
- PhD students: 0
- M2R students: 1 Abdul-Malik Khan
- Expert engineers: 1 David Champelovier
- Computer-science students: 3
  Jérôme Fereyre, Nathalie Lépy, Damien Thivolle

Three remarks about human resources

- VASY is currently bi-localized:
  - 9 persons in Montbonnot (INRIA Rhône-Alpes)
  - 2 persons in Lyon (LIP-ENSL / INRIA Rhône-Alpes)
- Turnover (students and short-term contracts)
  - 35 persons in VASY since 2000
  - not optimal for long-term software development
- Lack of PhD students
  - A critical issue for several LIG teams

Scientific topics of VASY

Asynchronous systems



- several processes (or tasks, agents, entities)
- that execute concurrently (in parallel)
- at different speeds (no central clock)
- with message-passing communications
- without shared memory (unless explicitly modelled)
- with unspecified communication latencies

Numerous application areas

- Hardware design
  - multiprocessor architectures
  - bus arbitration protocols
  - cache coherency protocols
  - asynchronous logic circuits
  - network on chip, etc.
- Telecommunications
  - protocols and services
- Software
  - distributed systems
  - mobile agents
  - clusters, grids, P2P networks, etc.

Research directions of the VASY team

- Design of reliable asynchronous systems
- Promotion of formal approaches:
  - process calculi
  - model checking (mu-calculus…)
  - equivalence checking (bisimulations…)
- Development of robust software tools

‘Turning formal methods dreams into reality’

Three main scientific directions

1. Specification languages and compilers
2. Formal models and verification
3. Software tools and industrial applications

1. Specification languages and compilers

Formal specification languages

- Formal langages for asynchronous concurrency
- Process algebras and functional languages
- First generation: LOTOS [ISO standard 8807]
- Next generation: E-LOTOS [ISO standard 15437], LOTOS NT
- Other languages:
  - CHP (TIMA)
  - FSP (Imperial College)
  - CSP/FDR2 (Oxford)
  - Connections with mCRL, Erlang, Java …

Motivations

1. Process algebras (LOTOS, mCRL…) are valuable when used by experts (steep learning curve)
2. General-purpose languages (C/C++, Java…) offer little support for asynchronous concurrency
3. Graphical languages (SDL, UML) are too heavy and lack formality required for mechanized proofs
4. Process algebras are the solution, but need user-friendly enhancements (=> LOTOS NT)

Compiler technology

- Goals:
  - Verification
  - Simulation
  - Rapid prototyping
- Requirements :
  - Compiler theory
  - Data flow analysis
  - Code generation

Tools developed so far…

- LOTOS data types (CAESAR.ADT compiler)
  - 'Dynamic' data types (lists, trees…)
  - Reduction of pointer usage
  - Sub-term sharing
- LOTOS processes (CAESAR compiler)
  - Rich semantic model (enhanced Petri nets)
  - State space reductions
- E-LOTOS data types (TRAIAN compiler)
- E-LOTOS processes:
  - New semantic model needed: NTIF
  - New algorithms required

2. Formal models and verification

Semantic models

- Formal models for asynchronous concurrency
  - Petri Nets extended with data
  - Communicating automata extended with data/ time
  - Boolean equation systems
- Logical properties (*model checking*)
  - Modal mu-calculus (extended with data)
- Behavioural properties (*equivalence checking*)
  - Bisimulations
- Performance evaluation
  - Probabilistic/stochastic models

Verification challenges

- A fundamental issue:
  - Fighting state explosion for asynchronous systems
- A technological issue:
  - Designing generic components for simulation, verification, and testing

Verification approaches

- Enumerative verification
  - BCG software environment
- On the fly verification
  - OPEN/CAESAR software environment
  - CAESAR_SOLVE library
  - EVALUATOR, BISIMULATOR, REDUCTOR
- Compositional verification
  - SVL, BCG_MIN, EXP.OPEN 2.0, PROJECTOR 4.0
- Distributed (massively parallel) verification
  - DISTRIBUTOR, BCG_MERGE, DSOLVE
- Compositional performance evaluation
  - BCG_MIN, BCG_STEADY, BCG_TRANSIENT, DETERMINATOR

3. Software tools and industrial applications

Software: the TRAIAN compiler

- TRAIAN: A compiler for the data part of E-LOTOS
- [PhD thesis of Mihaela Sighireanu – 1999]
- 48,000 lines of code
- Yearly releases (Sep. 1998, Feb. 2000, Nov. 2000, Nov. 2002, May 2003, Jun. 2004, Oct. 2005)
- Used by VASY for compiler construction:
  - AAL (16,009 lines of code, 49% in E-LOTOS)
  - CHP2LOTOS (17,600 lines of code, 65% in E-LOTOS)
  - EVALUATOR 4.0 (30,200 lines of code, 67% in E-LOTOS)
  - EXP.OPEN 2.0 (14,100 lines of code, 57% in E-LOTOS)
  - NTIF (12,400 lines of code, 68% in E-LOTOS)
  - SVL (9,200 lines of code, 47% in E-LOTOS)
- Downloaded from 50 different sites in 2005

Software: the CADP toolbox

- A verification toolbox for asynchronous systems
- A 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

Software: the CADP toolbox

- Four platforms supported
  - Sun/Solaris, PC/Linux, PC/Windows, MacOS
- International dissemination
  - license agreements signed with 345 organizations
  - since January 1st 2004: licenses granted to 1,214 machines
- Many applications
  - 86 case-studies accomplished using CADP
  - 21 research tools connected to CADP
  - 28 university lectures based on CADP (since 2002)

http://www.inrialpes.fr/vasy/cadp

Some industrial applications

- Hardware:
  - multiprocessor architectures
  - cache coherency protocols
  - bus arbitration protocols
  - asynchronous circuits
  - software/hardware codesign
- Middleware and Software architectures
  - dynamic reconfiguration protocol
  - automatic deployment protocol
  - distributed consensus protocol
  - federated knowledge management

Main Facts
about the VASY Team

Publications of the VASY team

	2001	2002	2003	2004	2005
International Journals	1		2		4
International Conferences	3	7	8	7	7
Invited Conferences - National - International		1 1	1 2	1 2	1 1
PhD theses defended			1		1
Book Chapters					1
Edition of Special Issues in International Journals	1	1	2		2

Contracts

- 2001-2003: RNTL project "Parfums"
  - INRIA, MGE-UPS, Scalagent, Silicomp
- 2002-2003 : ARC action "Modocop"
  - INRIA Sophia, Rennes, Rhône-Alpes, Verimag
- 2002-2005: IST 6 project "ArchWare"
  - Engineering, Thesame, Manchester, Pisa,
- 2004-2007: ACI Sécurité "Fiacre"
  - ENST, INRIA Sophia, FERIA, INRIA Rhone-Alpes
- 2001-2007: Bull contract "FormalFame [Plus]"
- 2005-2009: AESE project "Topcased"
  - Airbus, LAAS-CNRS (23 partners)
- 2006-2009: RNTL project "OpenEmbedd"
  - national project
- 2006-2009: Minalogic/EMSOC project "Multival"
  - Bull, CEA/LETI, INRIA, ST Microelectronics

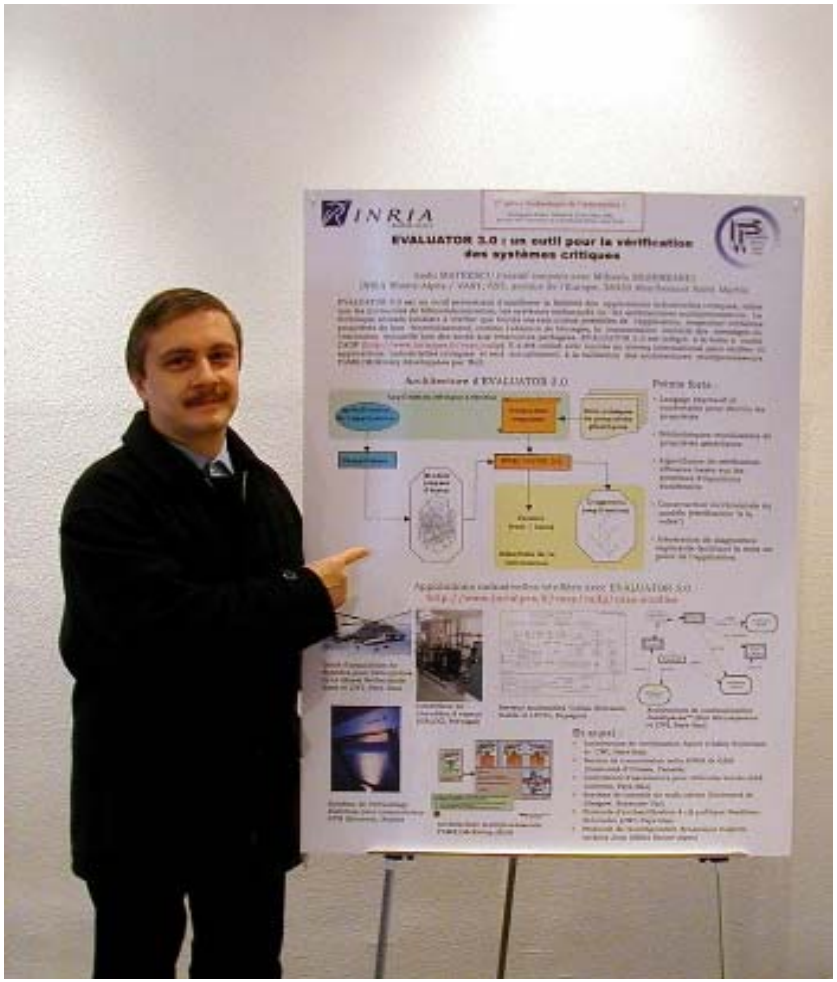
Some research collaborations

- Within France:
  - Numerous collaboration with other INRIA teams: verification, cluster, middleware protocols
  - Long-term (10 years) collaboration with Bull
  - INRIA/LETI joint research center for "System on Chip" technology
  - Collaboration with LAAS/CNRS (Fiacre, OpenEmbedd, Topcased)
- Within Europe:
  - "SENVA": joint team between VASY and CWI/SEN2
  - "FMICS": ERCIM working group on Formal Methods
  - Imperial College: connection LTSA and CADP

Success story #1

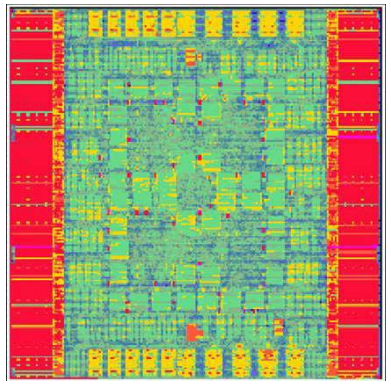
- **November 2002:**

  Radu Mateescu won the Information Technology Award granted by France Telecom and Foundation Rhône-Alpes Futur for his EVALUATOR 3.0 model checker

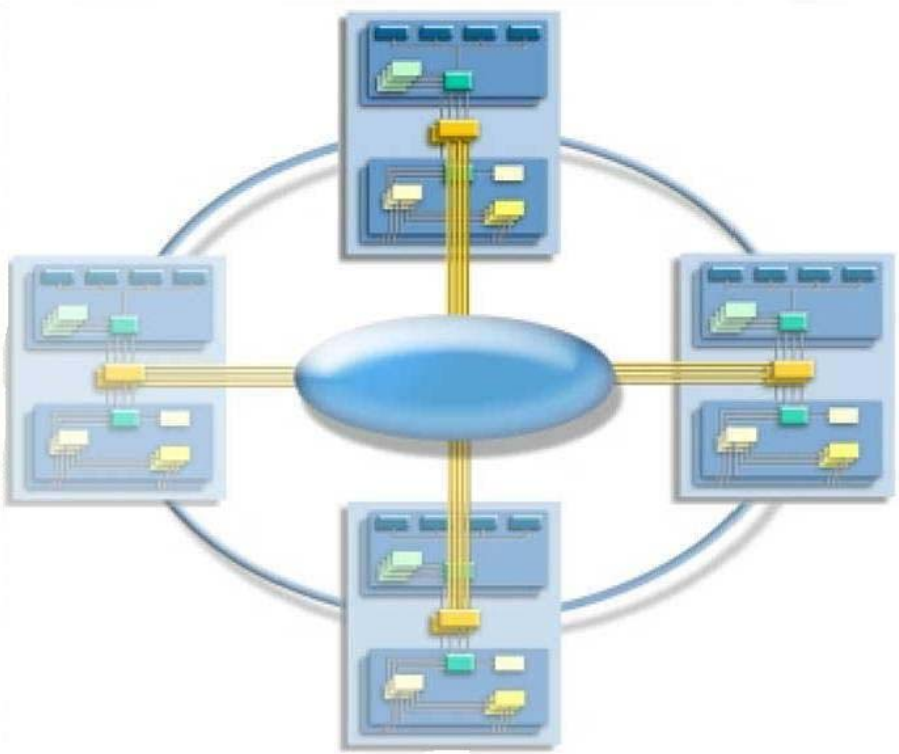


Success story #2

- The CADP tools found issues in the FSS, a critical circuit used in Bull's NovaScale servers (at the core of CEA's Tera10 supercomputer)
- The CADP tools are now part of Bull's official validation methodology



FSS chip (60 million gates)



Bull's FAME architecture

More information?

VASY Web site:

http://www.inrialpes.fr/vasy