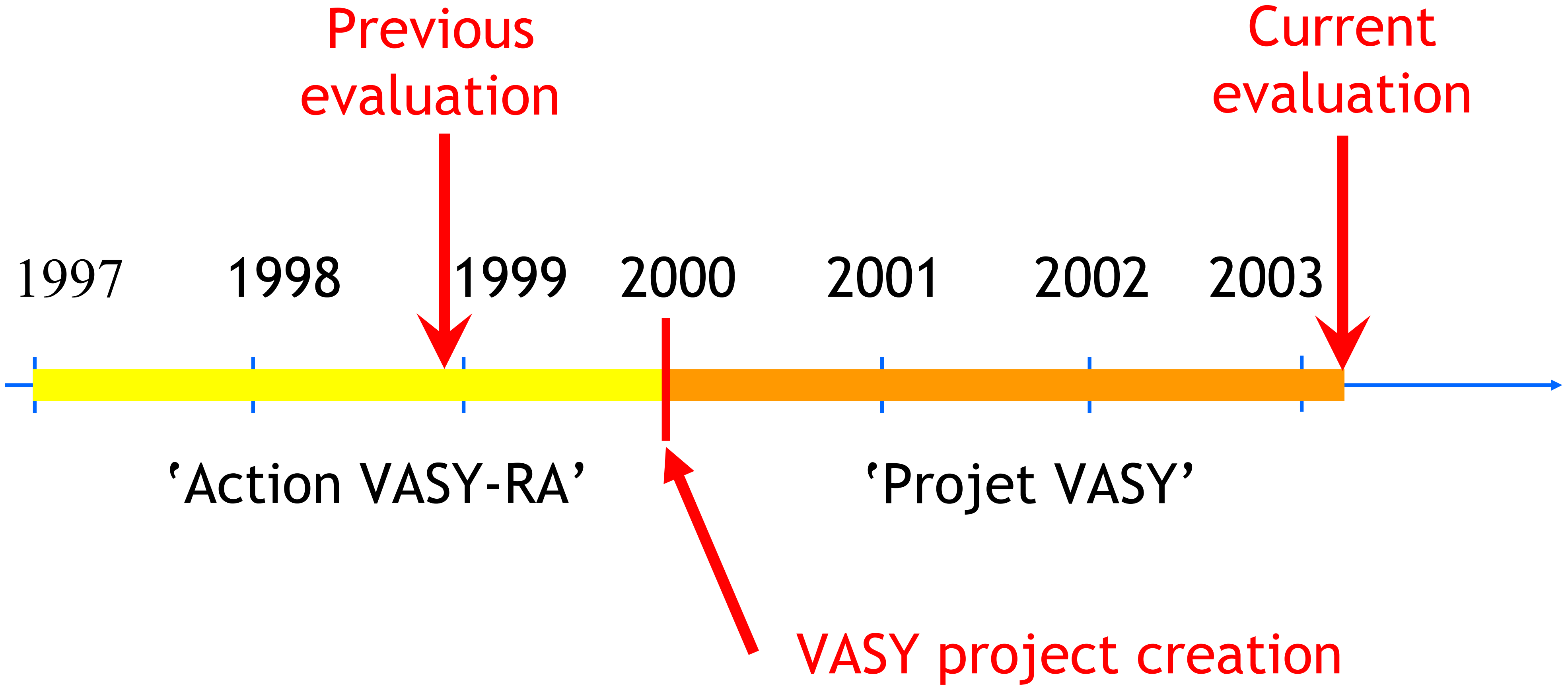
Evaluation INRIA 1C: The VASY Team

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

A note about timing



Previous evaluation

Current evaluation

‘Action VASY-RA’

‘Projet VASY’

VASY project creation

Scientific topics of VASY

Scientific topics

- Design of reliable computer systems
- Focus on asynchronous concurrency
  - Distributed processes
  - Message-passing communications
- Wide application domains
  - software
  - hardware
  - telecommunications
- Promotion of formal approaches
- Development of robust software tools
- *'Turning formal methods into reality'*

Three scientific directions

1. Languages and compiling techniques

- Formal specification of concurrent systems
- Langages supporting asynchronous concurrency
- Concepts: process algebras and functional languages
- Standards: LOTOS [ISO 8807], E-LOTOS [ISO 15437]
- Compiling techniques, flow analysis, code generation
- 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 (cont'd)

2. Models and verification techniques (cont'd)

- 'Explicit-state' methods
  - Reachability analysis
  - On the fly verification
  - Compositional verification
  - Distributed state space exploration
- 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

- middleware protocols, software architectures
- software/hardware codesign, embedded systems

The VASY team staff

March 2003: 14 persons

- INRIA scientists: 3
  - Hubert Garavel (DR2)
  - Radu Mateescu (CR1) since oct. 1998
  - Frédéric Lang (CR2) since sep. 2001
- Assistant: 1 (+5) Valérie Gardès
- Bull engineer: 1 (+2) Solofo Ramangalahy
- Post-docs: 2 (+2)
  - Aurore Collomb
  - Wendelin Serwe
- PhD students: 1 Christophe Joubert
- DEA students: 0 (+4)
- ‘Expert engineers’: 4 (+6)
  - D. Bergamini, D. Champelovier, N. Descoubes, F. Tronel
- Computer-science students: 2 (+3)
  - A. Catry (Polytechnique), G. Schaeffer (Supelec)

During the last 4 years: 34 persons in total

Scientific work done by VASY since the previous evaluation (End of 1998-March 2003)

1. Compiling ‘classical’ process algebras

- LOTOS processes (CAESAR compiler)
  - Richer semantic model (enhanced Petri nets)
  - State space reductions
  - Speed improvements
- LOTOS data types (CAESAR.ADT compiler)
  - ‘Dynamic’ data types (lists, trees…)
  - Reduction of pointer usage
  - Sub-term sharing
- Interactive simulation (OCIS)
- Code generation for embedded systems (EXEC/CAESAR)
  - Interfacing process algebras with the ‘real world’
  - Industrial usage: Bull’s multiprocessor architectures
- Numerous case studies
- Gateways from/to other languages: Java, mCRL, Erlang…

2. Forging ‘next generation’ languages

Rationale:

1. General-purpose languages (C/C++, Java…) offer little support for asynchronous concurrency
2. Graphical languages (SDL, UML) are too heavy and lack formality required for mechanized proofs
3. Process algebras are the solution but need improvements

- Contribution to the E-LOTOS standard (ISO 15337:2001)
  - process algebras combined with functional/imperative languages
  - quantitative time, exceptions, modules, genericity
  - formal semantics
- Implementation of (a variant of) E-LOTOS
  - data types: the TRAIAN compiler
  - processes: the NTIF semantic model and associated tools

3. Progressing ‘on the fly’ verification

- Key technology: Boolean Equation Systems
- Evaluator 3.0
  - On the fly evaluation of (altern. free) mu-calculus
  - Diagnostics generation
  - 11 published case-studies based on Evaluator
  - *2002: Rhône-Alpes foundation IT prize*
- Caesar_Solve: generic solver for B.E.S.
  - EVALUATOR 4.0: mu-calculus with value passing
  - BISIMULATOR: strong and branching equivalences

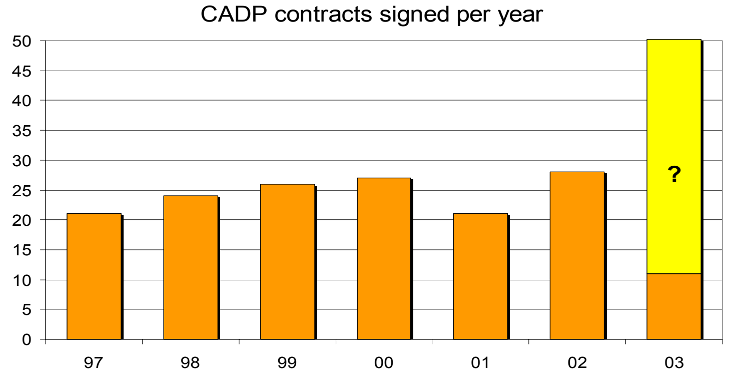
- Also: Trace-based verification (SEQ.OPEN)

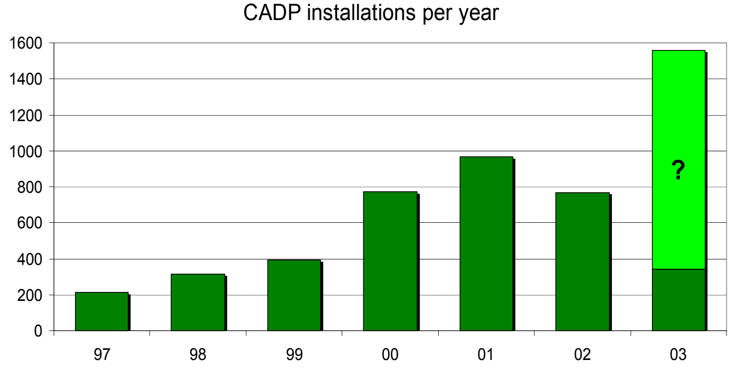
4. Progressing compositional verification

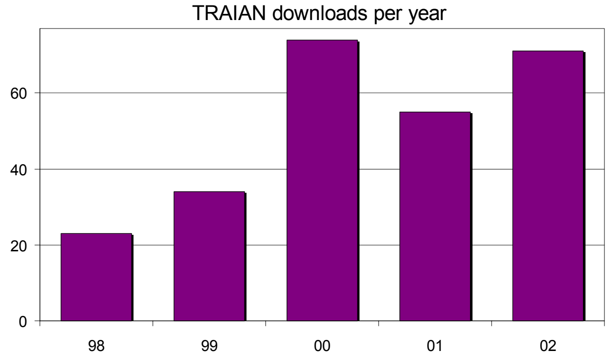
- Theoretical basis: [Graf-Steffen-Lüttgen-96] and [Krimm-Mounier-97]
- Work needed to make this approach tractable:
  - Automata minimization (BCG_MIN)
  - Automata product (EXP.OPEN v2)
  - Interface restriction (PROJECTOR v2)
  - Compositional verification scripting language (SVL)
- A growing number of applications
- Also: Compositional performance evaluation
  BCG_MIN, BCG_STEADY, BCG_TRANSIENT, DETERMINATOR

Software tools

- *‘Transfer theoretical results into robust tools for research, education, and industry’*
- CADP toolbox
  - New versions released regularly (Jan. 99, Jul. 01, Spring 03)
  - Licensed to 285 organizations
  - 64 published case-studies
  - 13 research tools based on CADP
- TRAIAN compiler for E-LOTOS
  - 48,000 lines of code
  - Several releases (Sep. 98, Feb. 00, Nov. 00, Nov. 02, Apr. 03)
  - Used by VASY for compiler construction (EVALUATOR 4, EXP.OPEN, SVL, NTIF, AAL)


CADP contracts signed per year


CADP installations per year


TRAIAN downloads per year

Industrial applications

VASY contracts

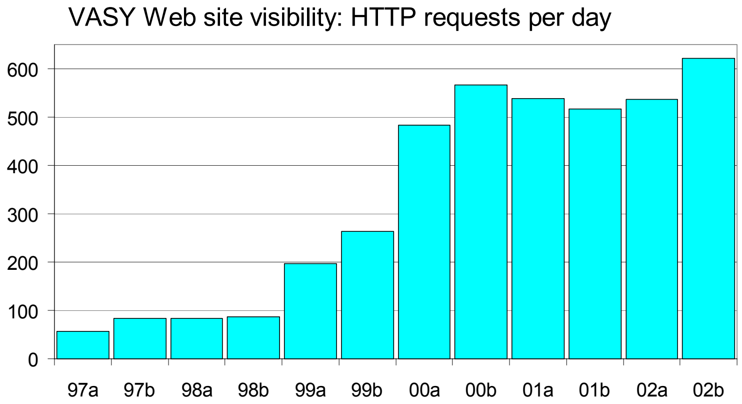
- FormalFame (98-04) Bull
- Reutel 2000 (99-00) Alcatel
- FormalCard (00-01) Schlumberger
- RNTL Parfums (01-03) MGE-UPS, Scalagent, Silicomp
- IST ArchWare (01-04) Engineering, Thesame

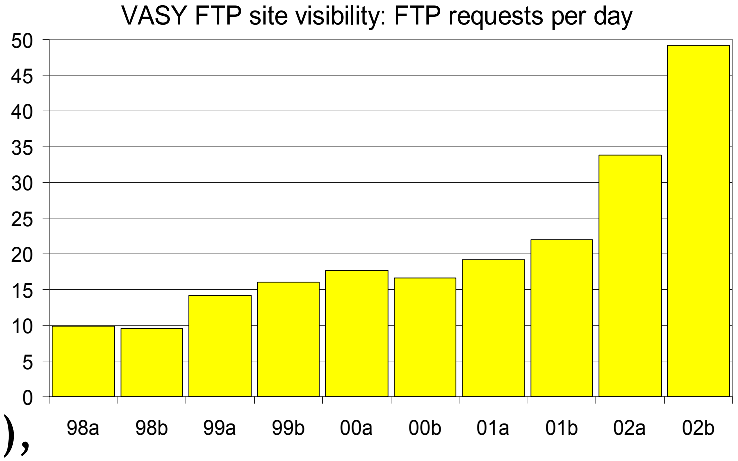
- System-level codesign
  - *LOTOS, C code generation, testing, co-simulation, temporal logic*
  - Cache coherency protocols
  - Bull *NovaScale* 64 bit servers (Itanium2)
- Middleware protocols Software architectures
  - *LOTOS, compositional verification*
  - Dynamic reconfiguration protocol
  - Automatic deployment protocol
  - Distributed consensus protocol
  - Federated knowledge management

Scientific positioning

VASY focuses on formal specification and verification of asynchronous systems

- Within INRIA
  - Theme 1A
    - Sirac/Sardes: protocols and distributed systems
    - Apache: distributed model checking, PC clusters
  - Theme 1C
    - Pampa/Triskell: Reutel contract
    - Pampa/Vertecs: FormalCard and FormalFame
  - Theme 2A
    - Lemme: smart card applications, proofs
    - Oasis: verification of Java programs
- In France
  - LAAS/CNRS: invited talks, RT-LOTOS
  - Université de Clermont: codesign
  - Université de Savoie: ArchWare contract
  - Verimag: collaboration on CADP
- In the world
  - Numerous users of CADP
  - University of Twente (performance evaluation)
  - CWI: muCRL toolset (connections with CADP)
  - Related work: Imperial College (LTSA), Oxford (FDR), Pisa (Jack), SUNY Stony Brook (Concurrency Factory)





Overall assessment

- Work done is in line with the topics listed in the VASY team proposal (Jan. 2000)
- Three new thematics have emerged:
  - Distributed model checking
  - Trace-based verification
  - Compositional methods for performance evaluation
- Former referees' recommendations have been addressed:

1. *Impact may be limited because of the choice of LOTOS*
   - funding for LOTOS available, progressive migration to E-LOTOS, generic tools interfaced with other languages (muCRL, Erlang, Java, UML…)
2. *Case studies should be carefully selected*
   - reduced number of case studies, selected topics (middleware protocols, software architectures, codesign, embedded systems)
3. *Symbolic verification techniques are also of interest*
   - NTIF model interfaces symbolic verification tools (IF, STG, TReX), E-LOTOS includes quantitative time

Goals of VASY for the next 4-year period

Scientific & applicative goals

- 1) Implementation of E-LOTOS
  - An international standard for asynchronous systems
  - No existing language with comparable functionalities
  - Adequate for both model checking and theorem proving
  - Scientific issue: *handling the full expressiveness of E-LOTOS*
    - Data types and functions (including exceptions)
    - Processes (including time)
    - Modules and genericity
  - Progressive migration from LOTOS to E-LOTOS
  - Merge of code bases (CAESAR.ADT, CAESAR, NTIF, TRAIAN)
- 2) Modal mu-calculus extended with data
  - Logical properties of value passing processes
  - On the fly evaluation and diagnostic generation
  - Software tool: EVALUATOR 4.x

Scientific & applicative goals (cont’d)

- 3) Fighting state explosion for asynchronous systems
  - Compositional verification
  - Dataflow analysis, static analysis on NTIF models
  - Distributed model-checking (‘Gigastate model checking’)

- 4) Generic components for simulation, verification, testing
  - Enhancements of BCG and Open/Caesar technologies
  - Support of larger (‘Gigastate’) state spaces
  - Support of user-defined data types and functions

- Targeted application domains
  - Embedded systems
  - System-level codesign
  - Software architectures

Potential difficulties and risks

- Part of the industry prefers semi-formal methods
  - Short-term interest in graphical methods
  - Mainly used for documentation and code generation
  - But other industrialists need verification (hardware)
  - Positive feedback received for E-LOTOS (tools are expected)
- Tool development requires important resources (manpower)
  - Vasy achieves important self-funding (90.6% in 2003)
- Tool development requires long term stability
  - Vasy benefited from the 'Dyade' (Bull-INRIA) partnership
  - Important turnover due, in part, to INRIA's employment contracts
- Risk reduction factors:
  - Focus on applicable tools
  - Assessment on case studies
  - Large community of users
- Institutional improvements expected:
  - Reduction of administrative overhead
  - Easier co-operation with Universities