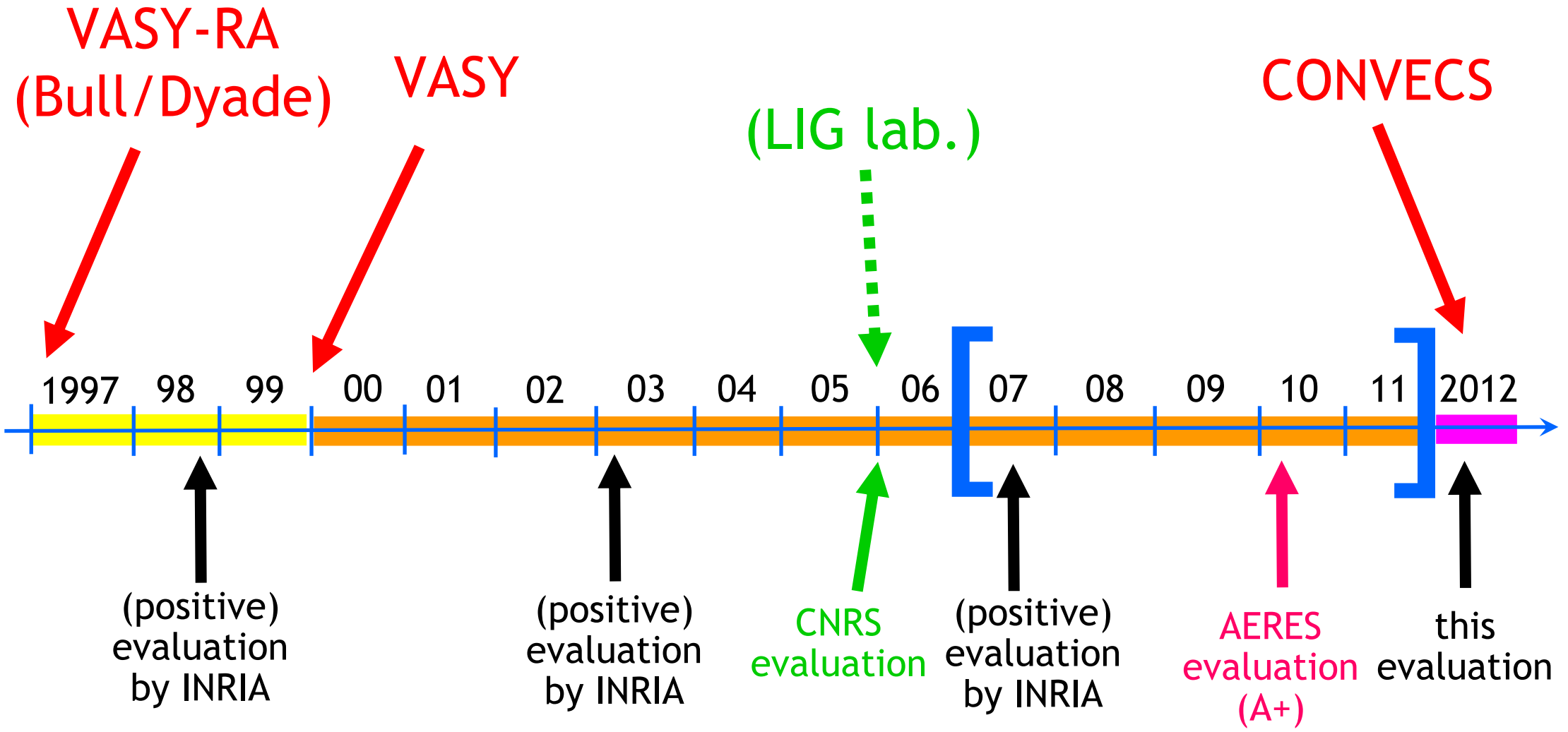
The VASY Team

Validation of Systems

History of the VASY team



Staff (2007-2011)

- Permanent scientists:
  - Hubert Garavel (Inria)
  - Radu Mateescu (Inria)
  - Frédéric Lang (Inria)
  - Wendelin Serwe (Inria)
  - Gwen Salaün (Grenoble INP)
- Guest scientists:
  - Holger Hermanns (Saarland University - 20%)
  - Etienne Lantreibecq (STMicroelectronics)
- Post-docs: 4 (~18 months)
- PhD students: 4 (~36 months - Bull, STMicro)
- Software engineers: 17 (~19 months)
- Assistants: M. Felici - D. Courtiol - H. Pouchot

Scientific topics of VASY

Motivation

- Design of reliable computer systems
- Focus on asynchronous concurrency
  - Distributed processes
  - Message-passing communications
  - No central clock assumption

- Promotion of formal approaches
- Development of software tools (CADP, TRAIAN)
- Confrontation with real-life applications

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

Main challenges

- A fundamental issue:

  Fighting state explosion for asynchronous systems

- A usability issue:

  Making formal methods acceptable by industry

- An architectural issue:

  Designing modular components for verification and performance evaluation

Three main scientific themes

1. Models and verification techniques
2. Languages and compilation techniques
3. Case-studies and industrial applications

Theme 1: Models and verification

- Formal models for asynchronous concurrency
  - Automata-based models
  - Probabilistic / stochastic / timed models
  - (Parameterized) Boolean Equation Systems
- Explicit-state methods
  - Reachability analysis
  - On-the-fly verification
  - Compositional verification
  - Distributed verification
- Logical properties (*model checking*)
  - Mu-calculus, temporal logics
- Behavioural properties (*equivalence checking*)
  - Bisimulations
- Modular architectures - generic software components

Theme 1: Highlights

- MCL / EVALUATOR 4.0
  - value-passing modal μ-calculus with data types
  - on-the-fly model checker based on parameterized B.E.S.

- SVL / BCG_MIN 2.0
  - compositional verification and performance evaluation
  - "smart reduction" automated strategies
  - signature-based minimization algorithms

- PBG / CAESAR_SOLVE
  - distributed verification using clusters (Grid 5000, PacaGrid)
  - distributed resolution algorithm for B.E.S.

Theme 2: Langages and compilation

- Formal languages for asynchronous concurrency
  - Process calculi
  - Functional / imperative languages
  - Standards: LOTOS [ISO 8807], E-LOTOS [ISO 15437]
- Pivot models / intermediate languages
  - Petri Nets extended with data
  - Communicating automata with data and time
- Compiling techniques
  - C code generation
  - rapid prototyping
  - interactive simulation
  - static analysis
  - source to source language translations

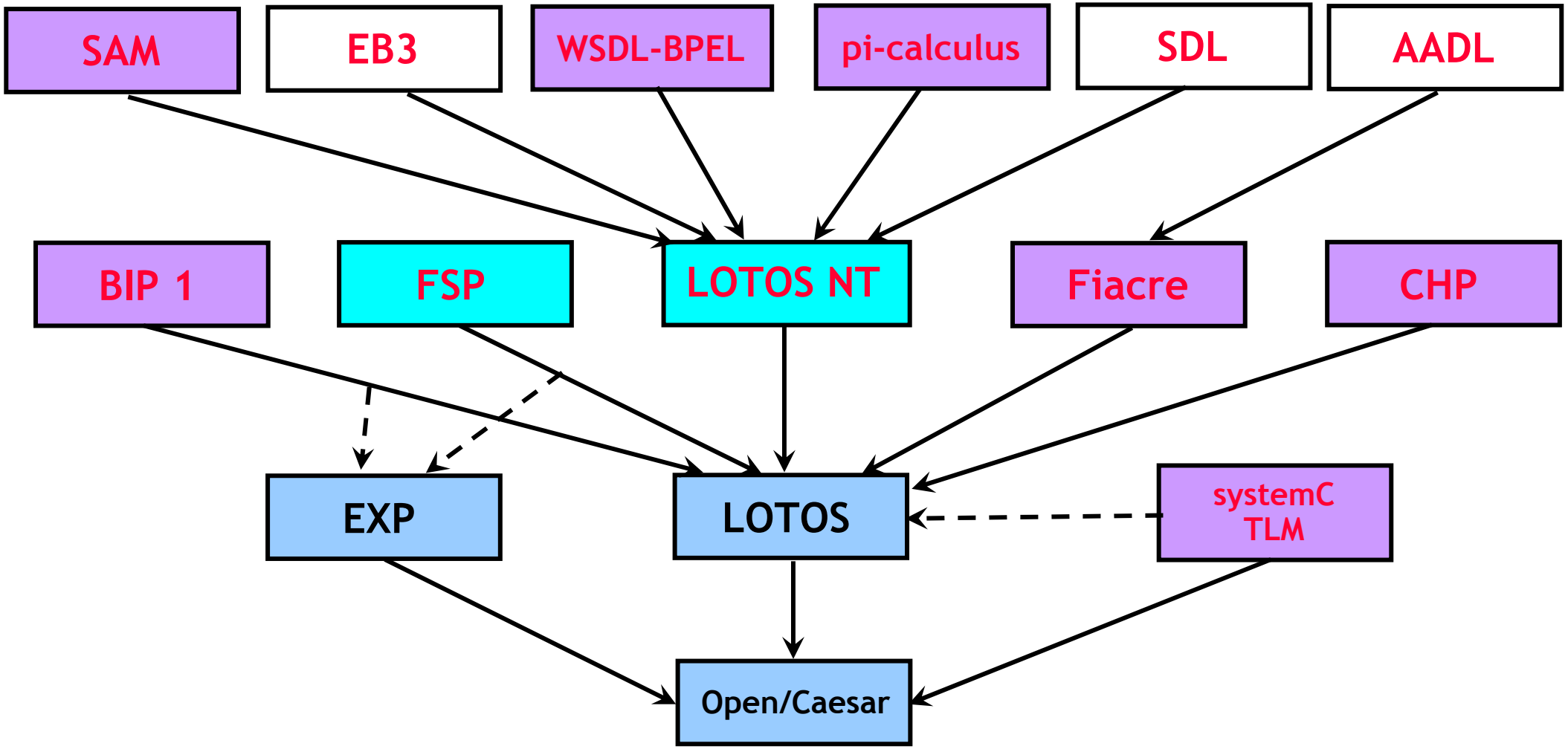
Theme 2: Highlights

- FIACRE (joint work with IRIT and LAAS-CNRS)
  - pivot language for asynchronous embedded systems
  - strongly inspired from our prior research on NTIF
  - part of OpenEmbedd/Topcased platforms ($\rightarrow$ Polarsys)

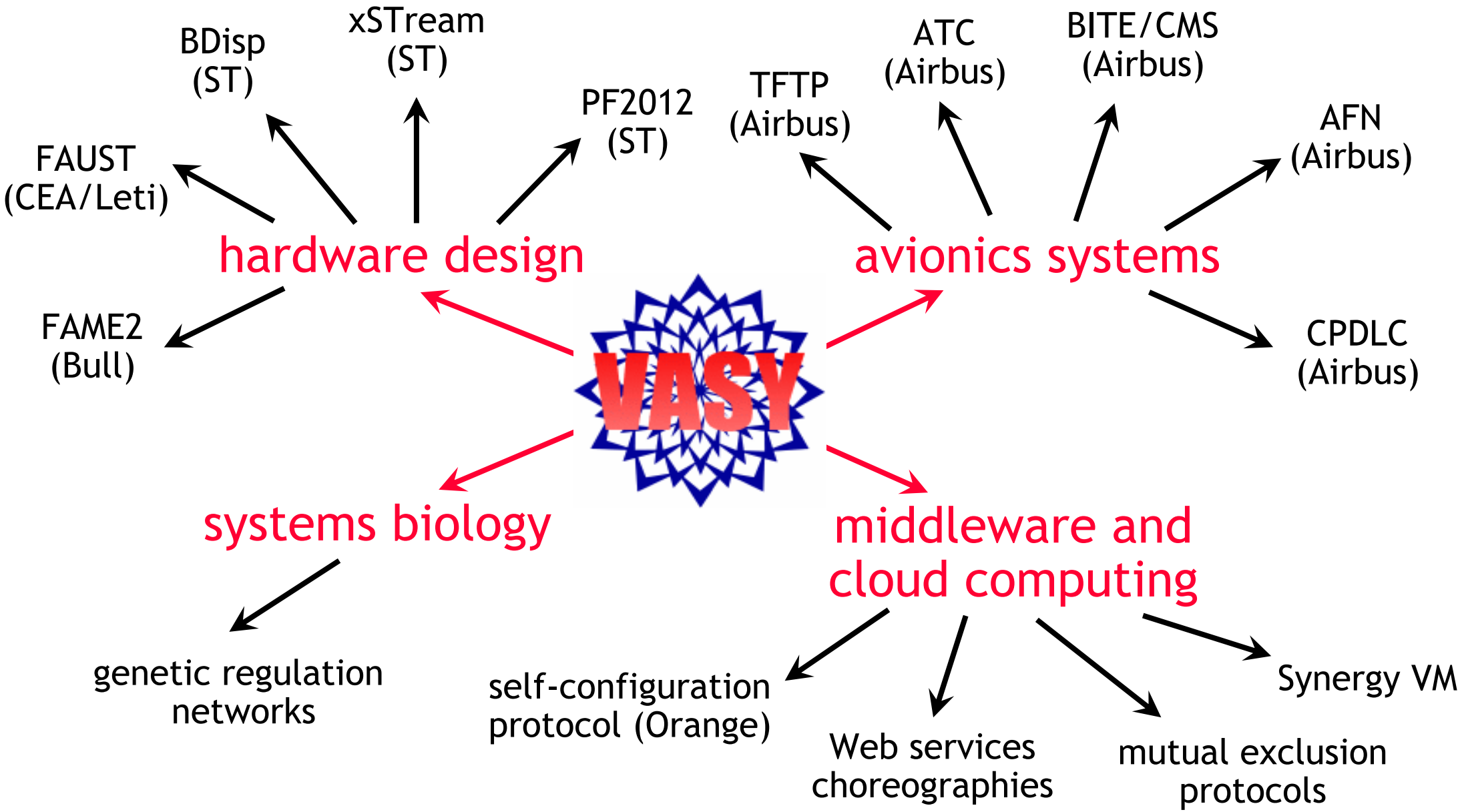
- CHP *(Communicating Hardware Processes)*
  - language for asynchronous circuits (Caltech, CEA, TIMA)
  - formal semantics given by VASY
  - reduction to "standard" calculi by translation to LOTOS

- LOTOS NT *(or LNT, for LOTOS New Technology)*
  - an implementable version of E-LOTOS (ISO 15437)
  - tool chain by translation to "standard" LOTOS
  - used by Bull, CEA/Leti, and STMicroelectronics

Theme 2: Language map



Theme 3: Industrial applications



Main facts about VASY

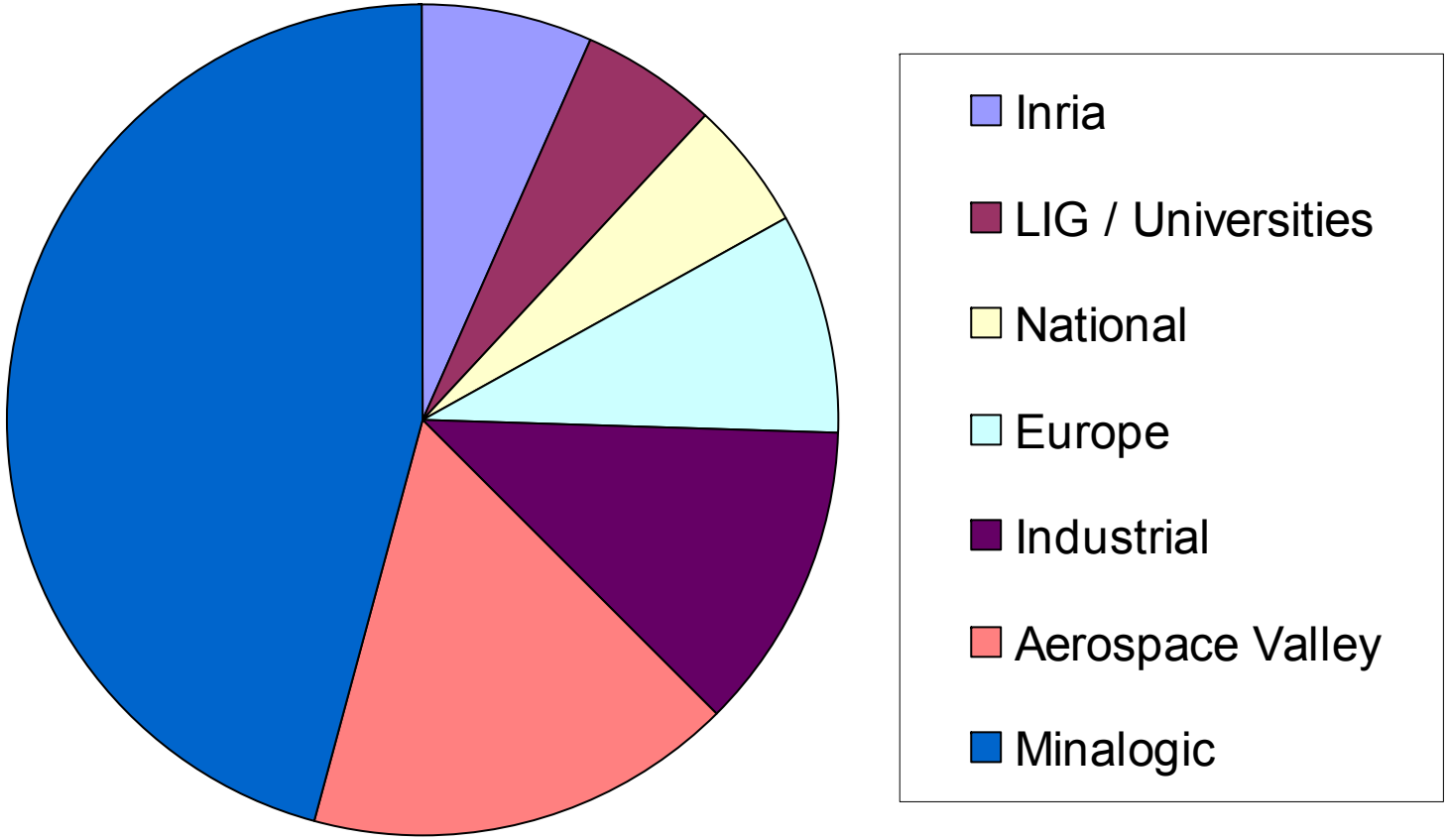
Publications (2007-2011)

- PhD theses: 5
- Habilitation these: 1
- Journal papers: 11 (+7)
- Conference papers: 49 (+4)
- Book chapter: 1
- Press articles: 5
- Deliverables: 15
- Technical reports: 8

Collaborations

- Local
  - IBIS, IIHM, SARDES
- National
  - Inria: ATOLL (Rocq.) - ESPRESSO (Rennes) - OASIS (Sophia)
  - LAAS-CNRS and IRIT (Toulouse) - LE2I (Dijon) - LRI (Orsay)
- International
  - Bucharest - Imperial College – Malaga – Twente - Saarland
  - MIT – Sherbrooke - California Santa Barbara
- Industrial
  - Airbus – Bull – CEA - STMicroelectronics

Attracted funding (2007-2011)



- Total: 2.241 M€
- Average: 448 k€ per year

Software: cadp.inria.fr

- A long-term effort
  - 50 tools, 20 code libraries
  - 750 pages of technical documentation
  - 12 machine architectures supported
- Academic dissemination
  - 441 license agreements signed
  - licenses granted for 3056 machines (2007—2011)
  - 56 new case-studies tackled using CADP (152 in total)
  - 30 new research tools connected to CADP (61 in total)
  - 10 university lectures based on CADP (2007—2010)
  - user forum: 200 members, 1330 messages
- Industrial dissemination
  - 36 yearly licences sold (180 k€)

Final words…

What should be retained from VASY?

- Never surrender to dominant opinions of the moment
  - Asynchrony is crucial for embedded systems
  - Process calculi still have a future
  - Explicit-state model checking is alive
- Continuum: theory - software tools - applications
- Quest for integration
  - process calculi - equivalence checking - model checking - performance evaluation
- Modular architectures for model checkers
  - explicit - on-the-fly - compositional - distributed
- Better formal methods
  - for models (operational): LNT (aka LOTOS NT)
  - for properties (declarative): MCL