Asynchrony in embedded systems: the Multival project

Hubert Garavel

INRIA Grenoble

http://vasy.inrialpes.fr

Challenges for embedded systems

- Increase performance
- Reduce size
- Reduce energy consumption
- Enhance usability and acceptance
- ...

Performance issues

- Past:
  - extra performance by increasing clock speed
- Present:
  - physical limitations (no more than 4 GHz)
- Future:
  - extra performance by adding processor cores

A price to pay for everybody

- Pressure on software developers
  - rewrite applications to exploit parallelism
  - better compilers
- Complexity of architecture design
  - Synchronous approach no longer adequate
  - Asynchrony mandatory (previously avoided):
    - massive concurrency
    - nondeterminism
    - message passing, distributed data, caches, etc.
  - Error-prone:
    - deadlocks, livelocks, unspecified receptions, etc.

How to proceed?

- Formal models of architectural design
  - emphasis on control, concurrency, synchronization, communications
  - system = set of concurrent machines
  - suitable languages: process calculi
    - CCS [Hoare], CSP [Milner]
    - LOTOS [ISO standard 8807]
    - E-LOTOS [ISO standard 15437]
- Formal specification catches many mistakes

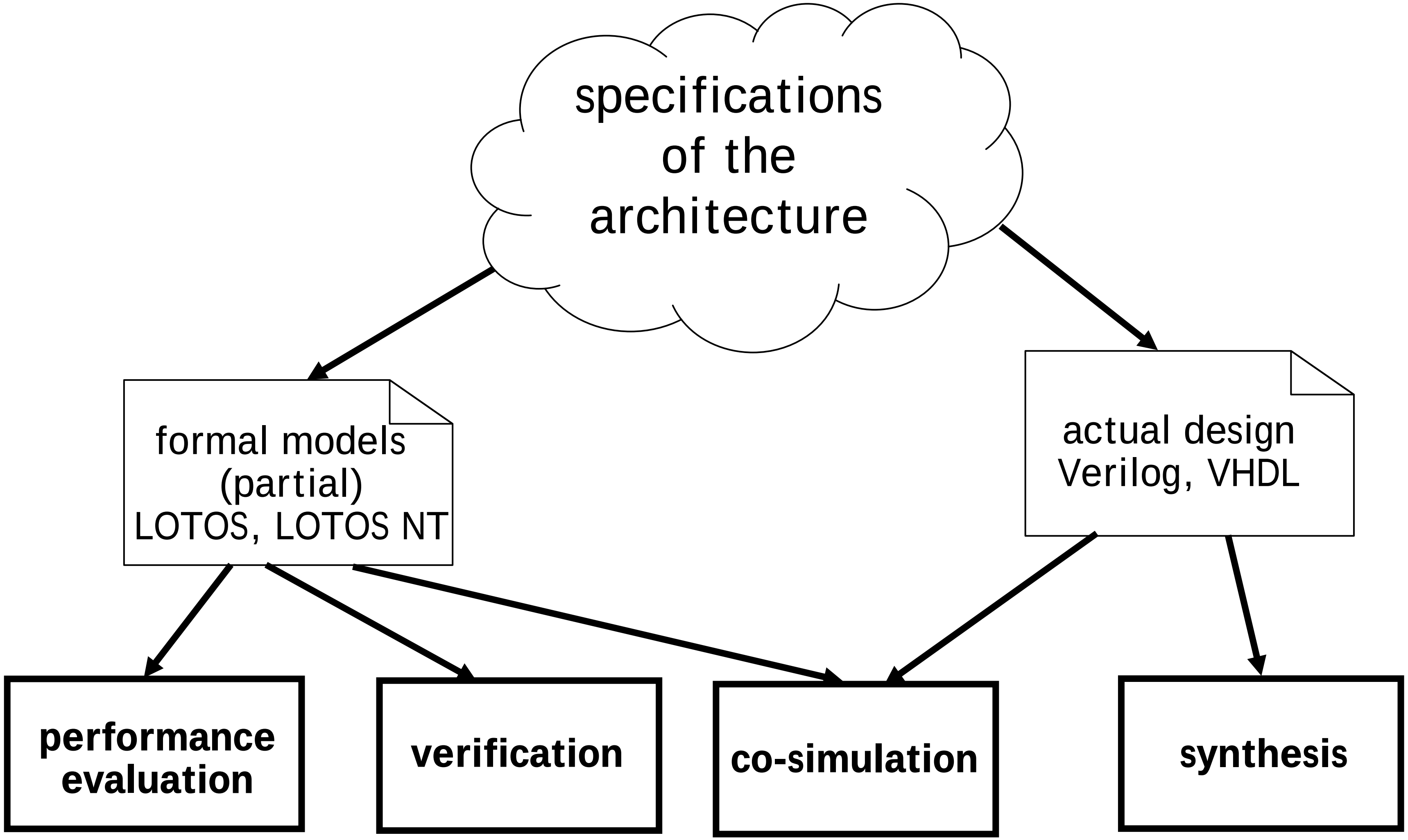
Functional verification

- Detect errors as soon as possible
- Analyze formal models
- Complementary approaches:
  - State space exploration
    enumerate all possibly reachable states
  - Equivalence checking
    compare two formal models for equality or inclusion
  - Model checking
    check if a formal model satisfies a set of logic formula
  - Co-simulation
    compare a model wrt traces generated from RTL

Performance evaluation

- Goal: predict numerical values
  - latencies
  - throughputs
- Formal models developed for verification can be reused
  - functional behavior extended with performance data
- Techniques:
  - Interactive Markov Chains (IMC, IPC)
  - steady-state and transient analysis
  - simulation

The global flow



specifications of the architecture

formal models (partial) LOTOS, LOTOS NT

actual design Verilog, VHDL

performance evaluation

verification

co-simulation

synthesis

Current applications

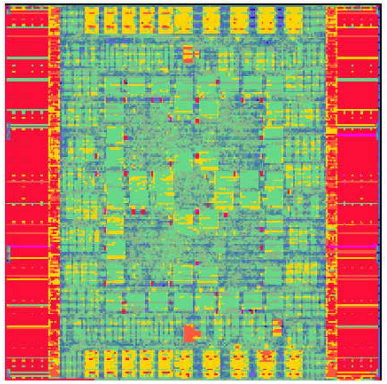
The Multival project (Minalogic)

- Four partners:
  - Bull
  - CEA/Leti
  - INRIA
  - STMicroelectronics
- Projet leader: Richard Hersemeule
- Duration : Dec. 2006 – Dec. 2010
- Budget : 7,5 M€

The CADP toolbox

- A verification toolbox for asynchronous systems
  - Several input languages
  - Step-by-step simulation
  - Rapid prototyping
  - Model checking
  - Equivalence checking
  - Test generation
  - Performance evaluation
- International dissemination
  - license agreements signed with 400+ organizations
  - 104 published case-studies accomplished using CADP
  - commercial licences available from INRIA

Collaboration with Bull



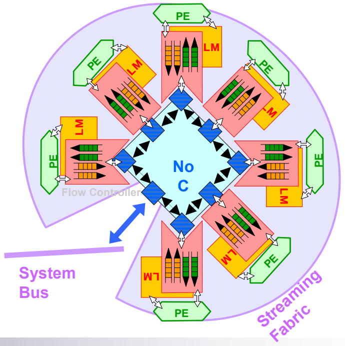
- Validation of supercomputers
- Continuous collaboration since 1995
- In crucial part of the BSPS chip (NovaScale servers), CADP revealed errors not detected using "classical" techniques

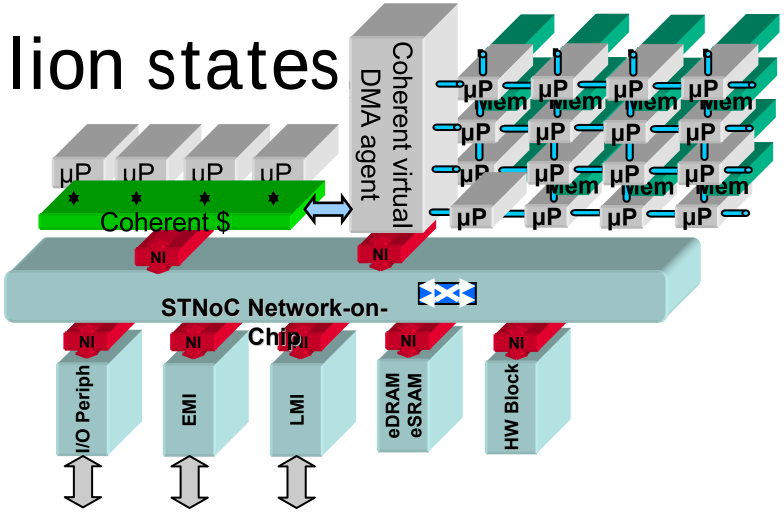
- Current work:
  - validation of FAME2 protocols
  - performance prediction for MPI

Collaboration with STMicroelectronics

- 2002: CADP revealed an error in the STBus
- 2006-2009: focus on the xSTream architecture (NoC for video : phones, set top boxes…)
- thanks to CADP, ST detected two design issues very early

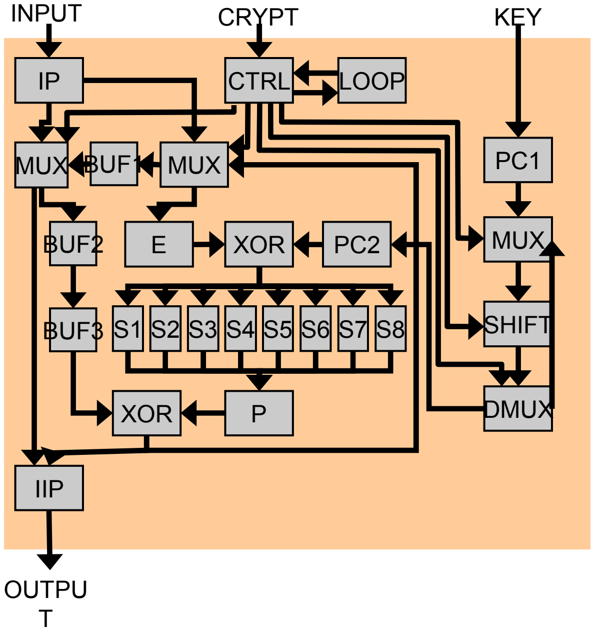
- (32 concurrent agents, 760 million states 6 billion transitions explored)

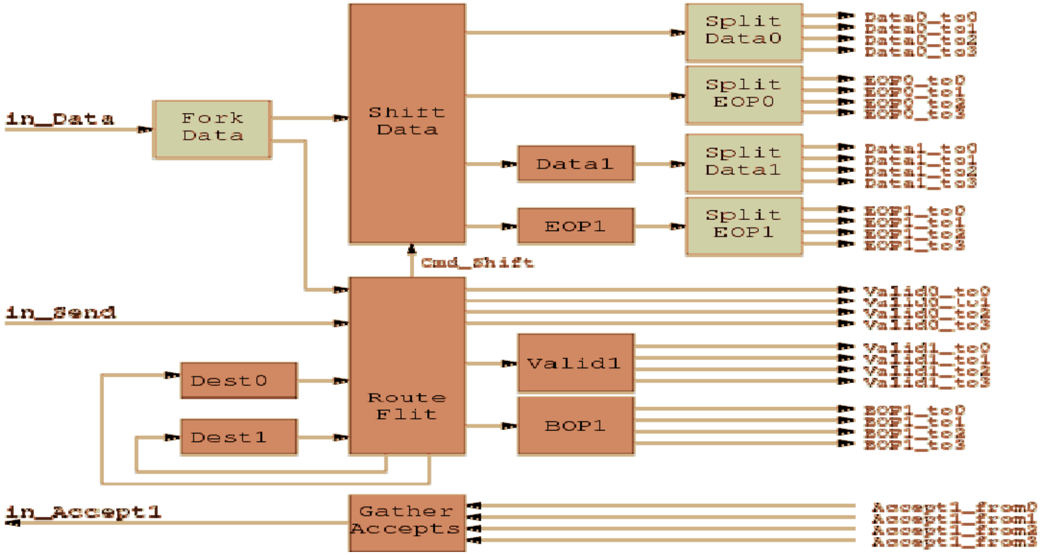


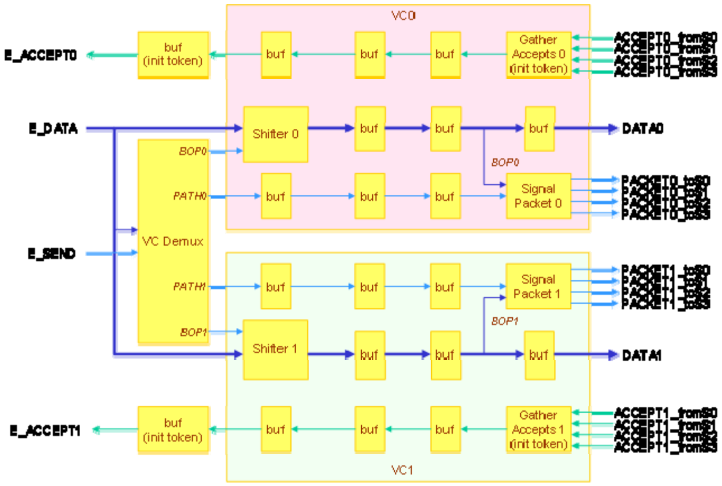


Collaboration with CEA/Leti

- CADP used to validate three chips designed at CEA/Leti (DES, FAUST v1, FAUST v2)
- Different levels addressed: system, micro-architecture, asynchronous logic (gate level)







Key findings

- Positive results
  - non-trivial issues detected ("high quality bugs")
  - link between verification and performance evaluation
  - bridges between SystemC/TLM and LOTOS
- Challenges
  - state explosion: complexity grows exponentially => "intelligent" strategies are required
  - need for training industry engineers

Conclusion

- Many new challenges in embedded systems
- Asynchrony is a major challenge
- Formal verification is unavoidable
- INRIA provides verification technology (CADP)
- Used from microprocessors to HPC servers

Multival:

- Verification for multiprocessor architectures
- *Multiprocessors architectures for verification*

More information...

http://vasy.inrialpes.fr