The Omega project

UML based modeling of real-time and embedded systems with formal validation
(2002-2005)

Partners

Academic (tool and technology providers)

- **Verimag**, France – coordinator
- Christian-Albrechts University **Kiel**, Germany
- **CWI** (Centrum voor Wiskunde en Informatica), Netherlands
- University of **Nijmegen**, Netherlands
- **OFFIS**, Germany
- **Weizmann** Institute, Israel

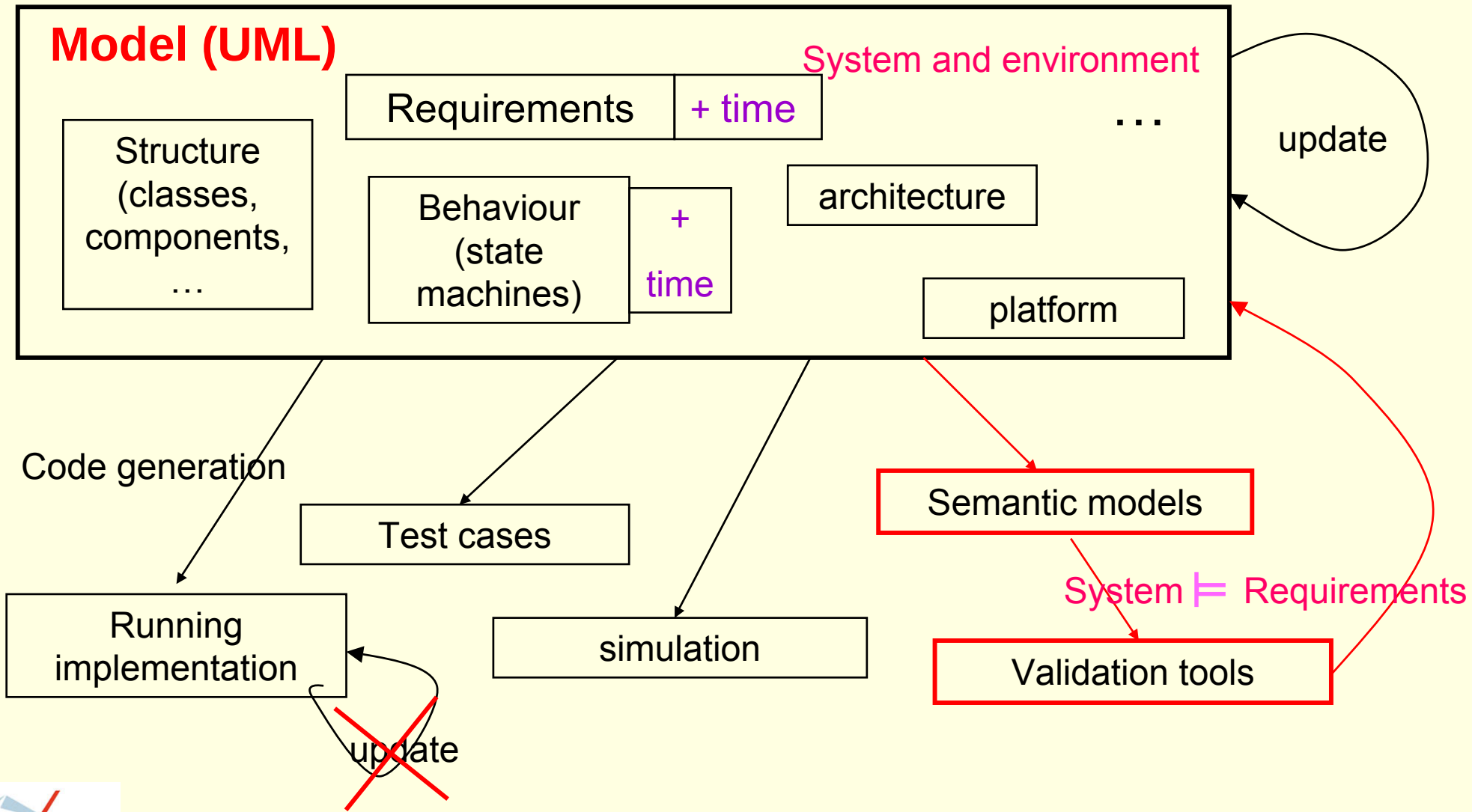
Users

- **EADS** Launch Vehicles, France
- **France Telecom R&D**, France
- **Israeli Aircraft Industries**, Israel
- **NLR** (Nationaal Lucht- en Ruimtevaartlaboratorium), Netherlands

Supporters (UML tool providers)

I-Logix --- Rational Software, IBM --- **Telelogic**

Model based development and validation of real-time systems



How well does UML fit ?

Strong points of UML

- Support of requirement level and design level notations, including architecture and components, which made their proofs
- User acceptance
- Existence of Case tools and model interchange format XMI
- Integration in development cycle possible

Weak points of UML (for validation of dynamics)

- Concepts are defined at syntax level, many issues in semantics are left to tools to fix them
- Weak support of real-time concepts (improved by UML 2.0)

Approach

1. Define a profile: select a suitable subset of UML
   - adapt and extend where needed with a special emphasis on timing
   - define an appropriate semantics

2. Propose a development methodology, based on
   - the user's development methodology
   - the UML modeling and specification capabilities
   - verification methods and tools developed in the project

3. Provide methods and tools for formal specifications and verification covering the chosen profile
   - Model interchange via standard XMI

4. Proposed methodology and tool-set evaluated on four industrial case studies

Results

1. Omega UML profile for real time

- A rich subset, useful for development
- Notations for design and requirement specifications
  - Kernel model: close to operational subset of profiles of main tool providers with real-time in the spirit of SPT
  - Component and architecture description
  - Requirement notations of different nature:
    - Operational: Live sequence charts, Observers
    - Declarative: OCL
- Positive feedback from users
- Some concepts may influence standard evolution
  - Timed extensions
  - Observers for expression of requirements
  - Live sequence charts
- Existence of formal semantics helpful for tool builders

Results: tools

Omega compliance check

XMI
Omega exchange format

Timed model-checking (IF)
OMEGA models with time extensions and observers
Internal: timed automata with priority rules
Enumerative MC
UML oriented feedback
Visual representation of properties and error traces

XML format (SXMI)
intermediate representation

PVS based validation
UML models and OCL with time in PVS
Infinite and parameterized models

Untimed Model-Checking (UVE)
Omega models with discrete time
Internal: symbolic transition relation
BDD based MC against LSC and temporal logic
Error traces = sequence charts

XML based execution

Rule based tool for execution of XMI

LSC tools
Extract class information from XMI
Editing of LSC with time (play-in)
Consistency of LSC
Export of LSC to XML
State machine synthesis (play-out)

XML
Representation of LSC

Results: tools

- A set of tools covering all notations of the Omega profile
  - Different aspects of a model are checked by different tools, abstracting from other aspects
  - Different kinds of properties are checked
  - Problem: some variations on common parts
  - ➔ No other validation tools cover such a large profile
- Tool integration
  - Tool interchange by sharing models via an identified exchange format (XMI/XML)
  - Requirement: all tools agree on the common features
  - No heavy integration

Omega profile and semantics

Frank de Boer - CWI, Bernhard Josko – OFFIS

IF simulation and verification tool for UML

Marius Bozga, Iulian Ober - Verimag

Omega Tools and Case studies

Modelling and verification of the Mars case study

Yuri Yushtein - Kiel Univ, Jozef Hooman - Nijmegen Univ

Ariane 5 flight program timing verification

David Lesens – EADS

A component based depannage service modelled with LSC

Pierre Combes - FTR&D, Hillel Kugler – Weizmann

Timing analysis of a voting monitor with 2 CPUs using IF

Meir Zenou - IAI