MESTRADO EM MECATRÔNICA

UFBA LASID

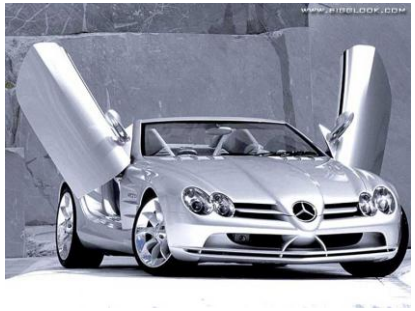
Integrating UML and UPPAAL for Designing, Specifying and Verifying Component-Based Real-Time Systems

UML&FM'2009

André Muniz, Aline Andrade and George Lima

Motivation

- Embedded systems are everywhere.



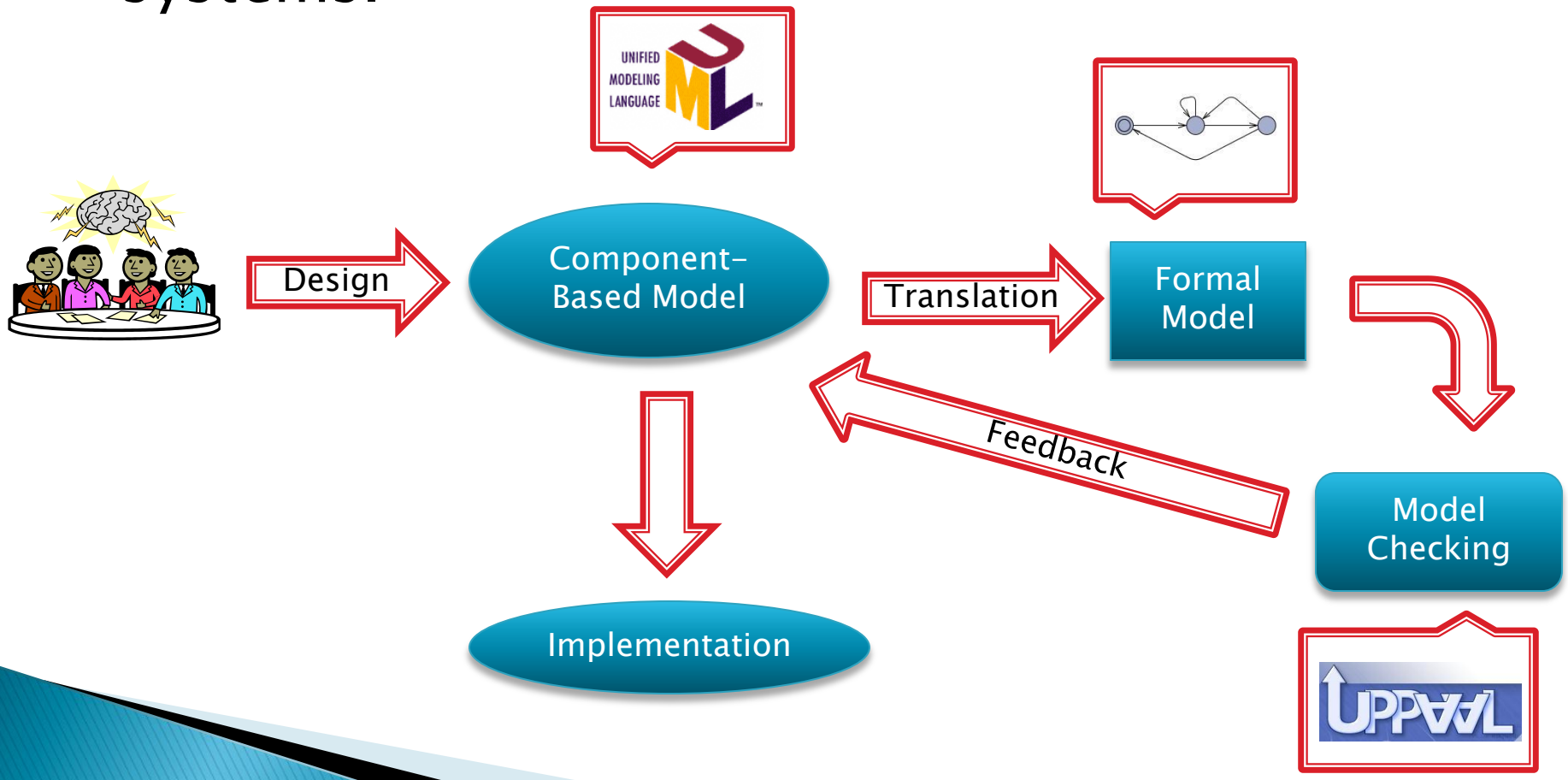
- Real-Time Systems
  - Increasing complexity
  - Design and Verification Challenge

Motivation (2)

- Component-Based Development (CBD)
  - Design and Implementation
- Gap between current verification techniques and component-based design.
- Keep consistency between two different models

Objectives

- Integrate Model Checking in the development process of component-based real-time systems.



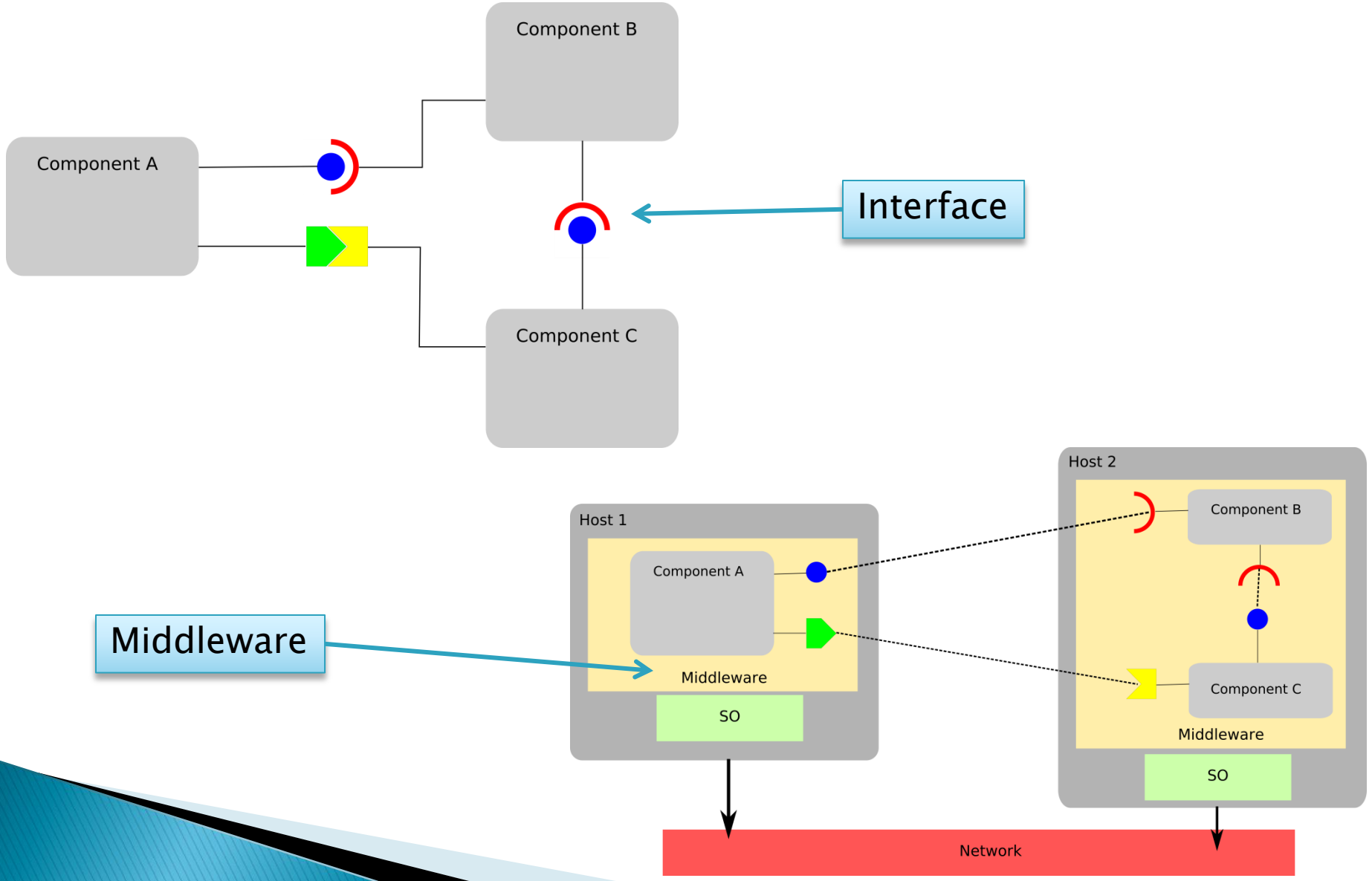
Objectives (2)

- Automatic Translation Tool
  - From UML models to timed automata
- Take into account middleware characteristics
  - Improve verification
  - Handle state-space

Related Work

- Specific Modeling
  - DSMLs and component models
- Automatic translation support tools
- Component Middleware
  - Incorporate functionalities
- Property verification
  - Functional requirements
  - Schedulability

Components

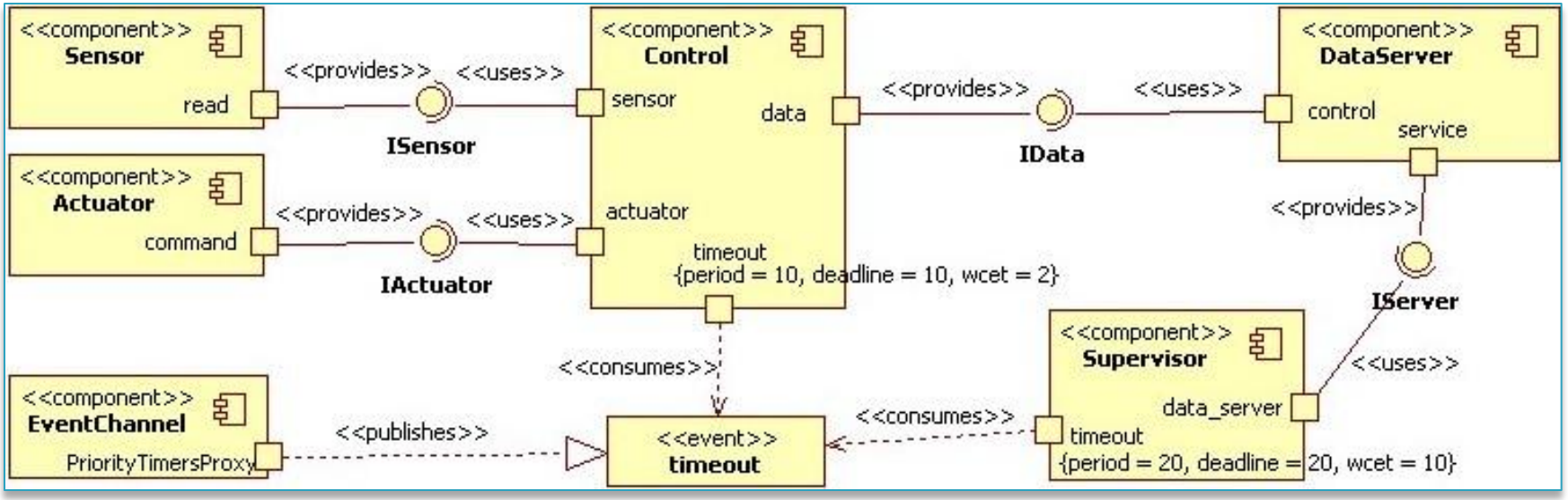

Component B
Component A
Interface
Component C
Host 1
Component A
Middleware
SO
Host 2
Component B
Component C
Middleware
SO
Middleware
Network

Components(2)

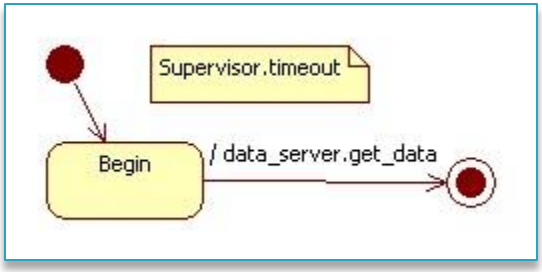
- Corba Component Model (CCM)
  - Component features
  - Middleware services
  - Independent of platform and programming language
- CIAO (Component-Integrated ACE ORB)
  - Implements *Lightweight CCM*
  - Real-Time Extensions
    - Real-Time Scheduling Service
    - Real-Time Event Service

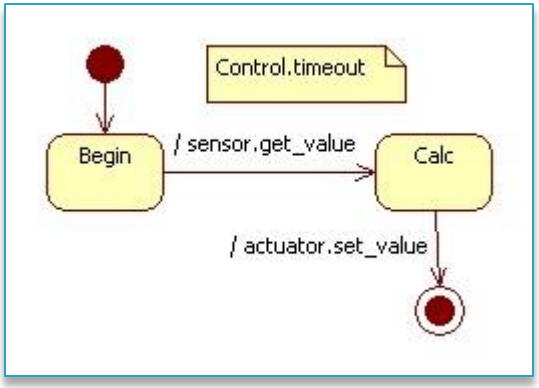
Translation

- Input
  - Component Diagram



  - Set of Statechart Diagrams

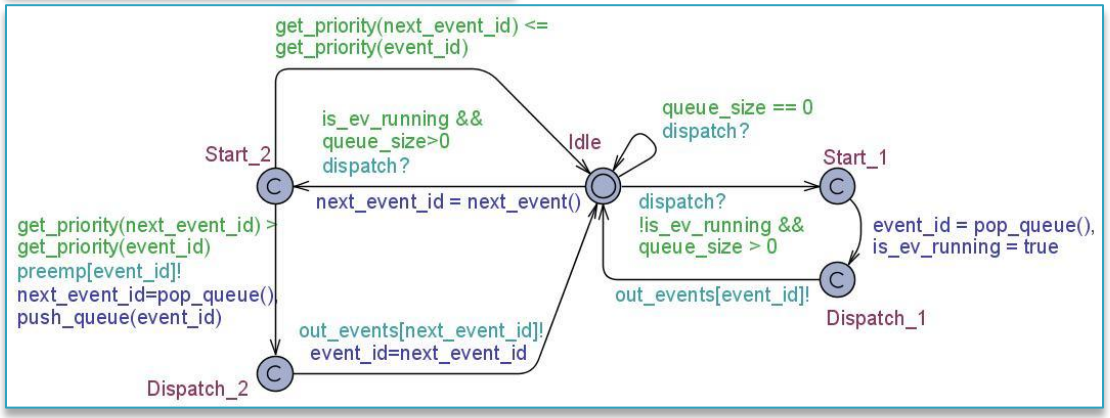




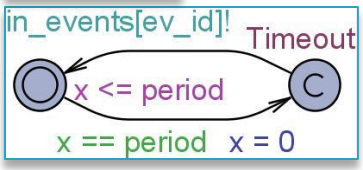
Translation (2)

- 1st Step
  - Component Diagram Translation (global variables)
  - Middleware related automata generation

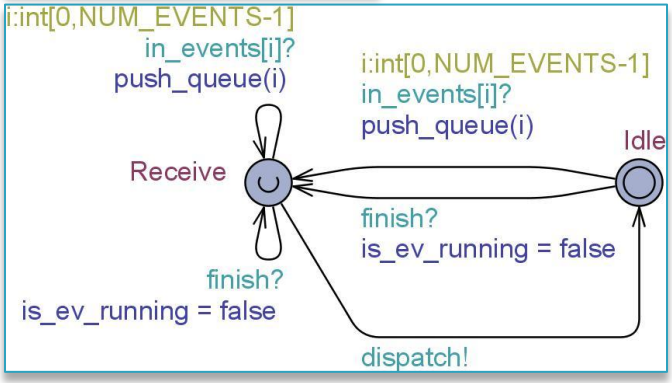
Dispatching Module



Timer

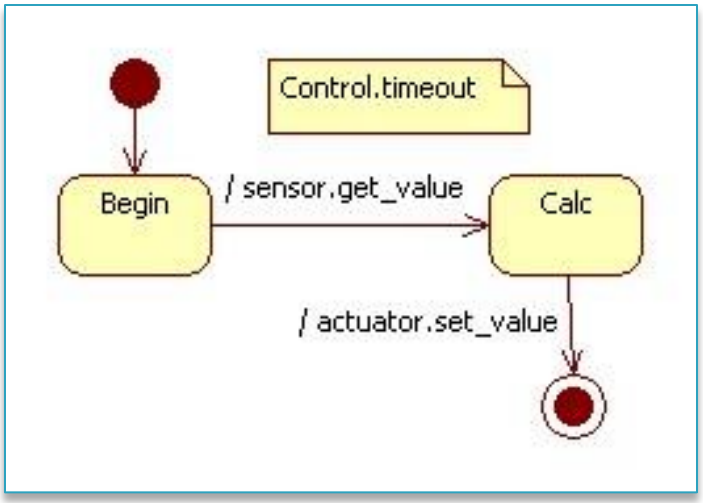


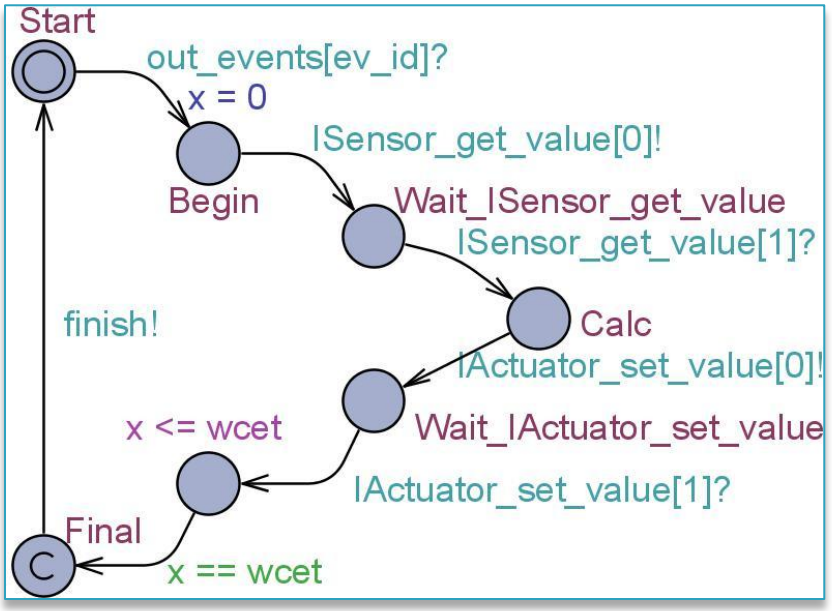
Event Channel



Translation (3)

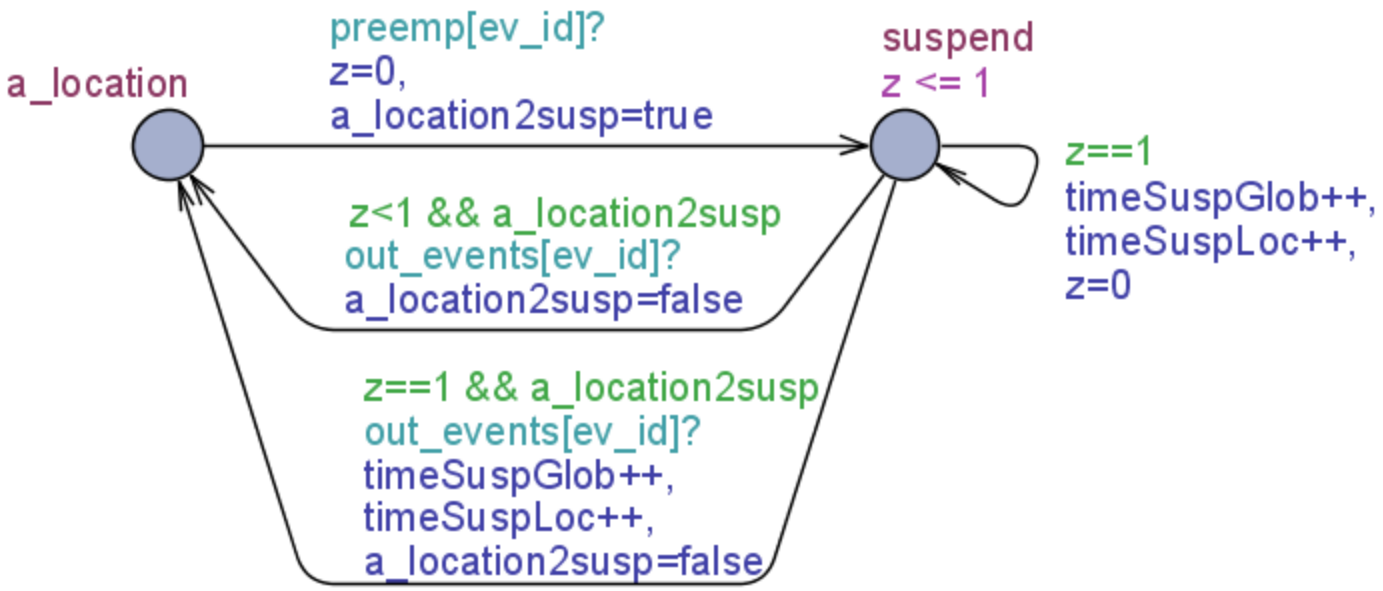
- 2nd Step
  - Statechart Diagram Translation





Preemption Support

- Preemptive *DispatchingModule* automaton
- Special location *suspend*



Model Checking

A[] not deadlock

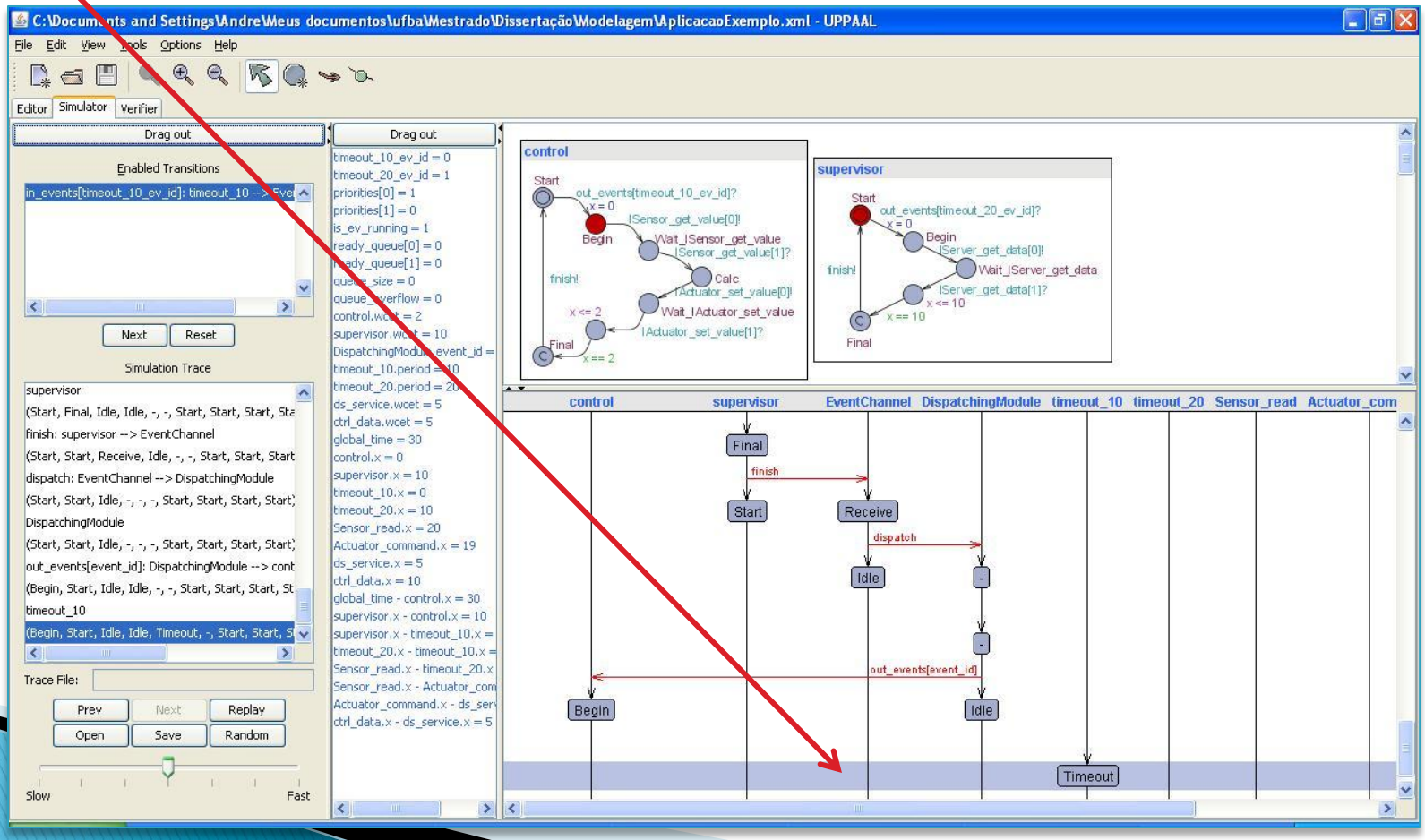
Property is satisfied.

E<> timeout_20.Timeout && !supervisor.Start && supervisor.x < supervisor.wcet

Property is not satisfied.

E<> timeout_10.Timeout && !control.Start && control.x < control.wcet

Property is satisfied.



Final Remarks

- Case study
  - Platform Screen Doors
  - 6 components and 28 statechart diagrams
  - State space explosion
  - Middleware functionalities
- Translation has been validated using model checking itself
- Improvements (next steps)
  - More elaborated scheduling policies
  - More refined configuration of generated models
  - Automatic generation of properties


Thank you!
amuniz@dcc.ufba.br
www.lasid.ufba.br
MERCADO MODELO
Salvador – Bahia – Brazil