Co-simulation of AADL and Simulink models using Polychrony on Polarsys

An Eclipse project of the Polarsys Industry Working Group
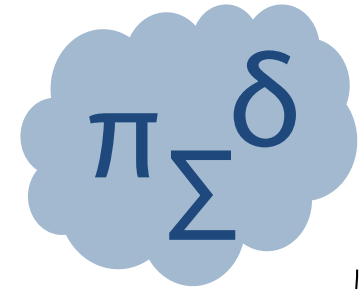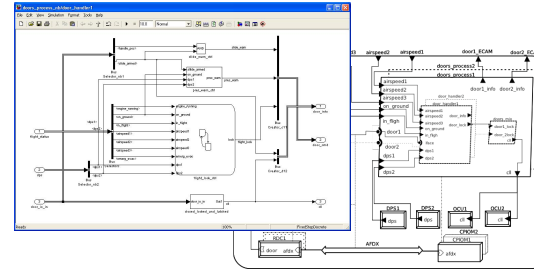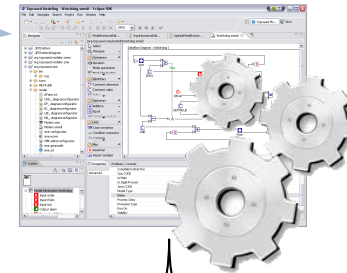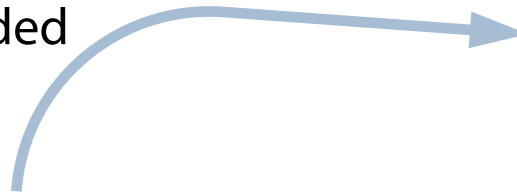
Jean-Pierre Talpin
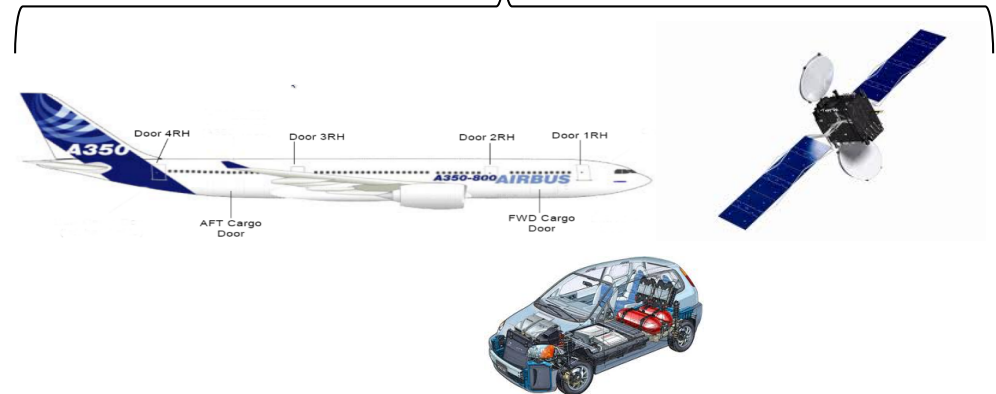
INRIA project-team TEA

Time
Events
Architectures

Formal methods for embedded system design

Focus on time modelling from an architecture perspective

Eclipse project POP for the open-source distribution of the toolset Polychrony on the platform of the Polarsys Industrial Working Group

Polychrony on Polarsys (POP)

An Eclipse project integrated in the platform of the Polarsys Industry Working Group

An implementation of the synchronous multi clocked model of computation of the data-flow language Signal
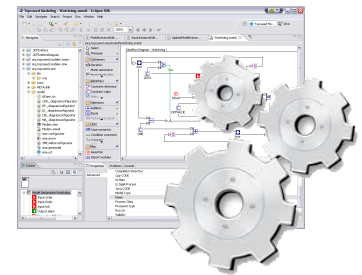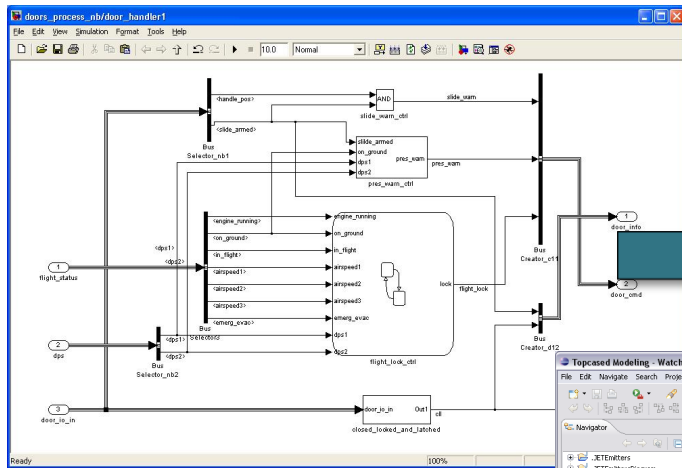
A toolbox for synthesis in computer-aided system design consisting of transformations, verification, and code generation functionalities
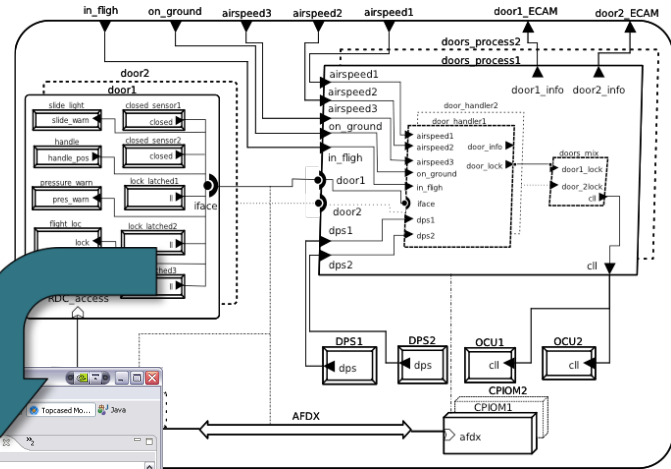
https://www.polarsys.org/projects/polarsys.pop

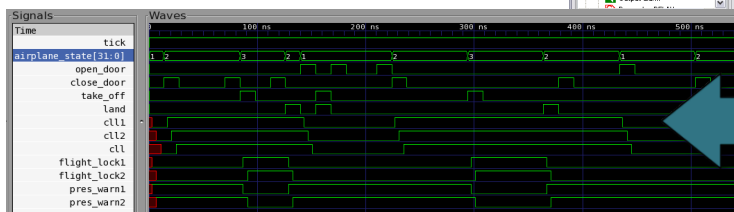# Case study of the A350 doors management system

Simulink functional models

AADL architecture model

VCD interface

verification and simulation code generation infrastructure

Co-simulation, profiling, scheduling, verification, performance evaluation

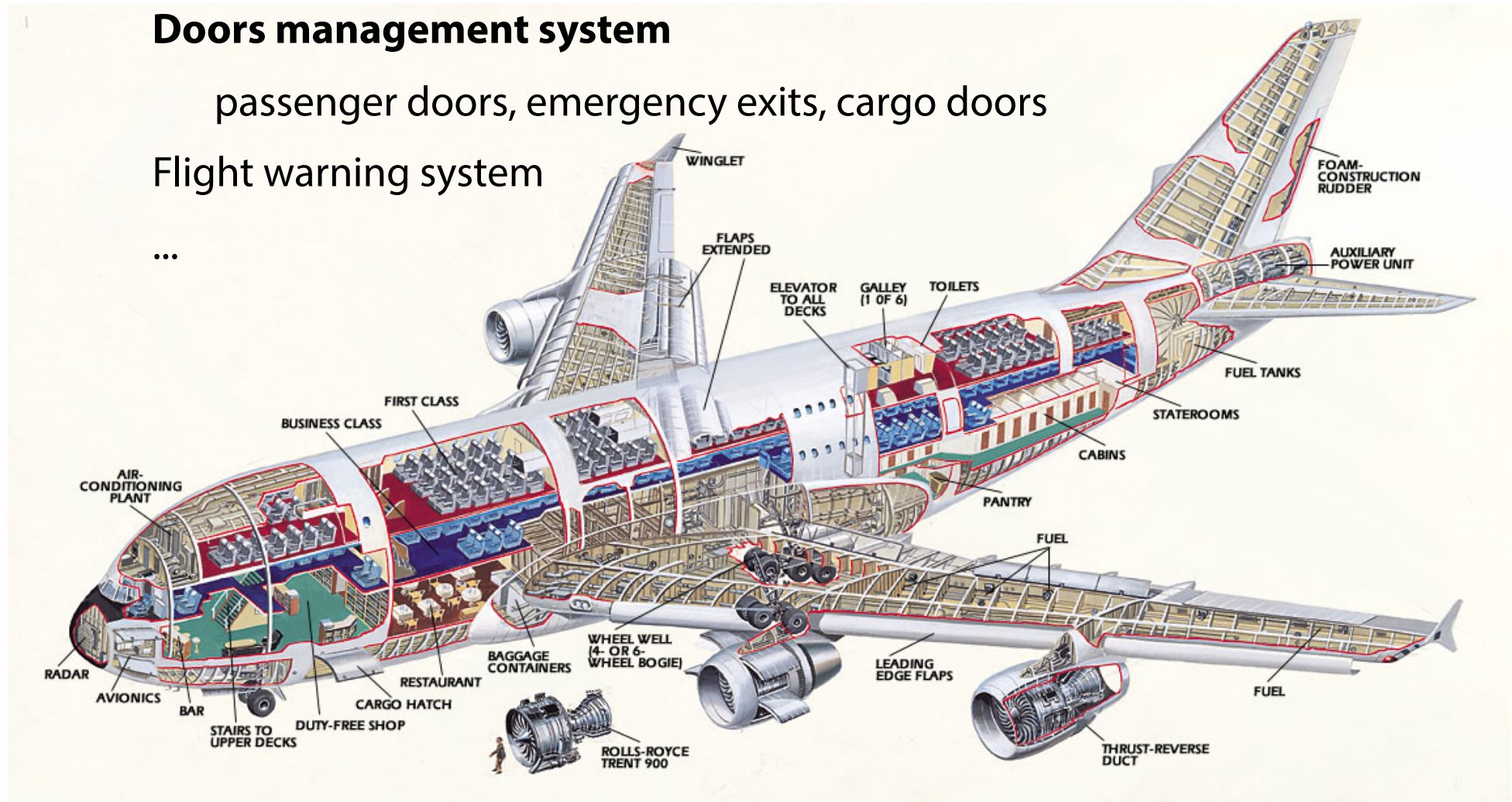# Case study of the A350 doors management system

Flight control systems

Landing gear system

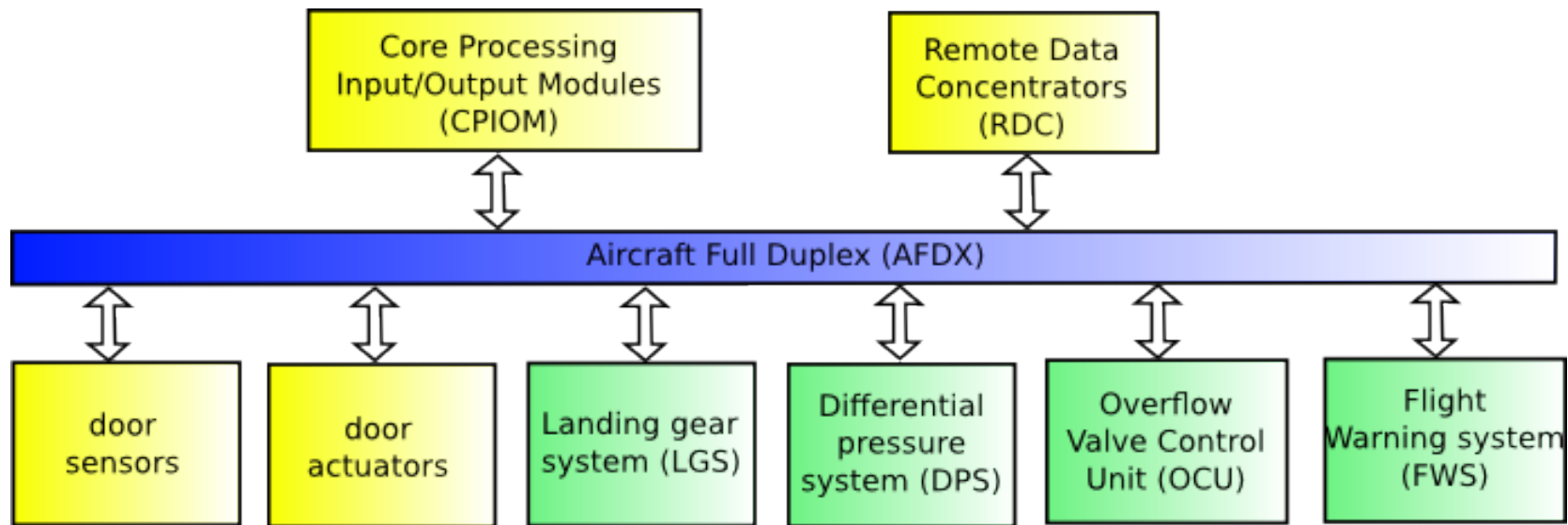**Doors management system**

passenger doors, emergency exits, cargo doors

Flight warning system

...

Case study of the A350 doors management system

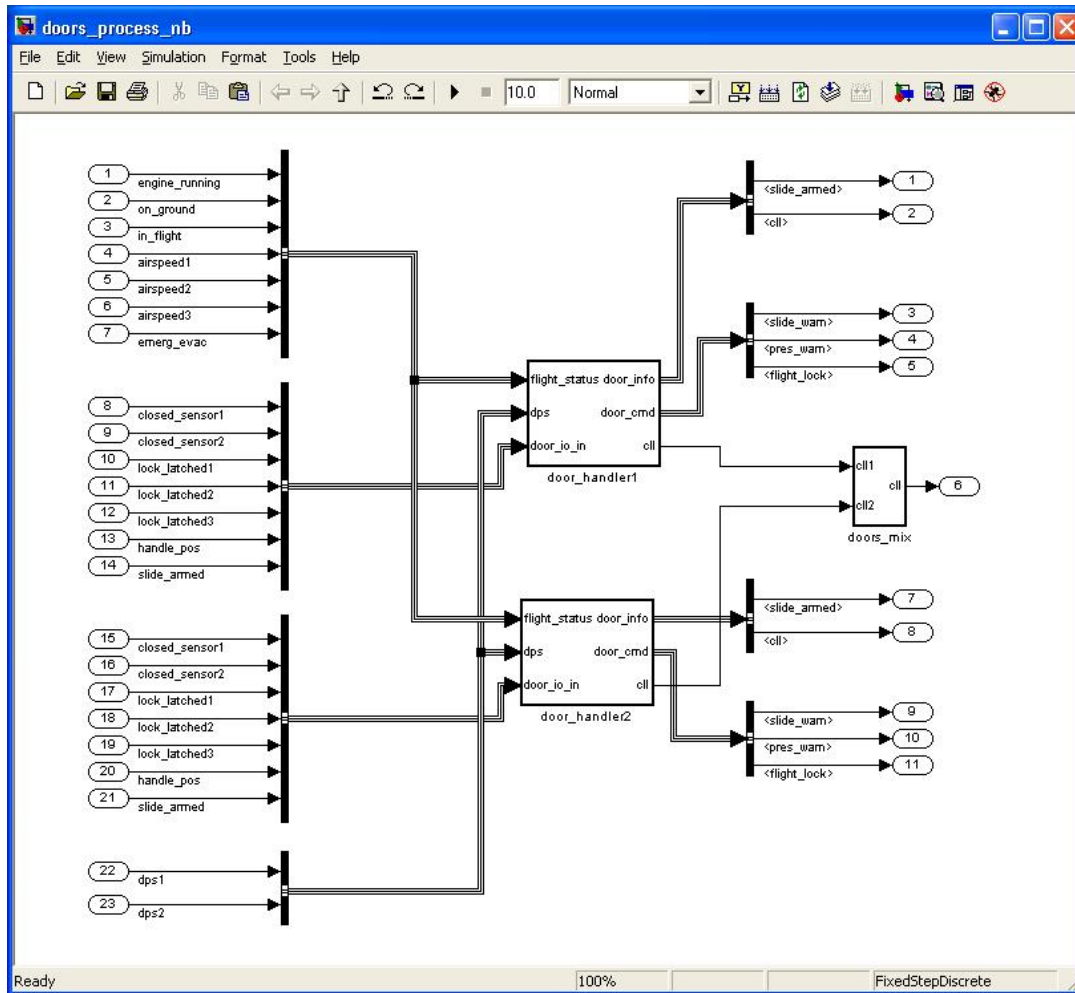**System-level model of the Doors and Slides Control System (SDSCS)**

Function

Monitor doors status via sensors

Control flight lock actuators

Manage the residual pressure

Inhibit incorrect cabin pressure

A safety-critical system

High-level modeling

Early validation & verification

Architecture exploration

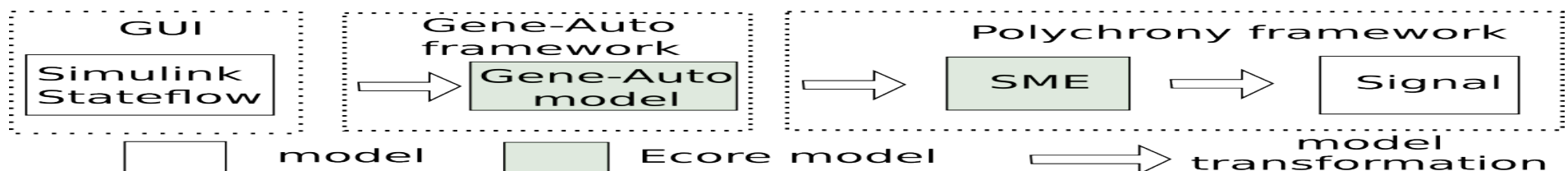# SDSCS functional model (Simulink)

Simulink
Matlab Simulink and Stateflow, a popular high-level modeling language

Gene-Auto
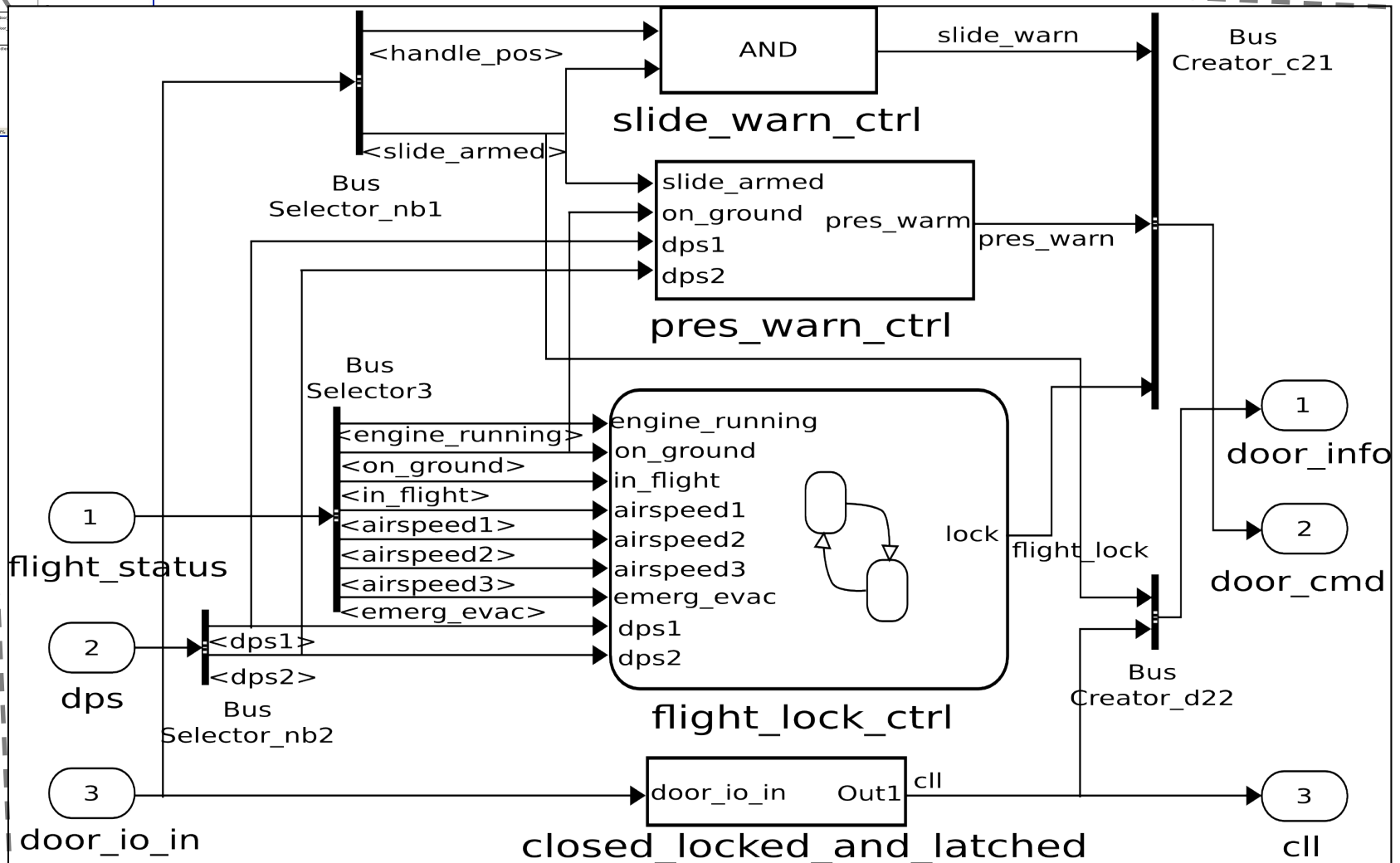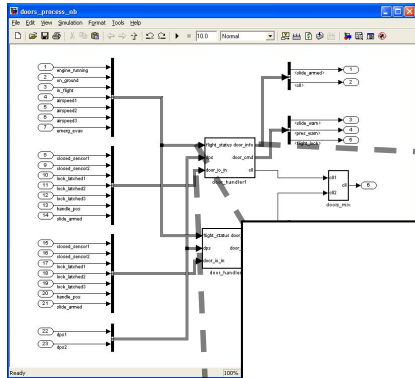A safe subset of Simulink/ Stateflow
Logical time and synchronized data-flow

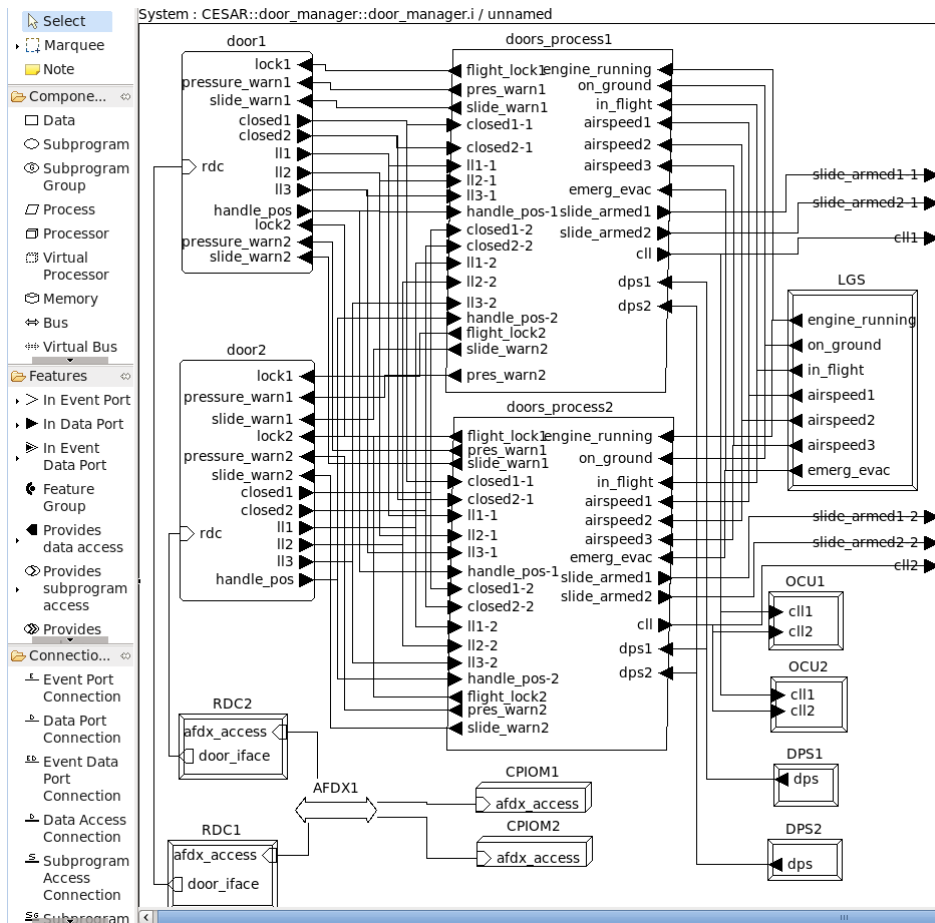**A complete transformation tool-chain with Polychrony**

SDSCS functional model (Simulink)

Zoom on the data-flows and mode automata of the door handler process

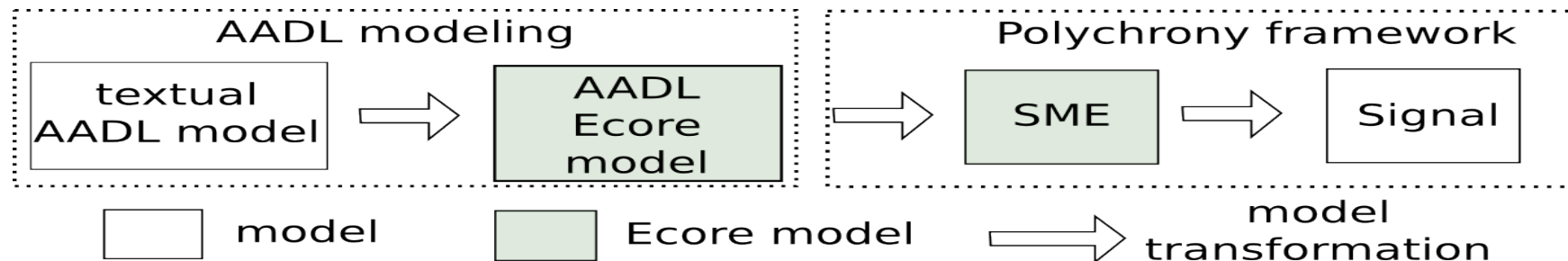# SDSCS architecture model (AADL)

AADL
An SAE standard for high-level, component-based, architecture modeling : application software, execution platform, composites
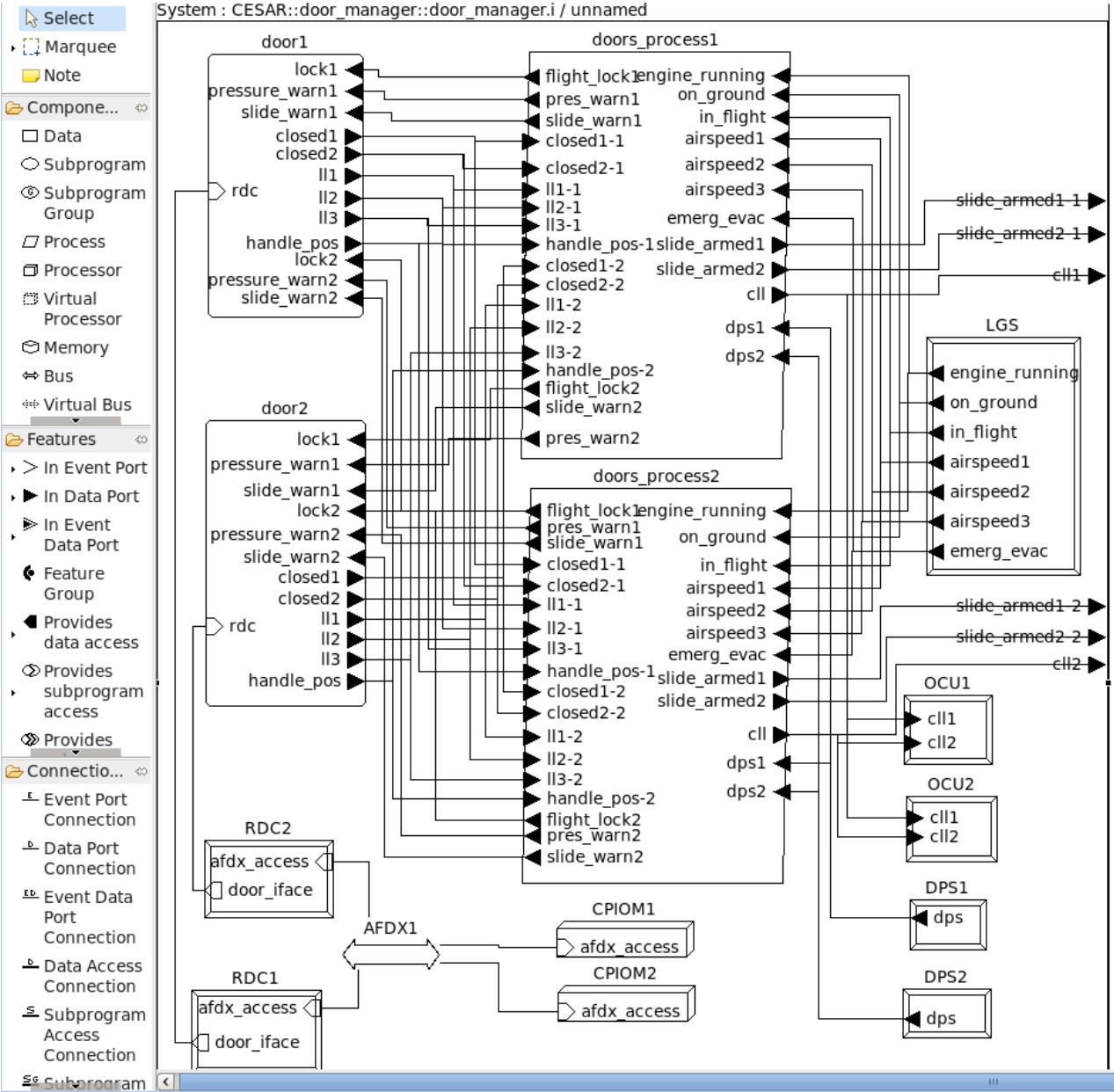
ARINC-653
An API for avionic software supporting the partitioned IMA approach

A complete transformation tool-chain with Polychrony
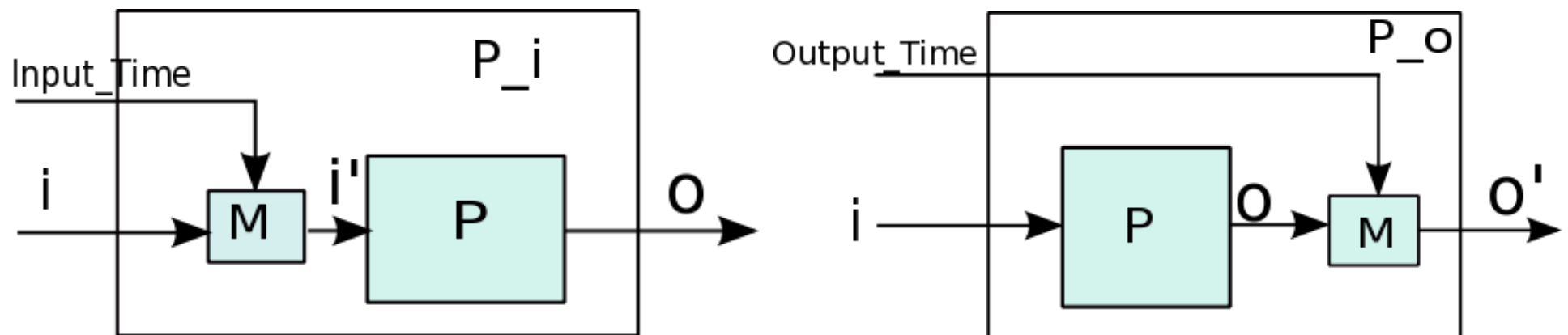
SDSCS architecture model (zoom)

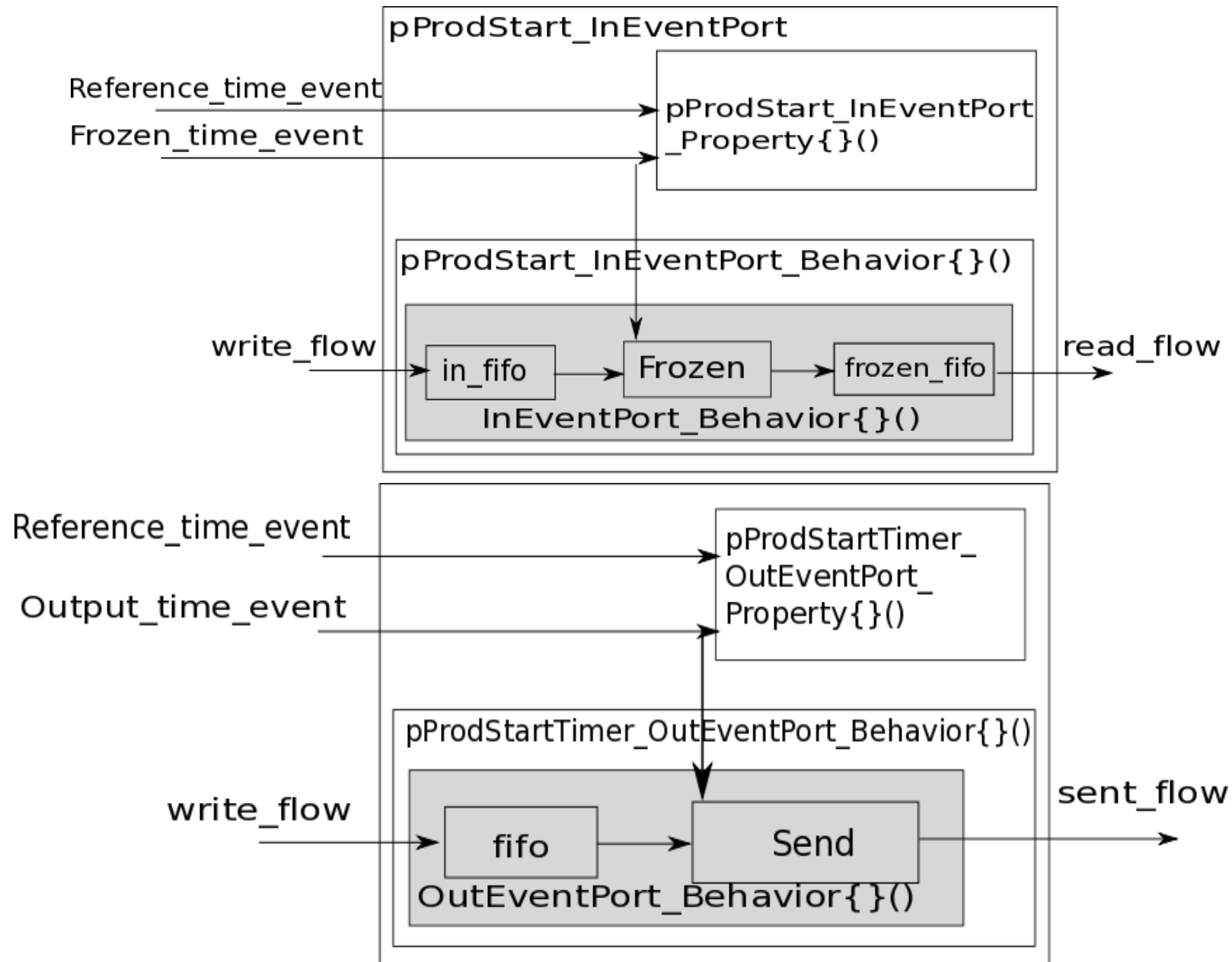# Modeling communication latency

Polychrony

    Time is abstracted by Boolean logic

    Communication is instantaneous

AADL

    Thread communicate at specified time intervals

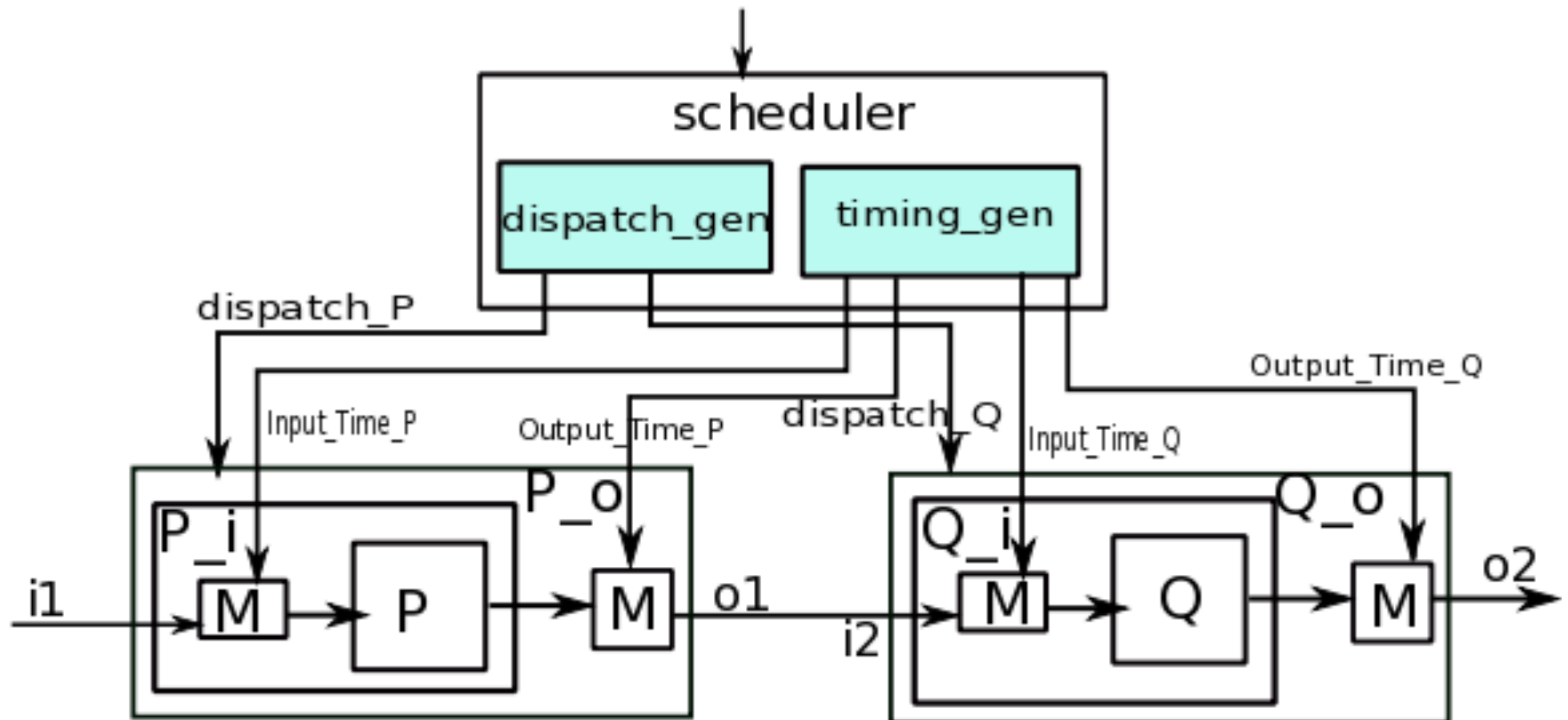   A process M models communication delay/timing
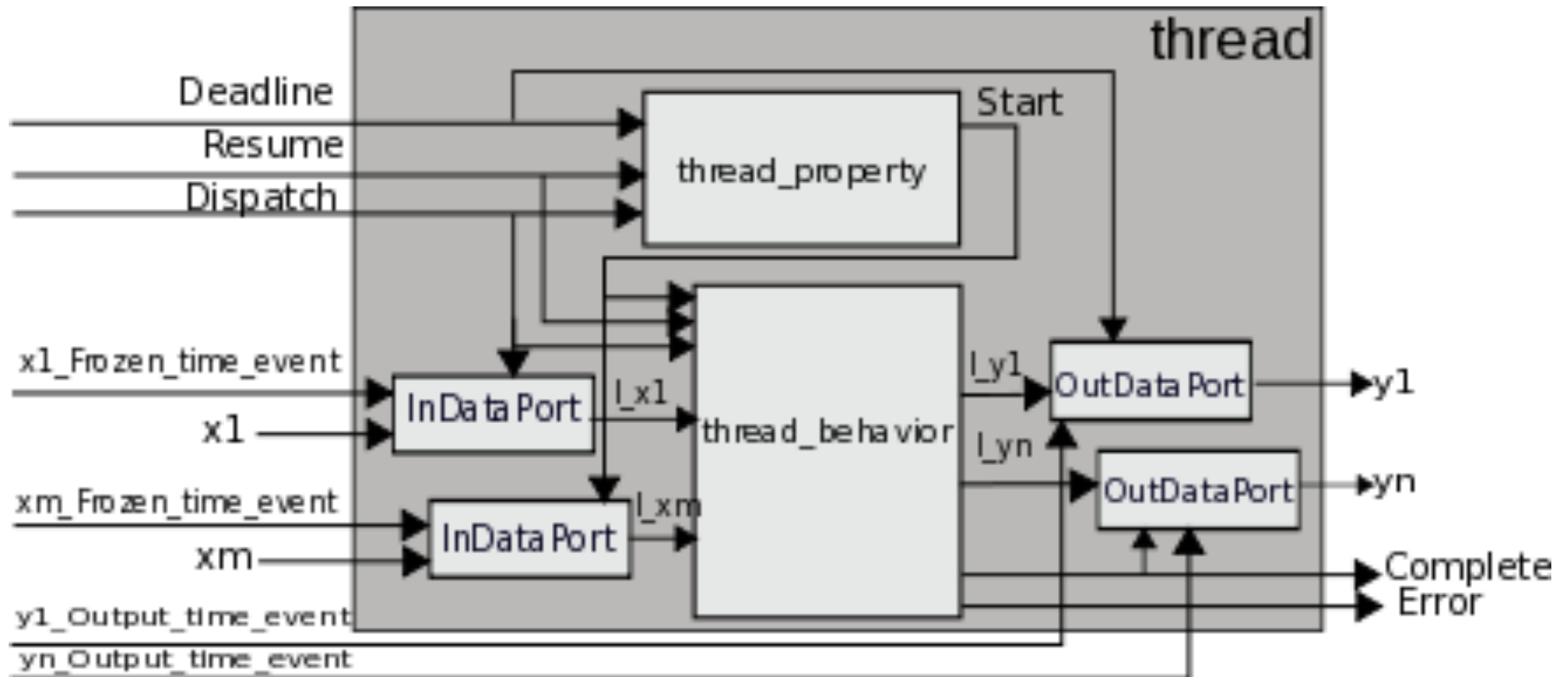
Modeling in/out event/data ports

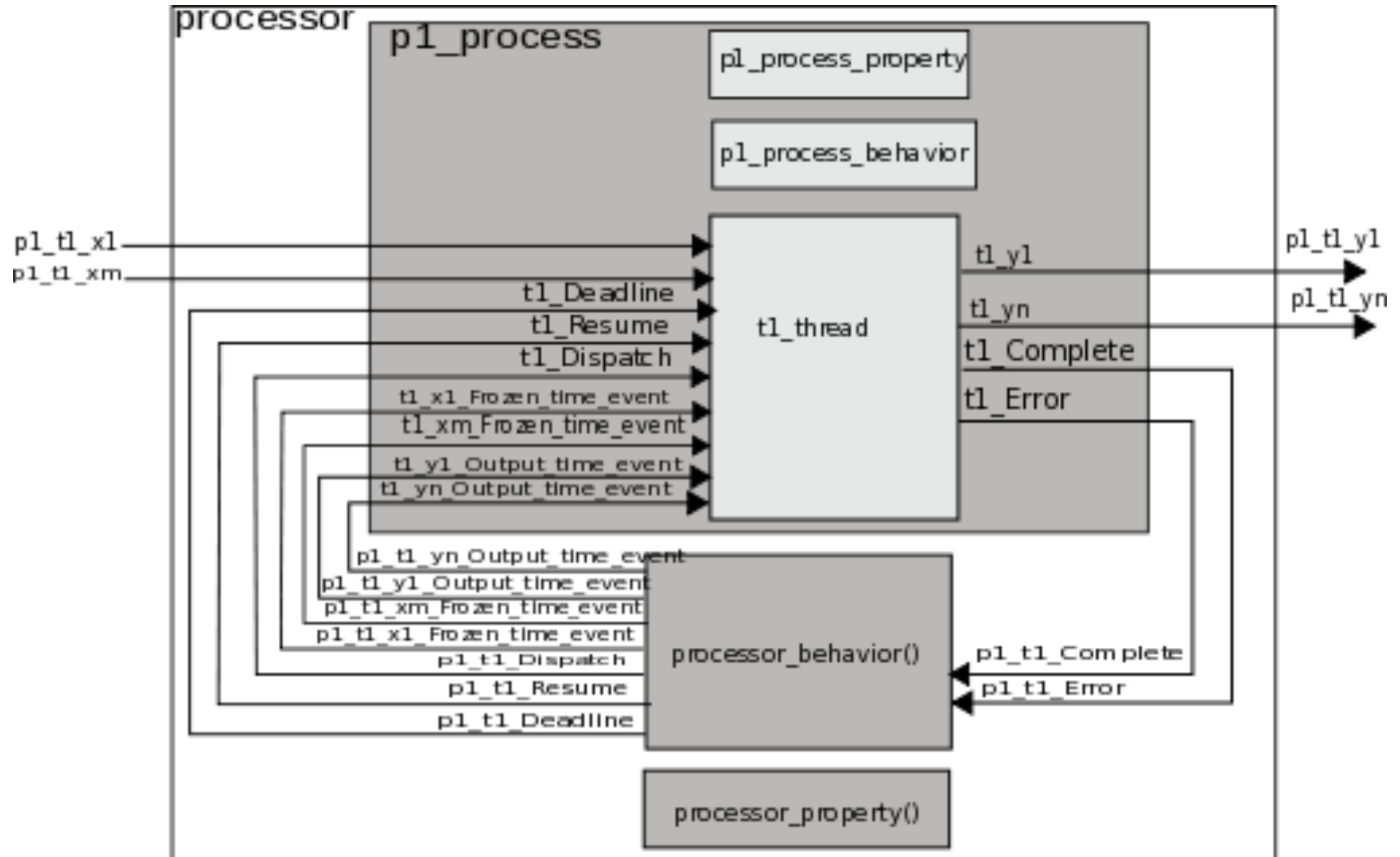# Modeling computation and communication scheduler

Polychrony

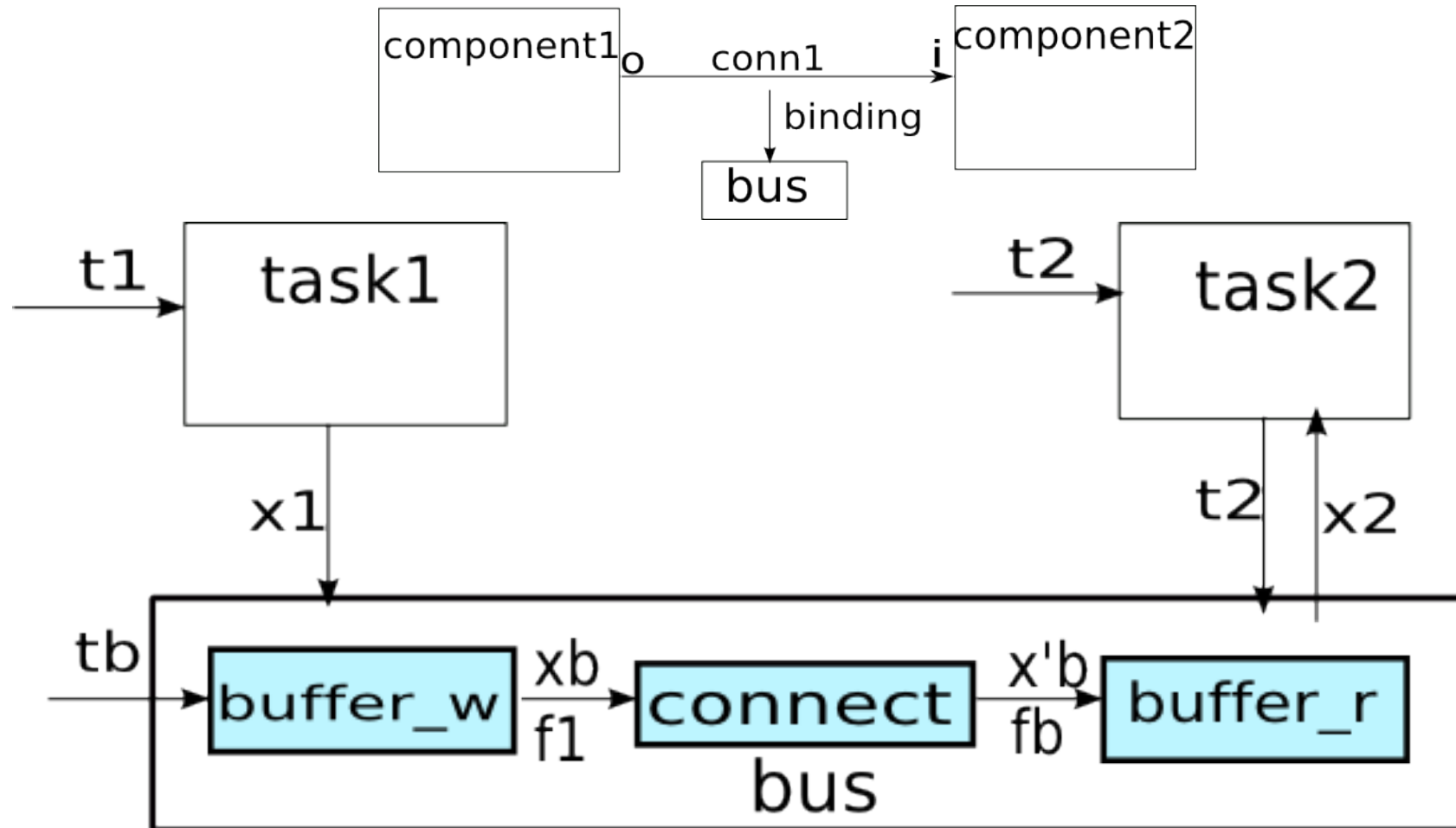Scheduling of communications can be synthesized

Modeling an AADL thread
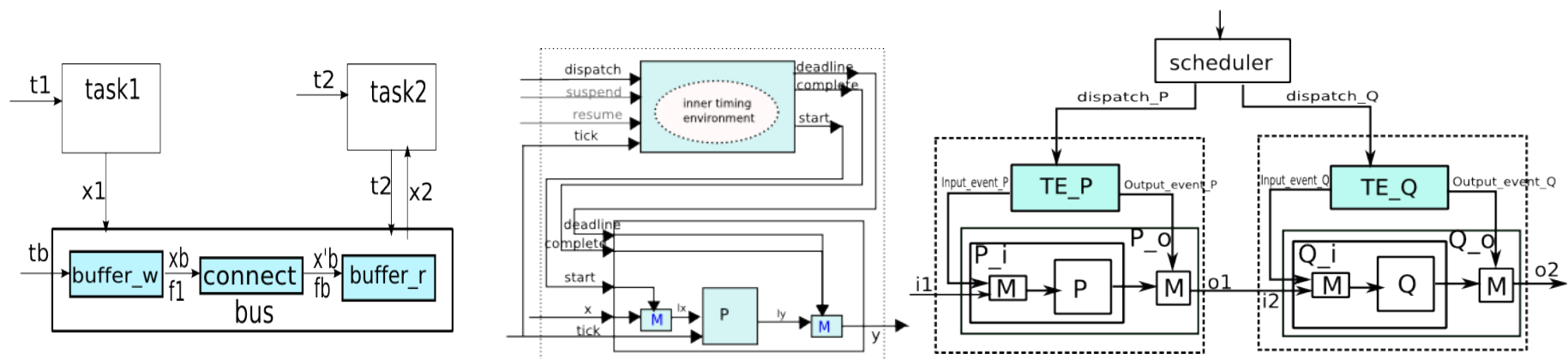
Modeling process/processor mapping
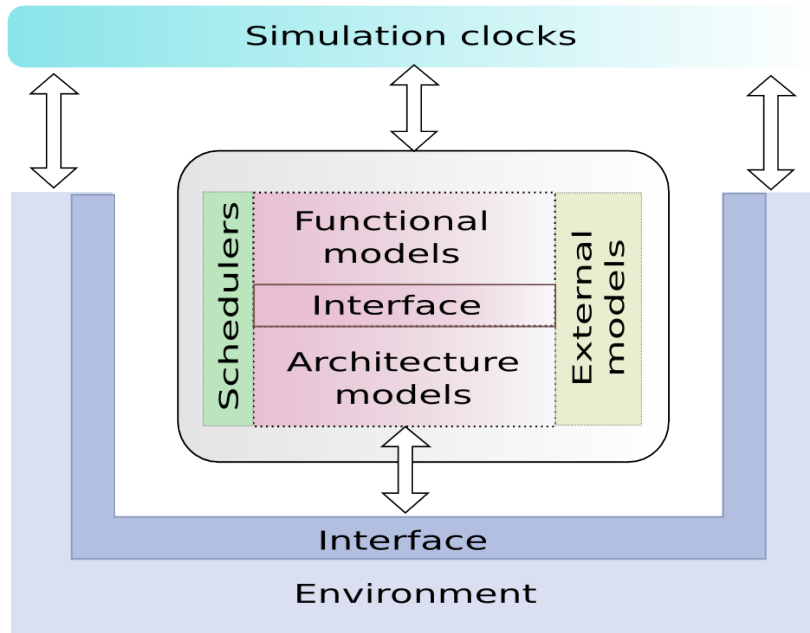
Modeling an AADL bus

Modeling AADL/RTOS services

Polychrony provides a library of templates to model
- AADL concepts (avionic standard to model architectures)
- ARINC-653 RTOS services (avionic standard to model IMAs)

Simulation model (Polychrony)

Additional models for open system simulation
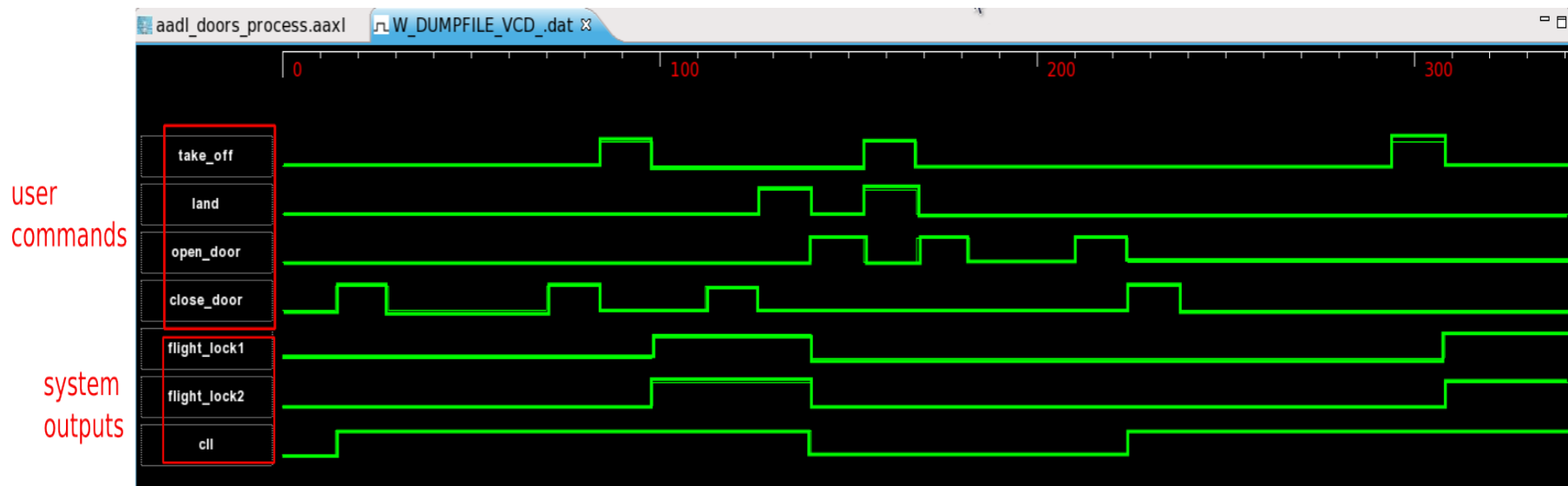
A simple, non-preemptive, static scheduler

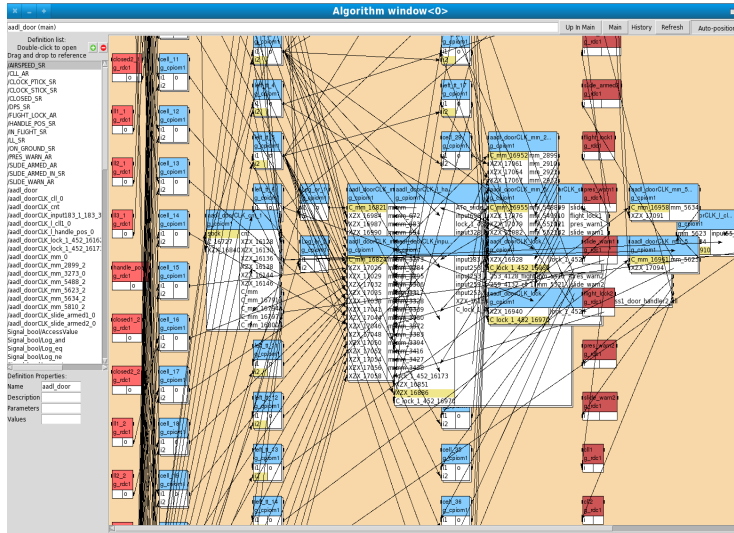Time intervals are abstracted

Simulation clocks

Reference clocks

Periodic clocks (threads)

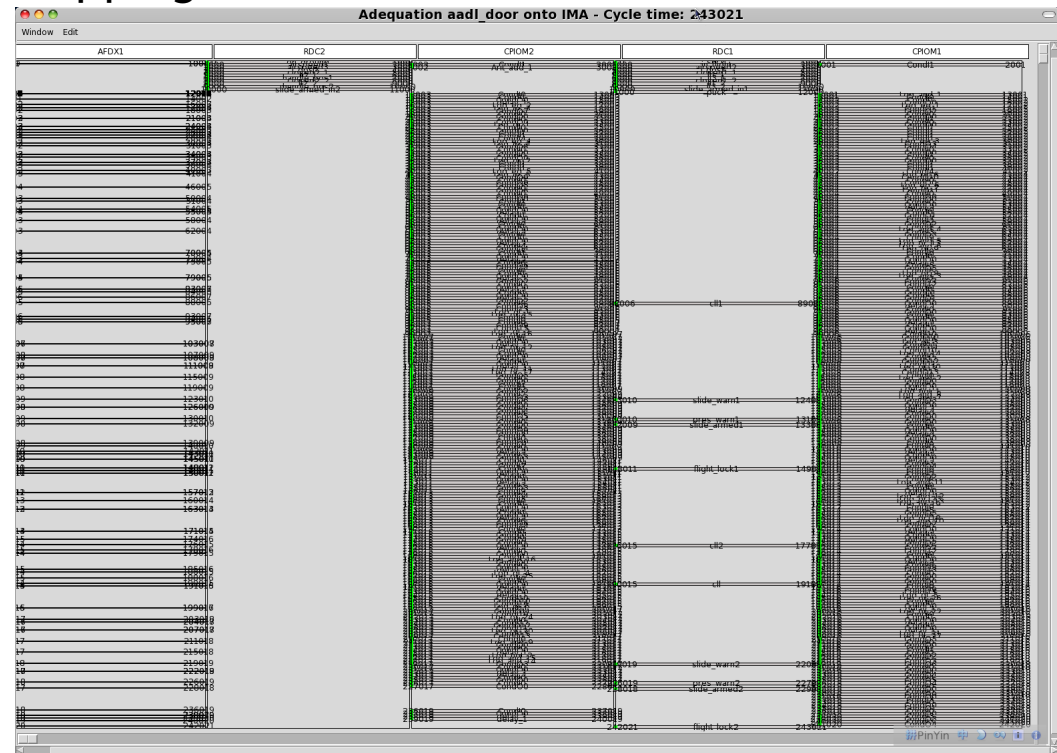**VCD interface -** Global simulation clock, interactive and of offline modes
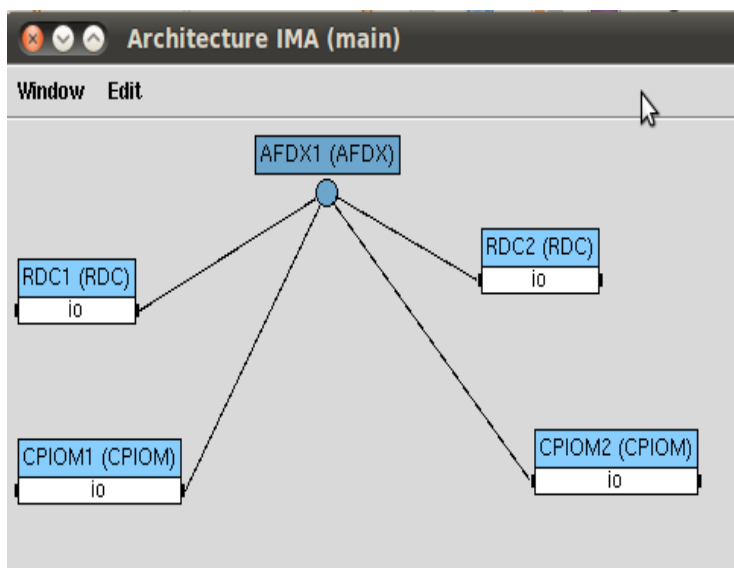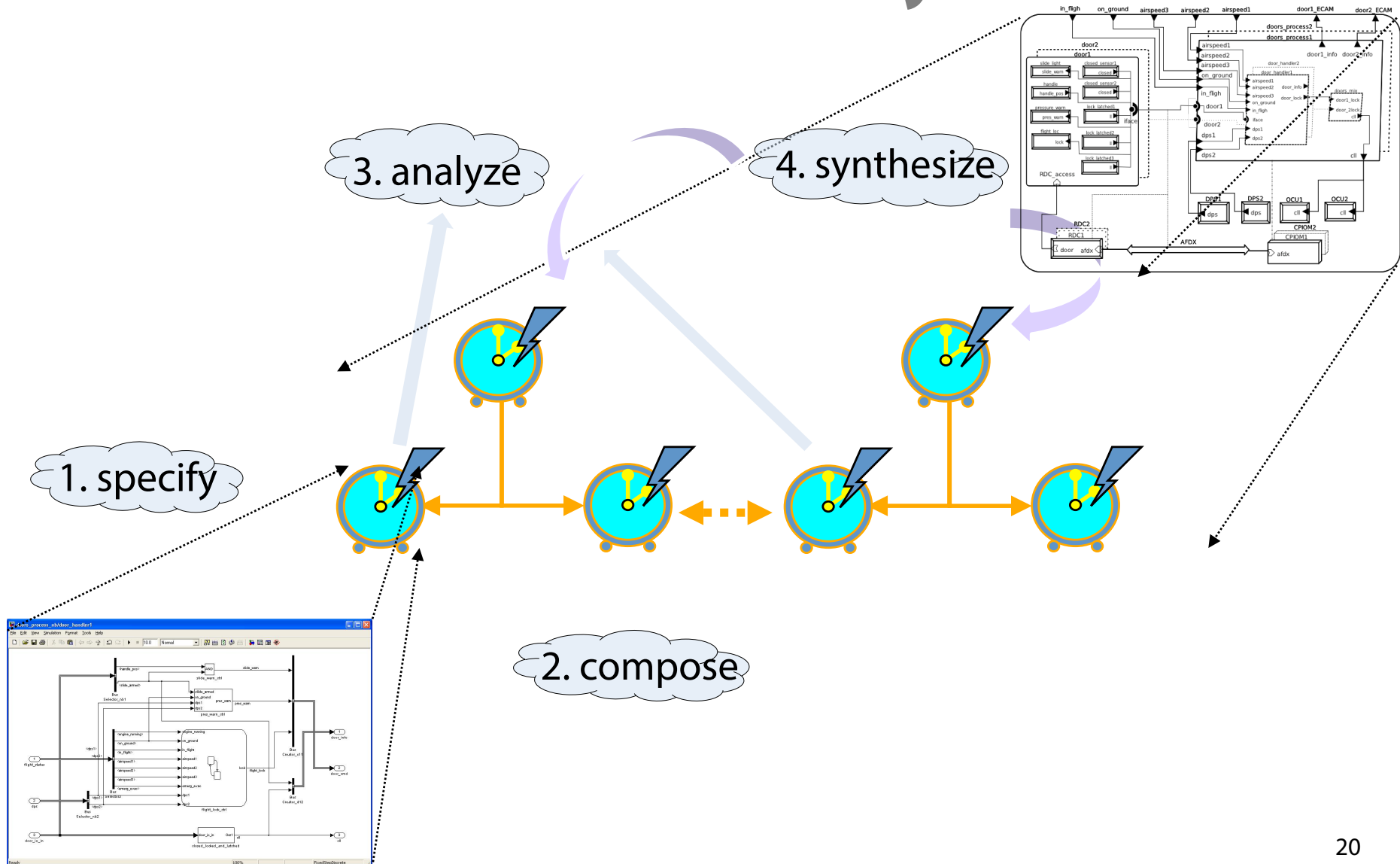
Real-time scheduling (Syndex)

Algorithm

Architecture

Mapping

Polychrony
A software architecture synthesis tool

3. analyze

4. synthesize

1. specify

2. compose

POP

A large toolbox for system architect

A model of computation and communication for software architecture exploration

• Data-flow for computation
• Mode automata for control
• Regular expressions for requirements
• Libraries for services

A toolbox of services
• Code generation
• Model transformation
• Model checking
• Controller synthesis
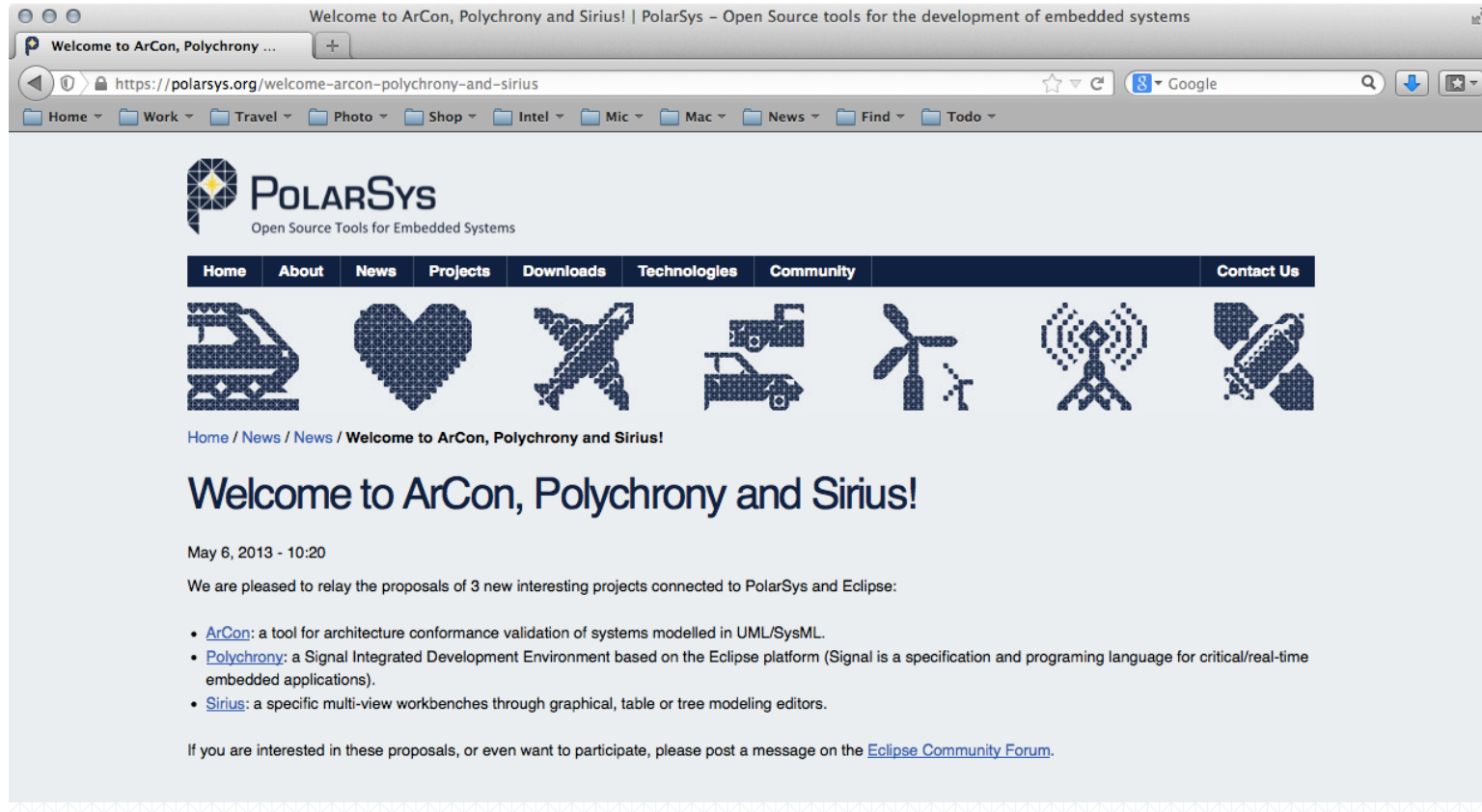• Syndex real time scheduling interface
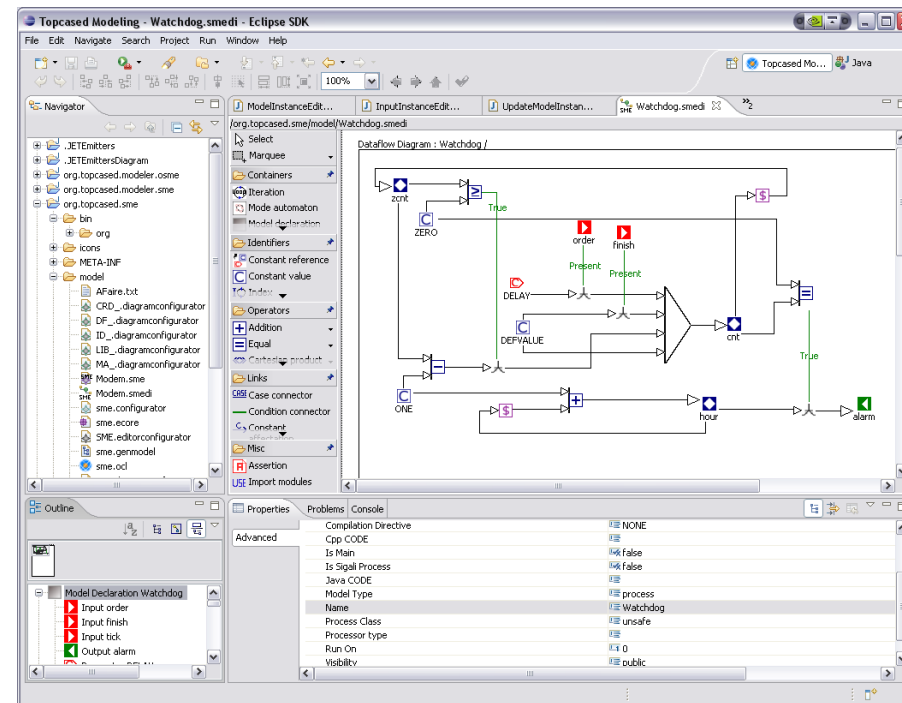
An interactive interface
• Open import functionalities
• Analysis and transformation
• Visualization and traceability

POP
An Eclipse project of the Polarsys IWG

https://polarsys.org/projects/polarsys.pop