Model-Based Approaches for an improved FDIR development and validation process

Jean-Paul Blanquart, Pierre Valadeau

ASTRIUM Satellites

ADCSS-2010 – NAVVA

Noordwijk, November 2nd, 2010

All the space you need

ASTRIUM
AN EADS COMPANY

Motivations

- Criticality, complexity of FDIR
- Needs
  - Rigour, formalism
  - Support to development, design choices
  - Validation
    - FDIR correctness, efficiency
    - Dependability properties
  - Linked to engineering artefacts, models
  - Support to changes, adaptation
- Model-based approaches

Objectives & Constraints

Need: Model the system dynamic in the presence of faults

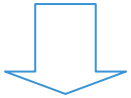
- Define a modelling technique
  - Express faults and failures propagation
  - Specify Fault, Detection, Isolation and Recovery mechanisms
- Demonstrate properties on Dependability/FDIR
- Appropriate modelling languages & tools

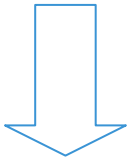
Requirements on modelling techniques

- FDIR
  - Spreading
  - Hierarchy
  - Time constraints
- Dependability
  - Deployment
  - Functional
  - Time constraints

- Simple modelling method
- Close to the engineering model

- Dysfunctional dynamic

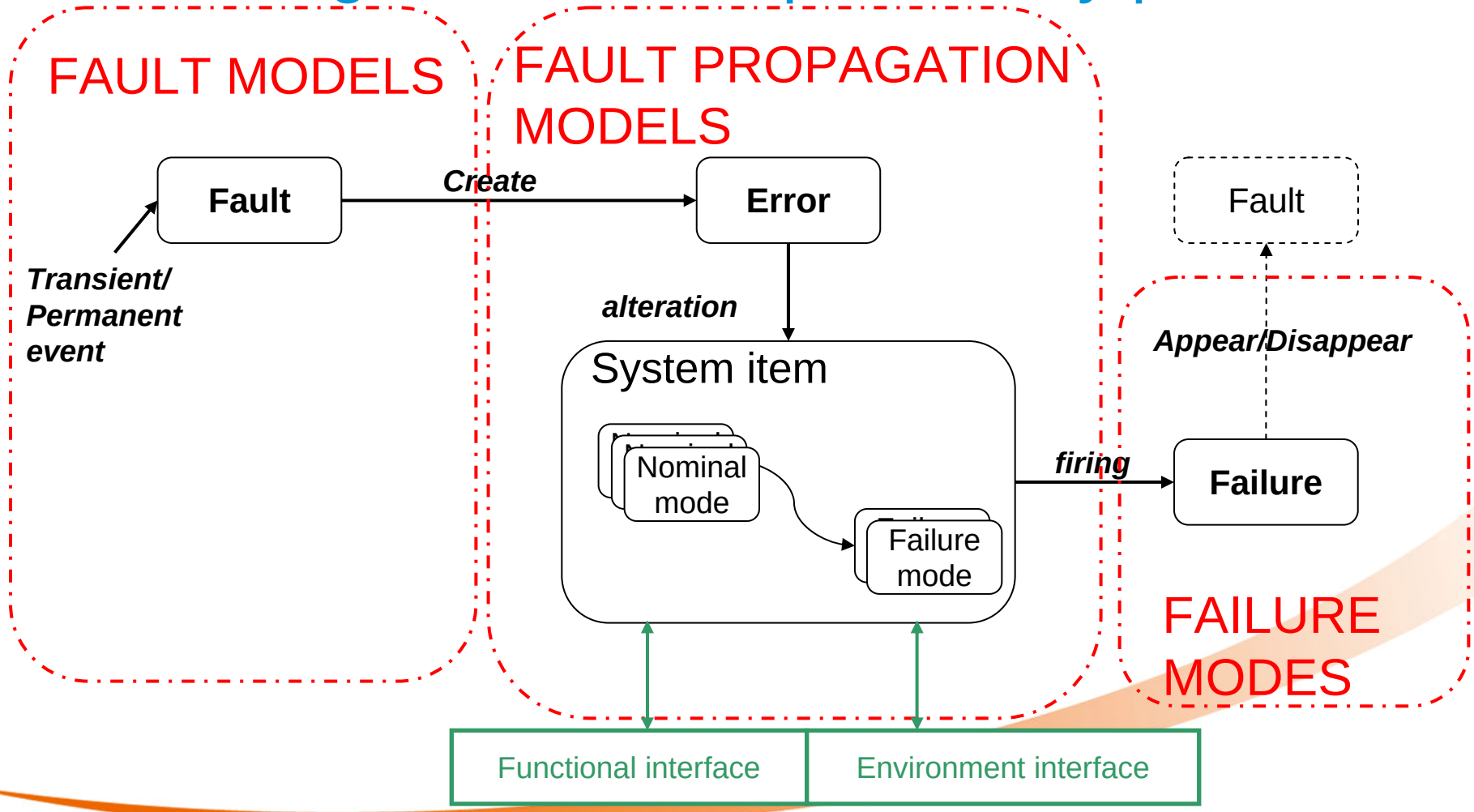




- Compositional approach
  - Dependability
  - FDIR
- Validation
  - Demonstration
  - Temporal

AADL → Timed automata(UPPAAL)

Modelling method – Dependability pattern



Modelling method

F4 :Data1 absent

=> {Data/ absent/…}

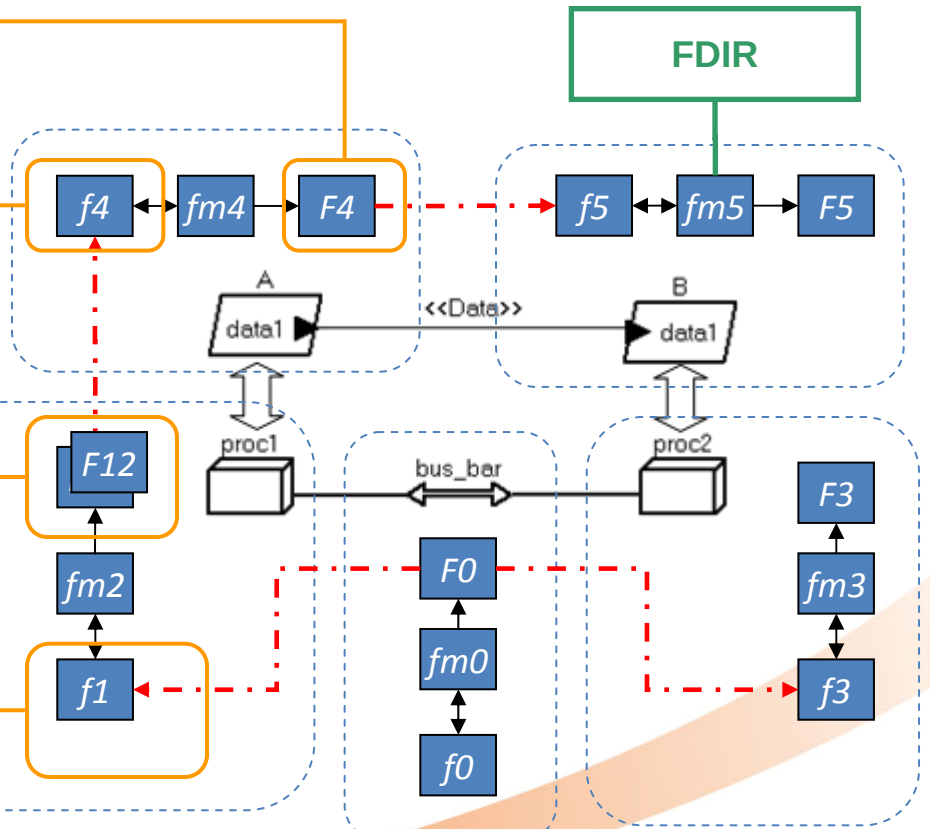
f4: => {resource/processor/computing/…}

F1 : total loss of computing power

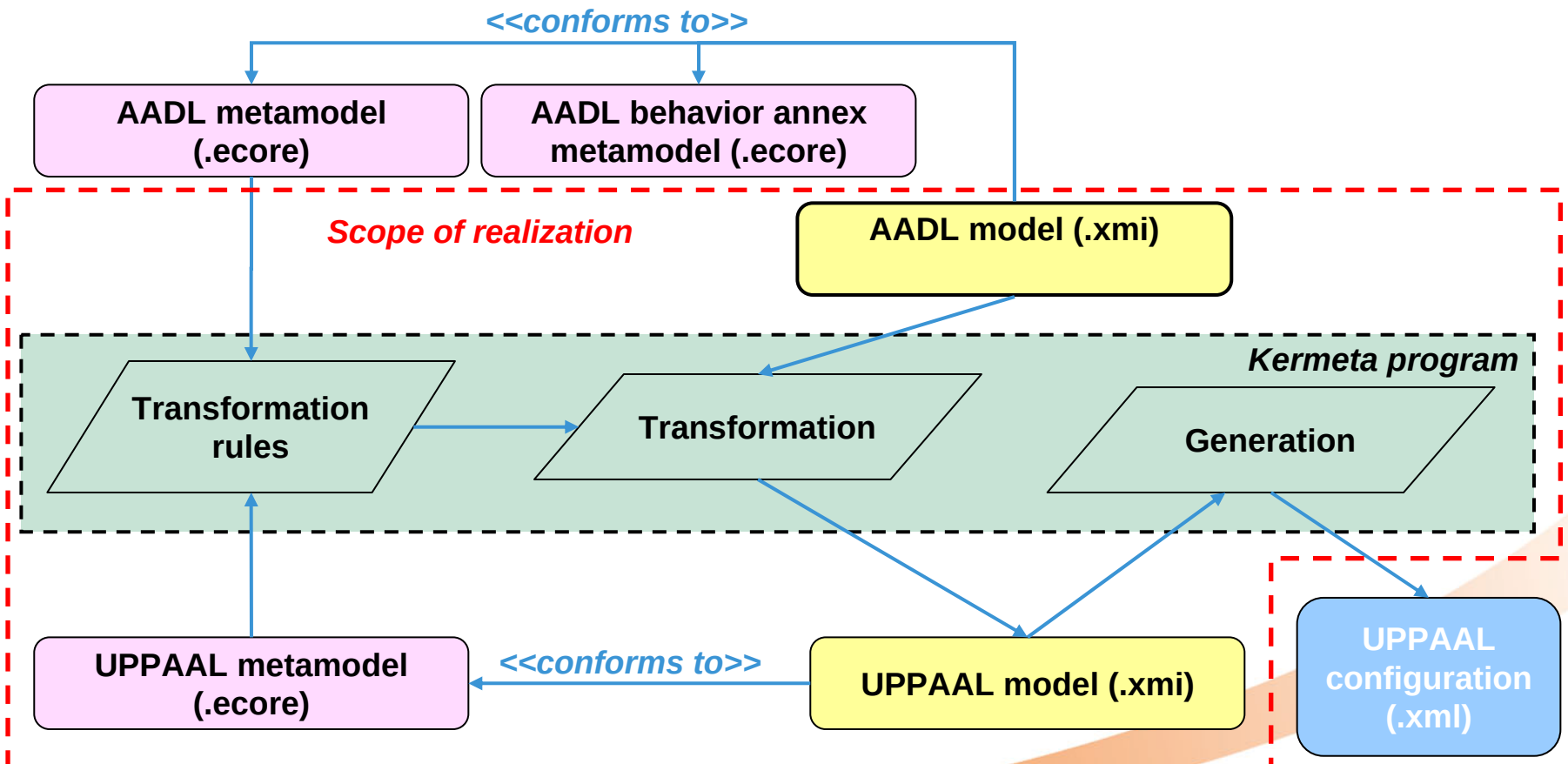
=> {resource/processor/computing/…}

f1 : CPU internal fault

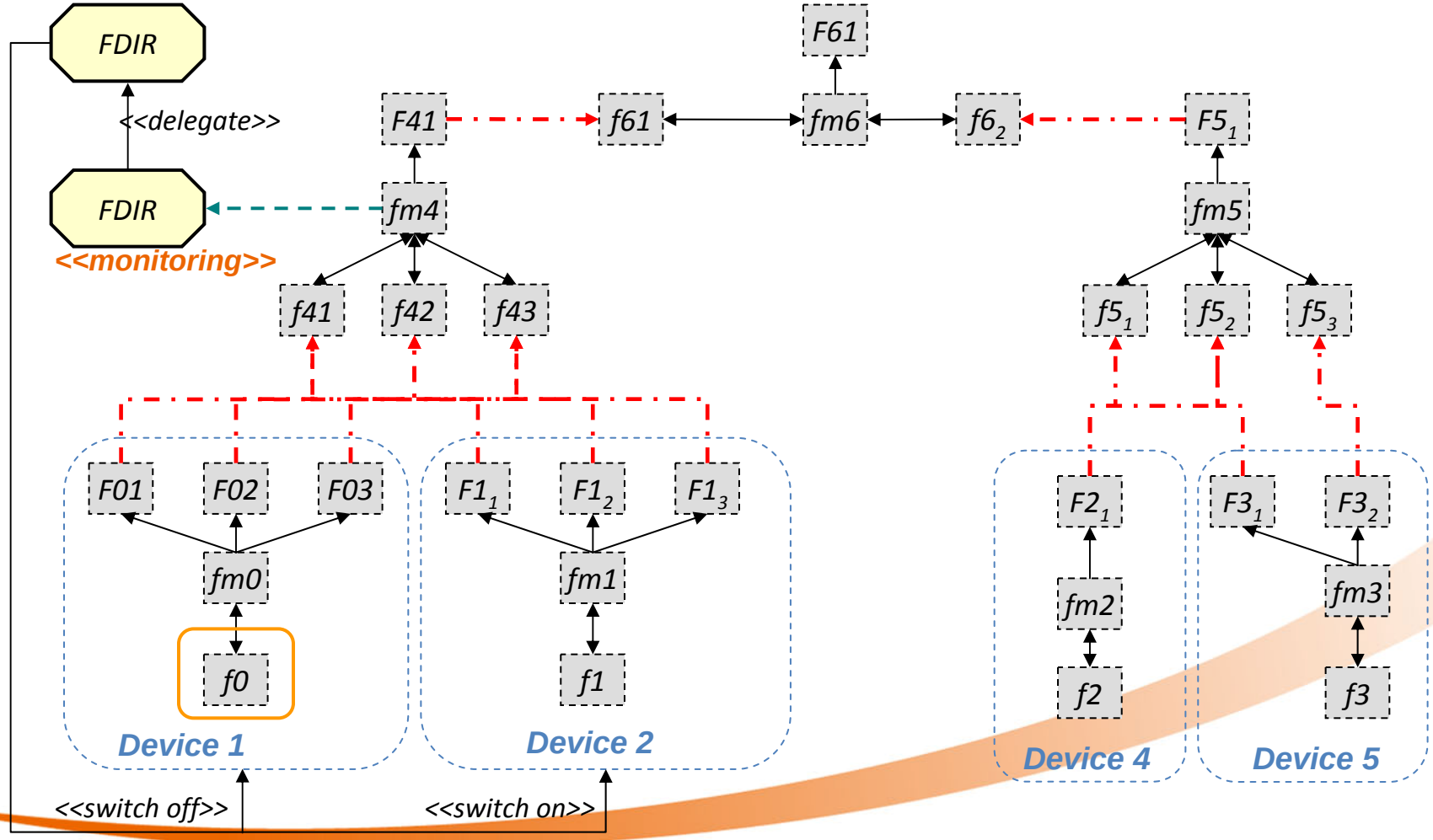
=> {resource/ processor/ computing/…}



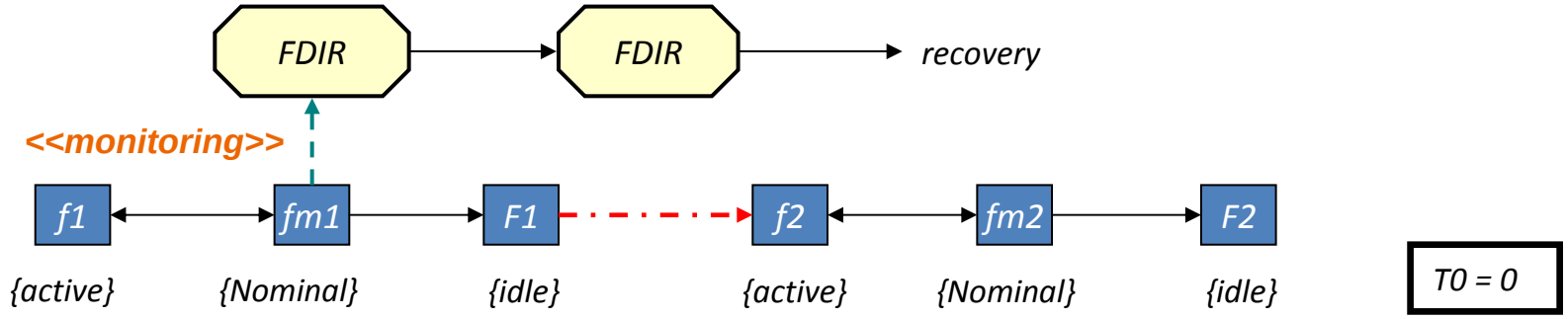
Model transformation



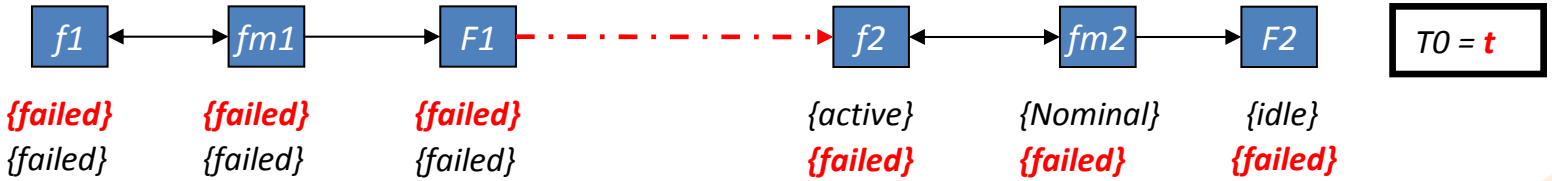
Model reduction – fault isolation



Model reduction – Step by step validation

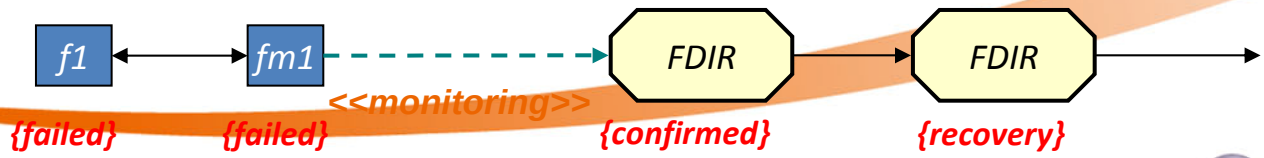


Find the earliest *t1 such that* this is true at *t*



Slowest recovery time(t2) < Fastest propagation time(t1)

Find the latest *t2 such that*



Conclusion, perspectives

- Systematic modelling method for dependability and FDIR
  - Compositional (dependability pattern)
  - Incremental (functional, dependability and FDIR layers)
  - Extensible (enhancement of deduced propagation paths)
  - Demonstrable (model reduction and model checking)
  - Complex propagation, common mode faults, external events, …
- Method improvements
  - Model reduction techniques, possibly resolution techniques
  - Complete libraries (fault models, failure modes, propagation rules)
- Integration into company's processes
  - Articulation of FDIR, Dependability, Engineering processes
  - Place of simulation, formal validation
  - Tools, methods benchmarking, training