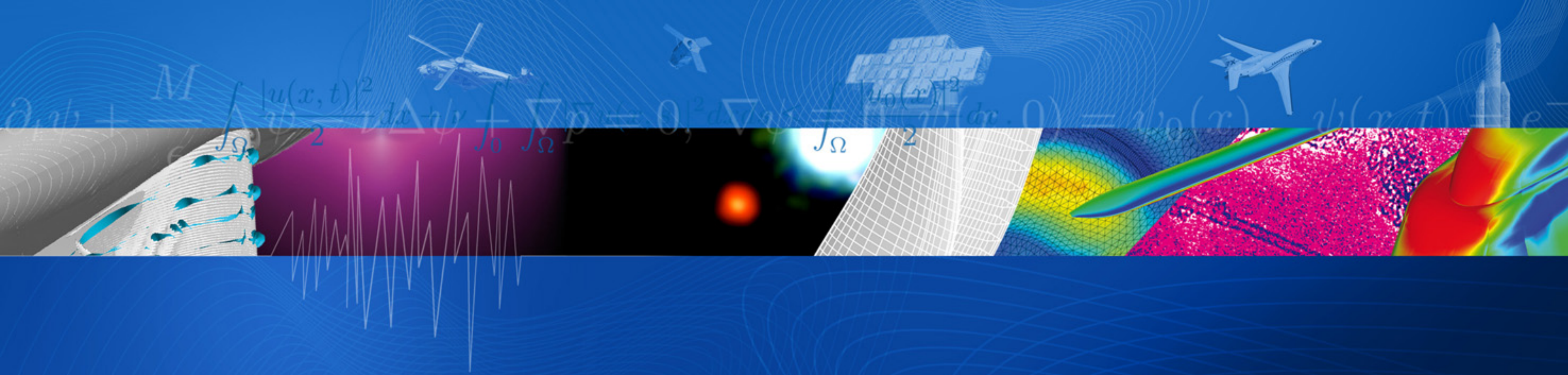


AltaRica language & tools
29/10/2015

J. Brunel, C. Seguin ONERA

ONERA

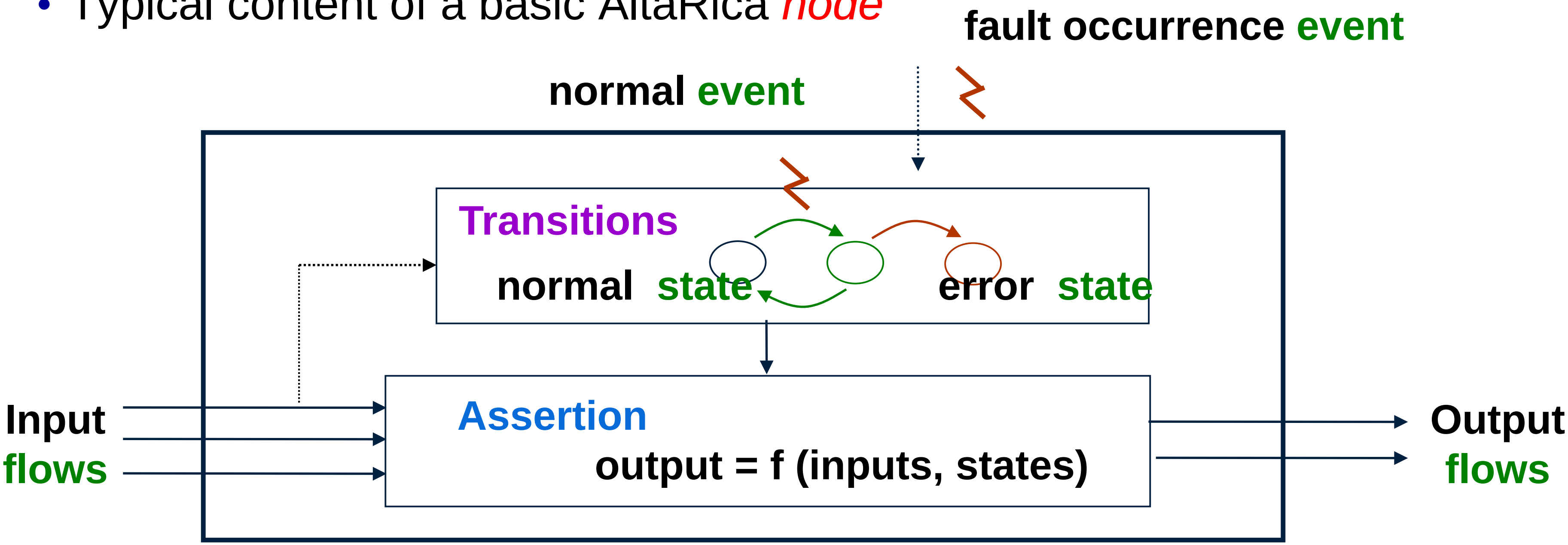
THE FRENCH AEROSPACE LAB

retour sur innovation

AltaRica language at a glance

- Language designed in late 90's at University of Bordeaux
  - for modelling both *combinatorial* and *dynamic* aspects of *failure propagation*
  - in a *hierarchical* and *modular* way
  - *formally*.

- Typical content of a basic AltaRica *node*



Several tools for analysing AltaRica models

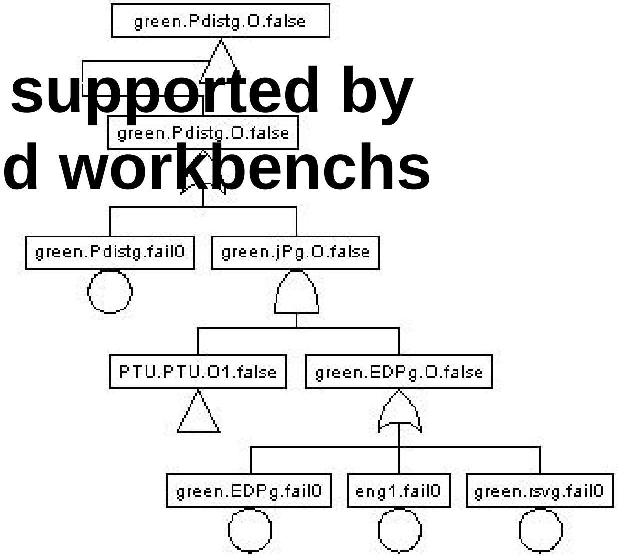
- Cecilia OCAS from Dassault Aviation
  - Used for the first time for certification of flight control system of Falcon 7X in 2004
  - Tested by contributors of ARP 4761 (cf MBSA appendix)
- AltaRica free suite from Labri
  - compatible with data flow restriction
  - http://altarica.labri.fr/wp/
- Safety Designer from Dassault System
- Simfia from APSYS Airbus group
- RAMSES from Airbus
- And plugins to independant tools
  - NU-SMV (FBK Trento), MOCA-RP (Satodev Bordeaux), Arc (LaBri Bordeaux) EPOCH (ONERA Toulouse)….

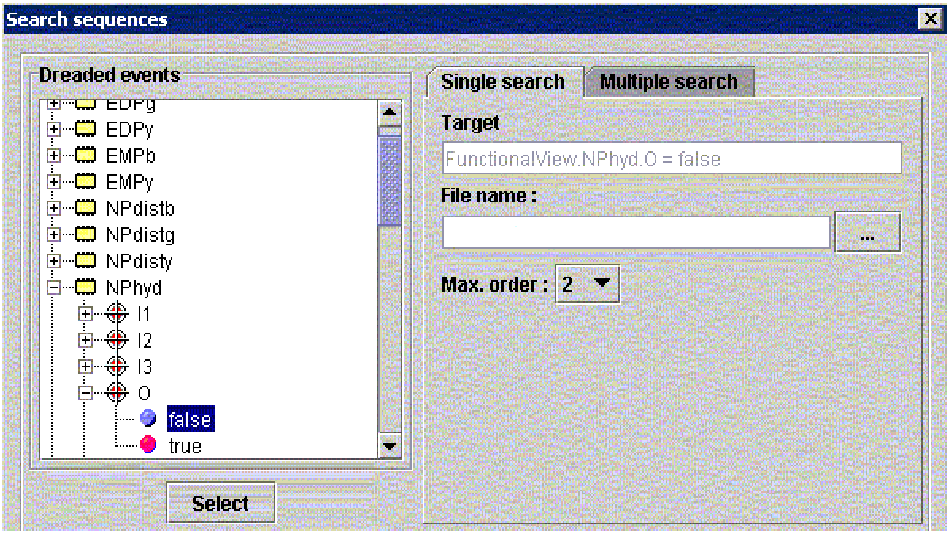
+ potential compatibility with tools of AltaRica 3.0 project

Several functions provided by the various tools

- Simulation
- Fault tree generation
- Sequence generation
- FMEA generation
- Stochastic simulation (MOCA-RP)
- Model-checking (ARC, Nu-SMV)
- Probabilistic model-checking (EPOCH)

Minimal set supported by all integrated workbenchs




Search sequences

Dreaded events
- EDPg
- EDPy
- EMPb
- EMPy
- NPdistb
- NPdistg
- NPdisty
- NPhyd
  - I1
  - I2
  - I3
  - O
    - false
    - true

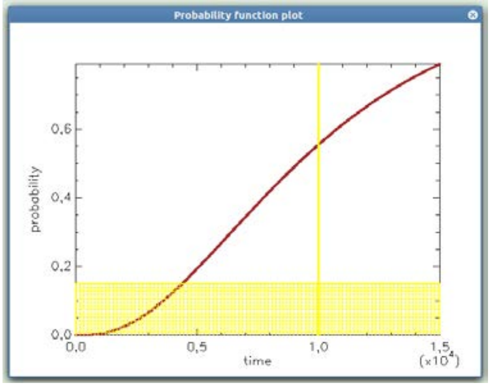
Select

Single search | Multiple search

Target: FunctionalView.NPhyd.O = false

File name :

Max. order : 2

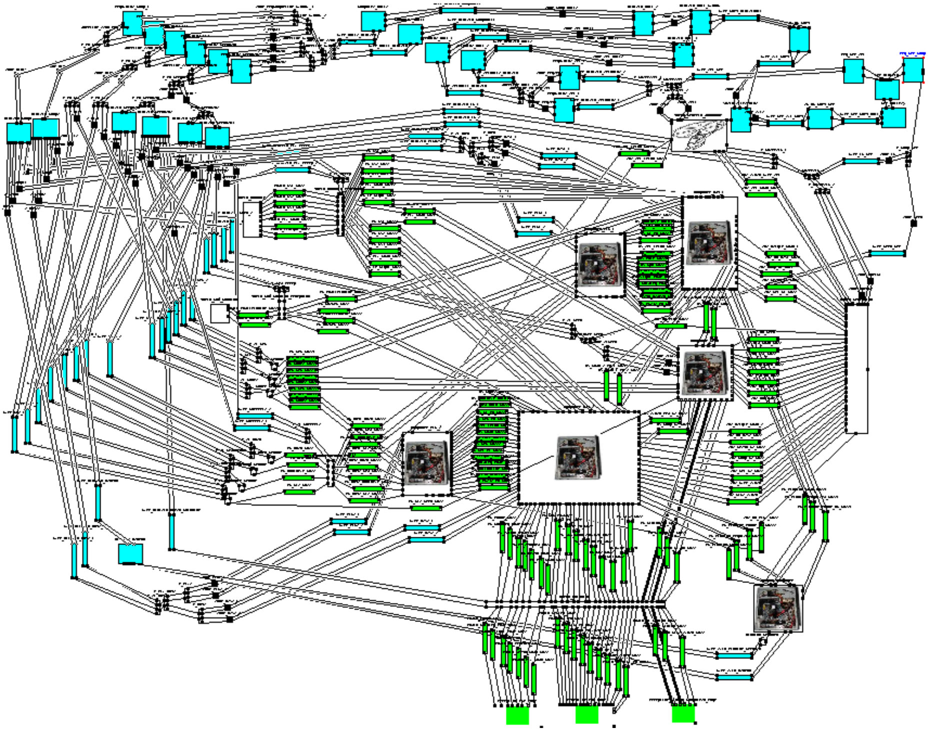


Example of application: architecture of flight control system of ONERA Vario UAV helicopter

- Safety requirement to be checked:

  "Total loss of the flight control is catastrophic.

  - *The probability rate of this failure condition shall be less than 10^{-9} /FH.*
  - *No single event shall lead to this failure condition."*



- AltaRica model of the system architecture
  - High combinatorial complexity:
    ~ 1000 components
    ~1500 failure events
    ~5500 port variables