ONERA

Formal techniques for embedded safety critical systems

P. Bieber, C. Castel, C. Kehren, C. Seguin

Office National d'Études
et de Recherches Aérospatiales
www.cert.fr

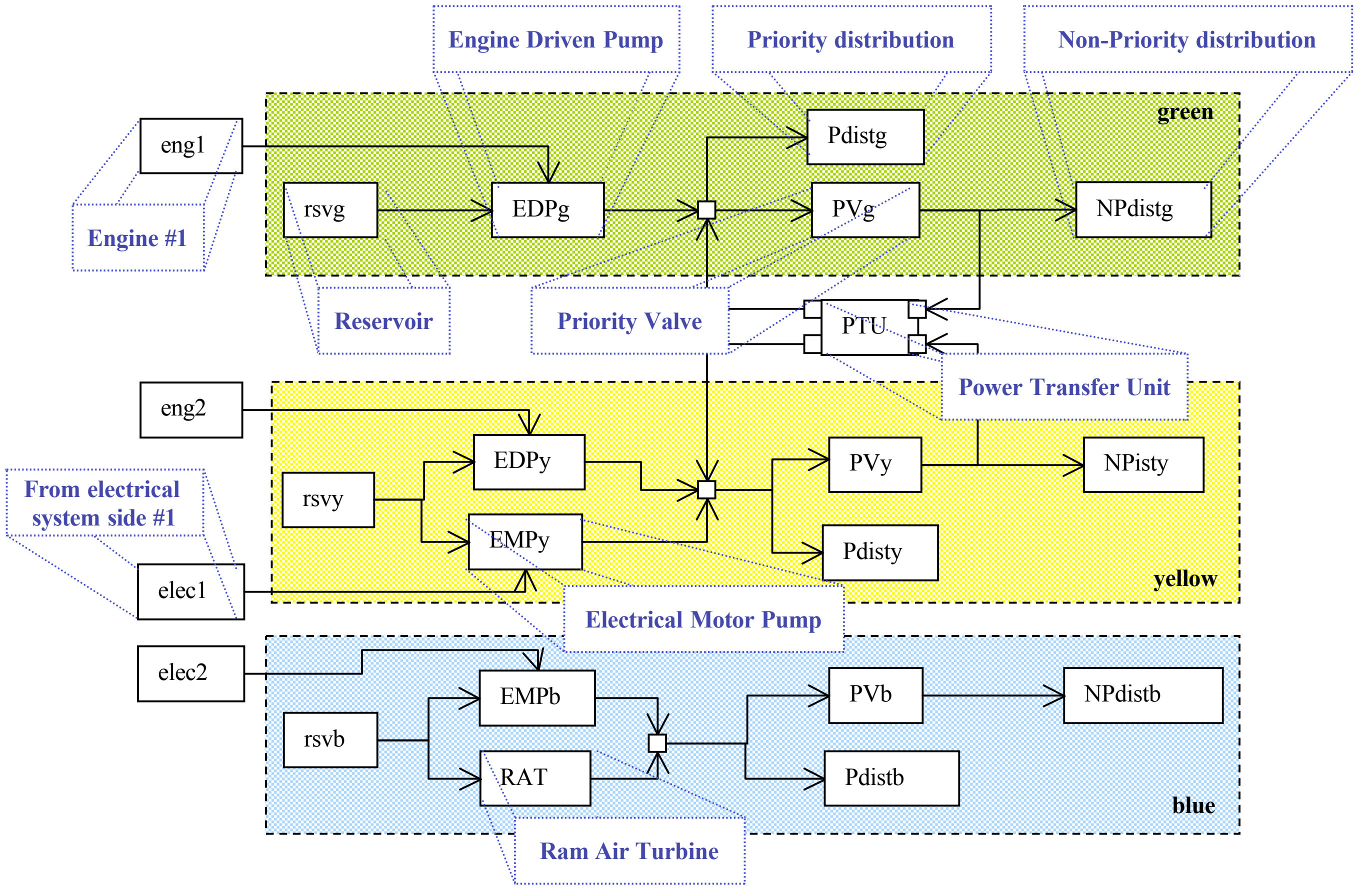
Presentation objectives

- Give a detailed introduction to formal approach for the assessment of safety critical systems
  - Overview of the assessment process
  - Focus on formal models and techniques that assist the failure propagation analysis
- Launch the discussion about the applicability of the approach for robotics systems

(Very) simplified assessment process for safety critical systems

- Starting point: hazard analysis
  - Goal: provide safety requirements to ensure that the probabilities of occurrence of feared events remain acceptable
- Failure propagation analysis
  - Goal: verify if a system architecture meets the safety requirements depending on some hypothesis about fault models and Fault Detection, Identification and Recovery mechanisms
- System verification
  - Goal: check if the implemented system is compliant with the hypothesis about fault models and FDIR

Model based failure propagation analysis: the example of the A320 like hydraulic system



_ Safety architecture: 3 independent lines

About 20 components of 8 classes: reservoir, pumps, pipes, valves ...

ONERA

Model based failure propagation analysis: example of safety requirements

- **Requirement :** "*Total loss of hydraulic power is classified Catastrophic, the probability rate of this failure condition shall be less than 10^{-9} /FH. No single event shall lead to this failure condition* " (SSA ATA29)

- **Extended qualitative requirements could be added to reveal architecture design concerns:**

  "if up to N individual failures occur then failure condition FC should not occur",

  with N= 0, 1, 2 if FC is Minor, Major or Hazardous, Catastrophic.

Model based failure propagation analysis: the AltaRica proposal

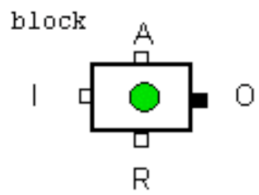
- **Language** (University of Bordeaux, 2000),
  - **formal,**
  - **well suited to safety**
  - **able to deal with complex models :**
    - _ hierarchical and compositional
- **Several available tools**
  - **By Dassault Aviation, Apsys EADS, Arboost, Bordeaux University, …**
  - **user friendly graphical model editor**
  - **Gateways to safety and validation tools**
    - _ boolean formulae _automatic FT generation …
    - _ (Petri nets, Markov chains) _stochastic simulation …
    - _ transition systems (SCADE, SMV, Mec V) _qualitative safety requirement assessment by model-checking …

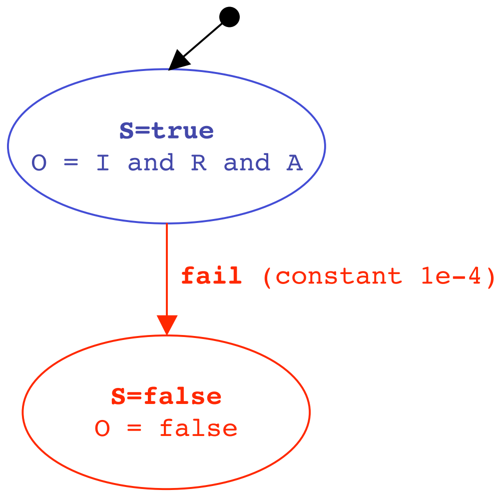
Model based failure propagation analysis: system modelling with AltaRica

- **AltaRica model is a set of interconnected nodes**
- **Node has 3 parts : variable declaration, transitions and assertions**

code | drawing | equivalent automaton

```
Node pipe
 flow I,A,R : bool : in;
 O : bool : out;
 state S : bool;
 event fail;
 trans S=true |- fail -> S := false;
 assert O = I and S and R and A;
 init S := true;
law extern <event fail>=«constant 1e-4»
edon
```





Model based failure propagation analysis: formal requirement modelling

- Formalization of the failure condition using Propositional Logic :
  _ instantaneous view
  3_hyd_loss : (blue_output = no) and (green_output = no) and (yellow_output = no)

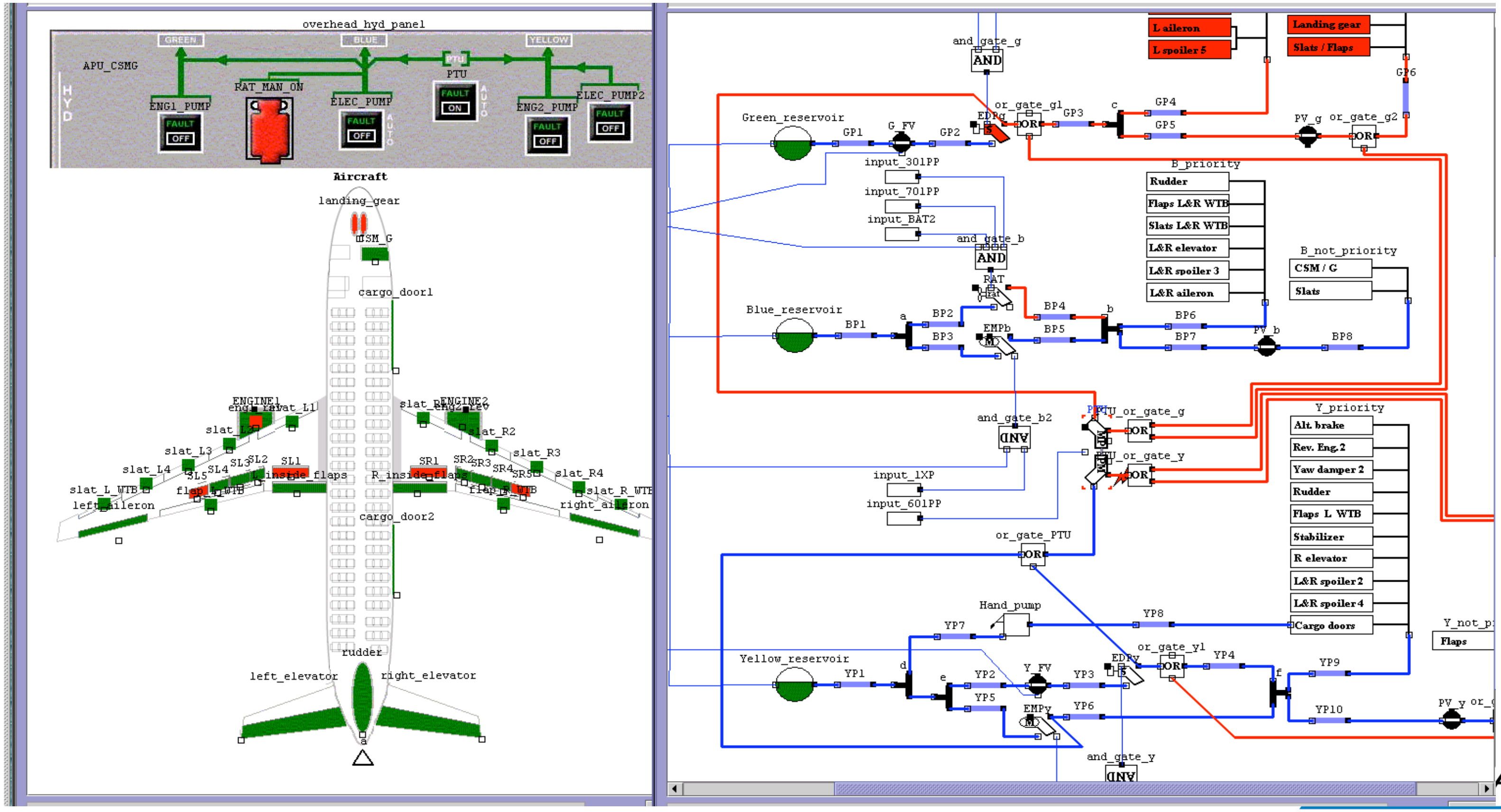
  _ observation of the state of the system at one moment
  _ reconfigurations not taken into account

- Formalization of the requirement using Temporal Logic :
  _ dynamic view
  _ reach permanent loss of hydraulic power :
  Eventually Always 3_hyd_loss

  _ Qualitative requirement to check :
  Always upto_2_failures -> not(Eventually Always 3_hyd_loss)

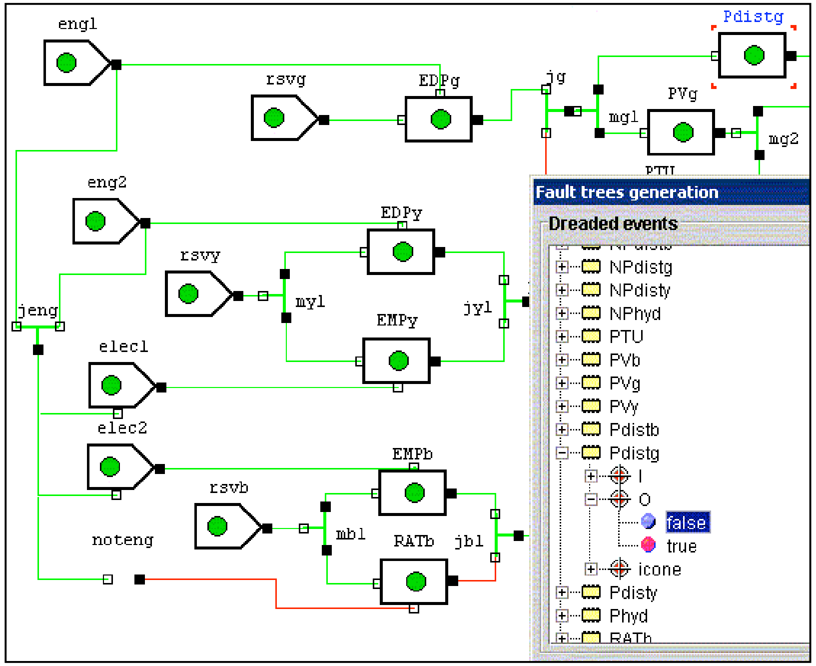
Model based failure propagation analysis: Safety Assessment Techniques

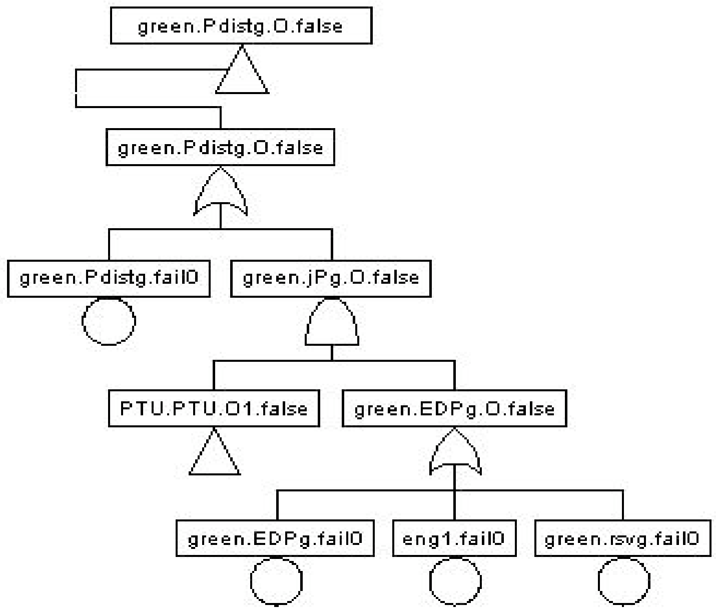
- **Interactive simulation**
  _ observers added into the model to detect requirement violation
  _ play simple combination of failures (in the style of FMEA)



Model based failure propagation analysis: Safety Assessment Techniques

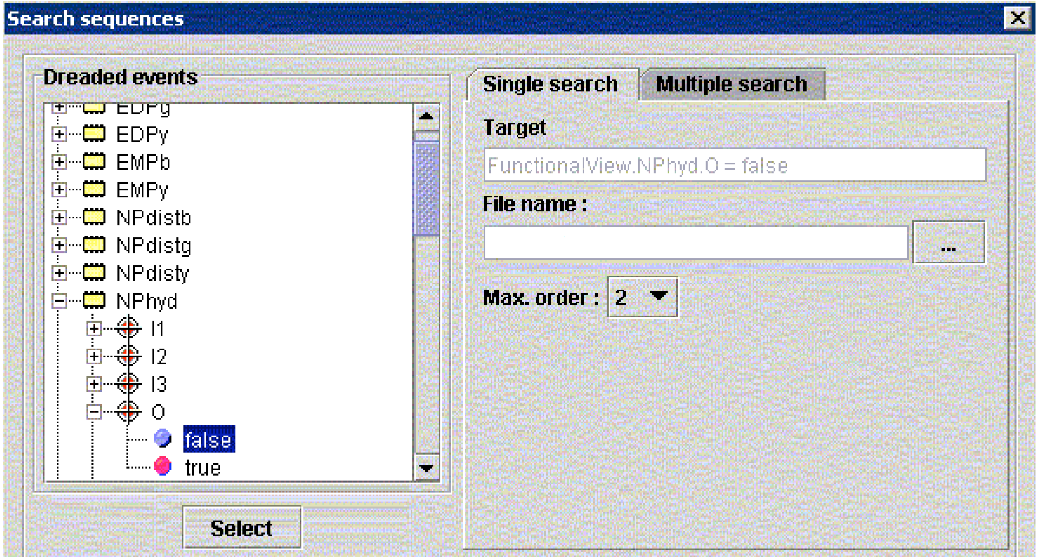
- OCAS Fault-Tree generation
  - The fault tree can be exported to other tools (Simtree, Arbor,...) to compute minimal cut sets and probabilities





Model based failure propagation analysis: Safety Assessment Techniques

- OCAS Sequence Generator
  - Automatic generation of sequence of failure that lead to the violation of Safety Requirements
  - Limit on the number of failures to be considered



Model based failure propagation analysis: Safety Assessment Techniques

Cadence Labs SMV Model-checker

- Translation from Altarica to SMV
- Formalisation of Temporal S/R Requirements in SMV code

```
/* Loss of three electric Systems                                   */
/* ------

/* Two failures ->   DCside1 or DCside2 or DCess_ok                         */

  DCside1_DCside2_DCess_ok : assert G F (elec.el.observer.DCside1_DCside2_DCess_ok);
  using two_failures prove DCside1_DCside2_DCess_ok;

/* Two failures ->   ACside1 or ACside2 or ACess_ok                         */

  ACside1_ACside2_ACess_ok : assert G F (elec.el.observer.ACside1_ACside2_ACess_ok);
  using two_failures prove ACside1_ACside2_ACess_ok;
```

event	ev_el_n1XP_loads_breaker_fail_opened	ev_el_BAT2_fail_short_circuit	ev_update
fail_evt	1	1	0
failures.count	0	1	2
failures.fail_evt	1	1	0

Specificities of robotic architectures

- Robotic architecture consist in
  - Sensor, actuators, controllers, … as traditional embedded systems
  - + a deliberative part to transform high level goals into achievable sequences of basic control actions
- Issue for failure propagation analysis: identify all possible goals and plans used to control the basic devices
- Track of solution:
  1. do not specify the plans at all, the failure propagation analysis will identify the hazardous sequences
  2. check whether the robot architecture enable to filter such sequences
     - A priori: thanks to constraints put in the model used to build the plans
     - A posteriori: by monitoring the plan execution