THALES

Evaluation Altarica / OCAS autour d'une architecture avionique d'un Regional Jet

THALES Avionics - M. MOREL / J.D. CHAUVET

Contents

Assessment of Altarica approach & OCAS tool

- Objectives
- Means
- Modelling subject & overview
- Results
- Synthesis / Further investigations

Objectives

Investigations on the behaviour modelling approach

- Capabilities
  - Early validation
  - Complex system modelling
  - Reusability of Models (objects)
  - Sharing of a graphic safety-oriented representation of a system more user-friendly than FTA
  - Automation of safety tasks / analyses (FTA, FMEA)
- Constraints
  - Modelling of a system and comparison of results with existing PSSA based on classical top-down FTA approach
  - Model complexity versus computation time

Means of investigation

Technical / Human means

- Tool choice : Why OCAS ?
  - Because apparently the most finalized
  - Because interoperable with current Thales Fault-Tree Tool (Aralia Workshop)

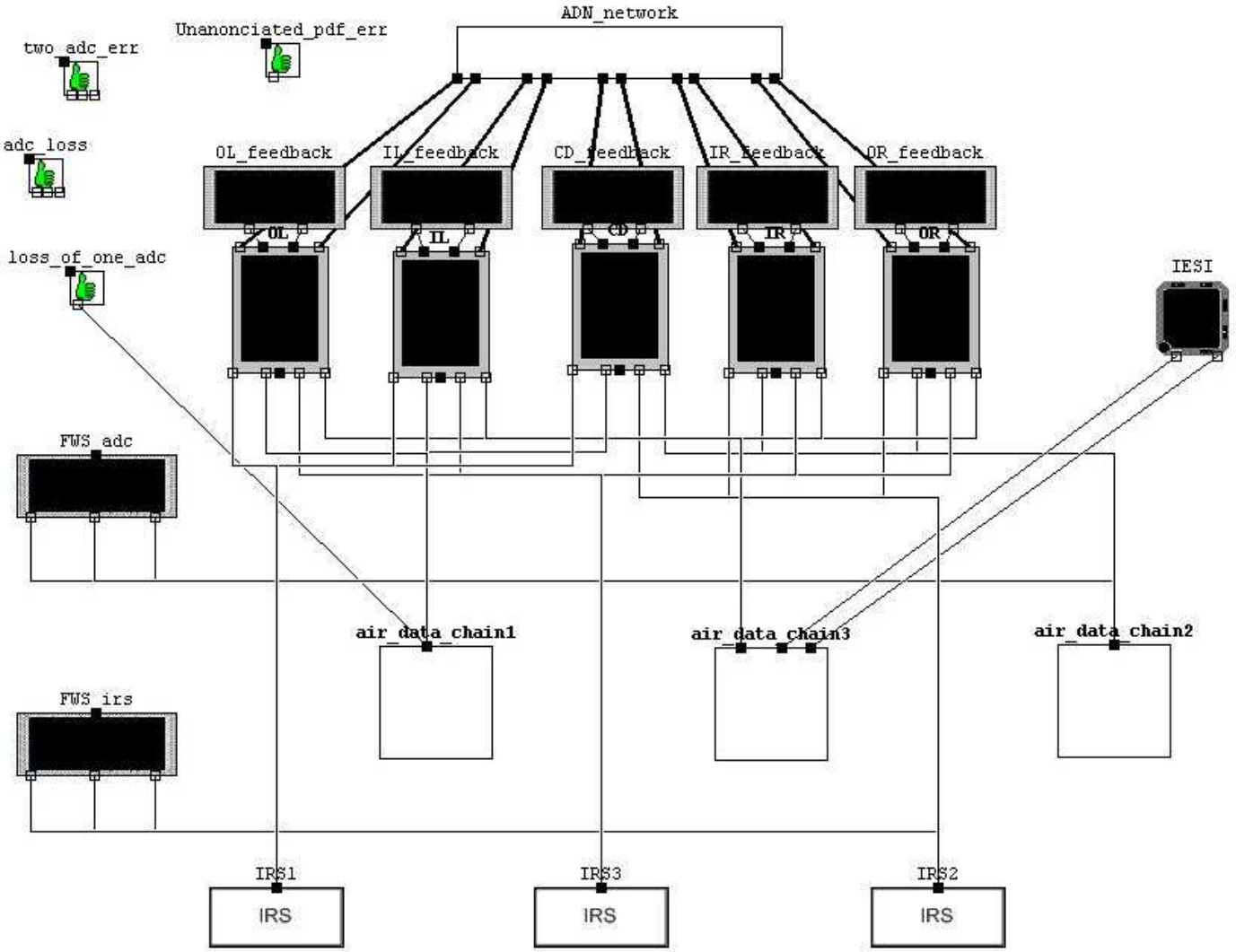
- Human means :
  - one person in training course 6 months
  - 3 persons in close loop mainly with a safety experience (not full time)
  - 4 persons from different horizons (system / component design, ILS, modelling tools, etc.)

Subject of OCAS modelling (1/2)

Modelling of Cockpit Displays and Primary References

- Full knowledge of the subsystems (full support)
- Existing conventional modelling :
  - All safety input data available
    - Equipment FMEA / FMES
    - System FMEA
  - OCAS result may be compared with the FTA
- Dual type of safety objectives (availability / integrity)
  - Undetected erroneous display of air data
  - Loss of display of air data
  - 2 over 3 erroneous air data providing to external systems
- End to end modelling

Cockpit Displays & Primary References



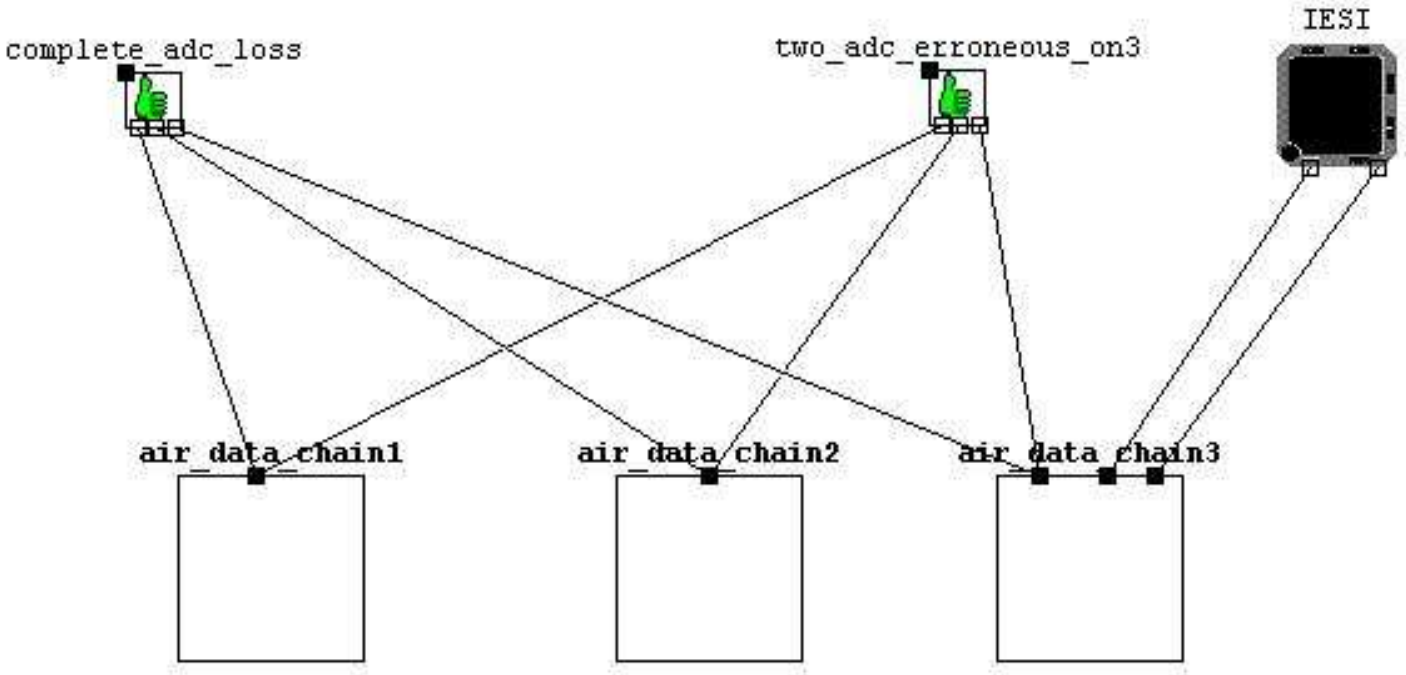
THALES

Subject of OCAS modelling (2/2)

Modelling of Cockpit Displays and Primary References

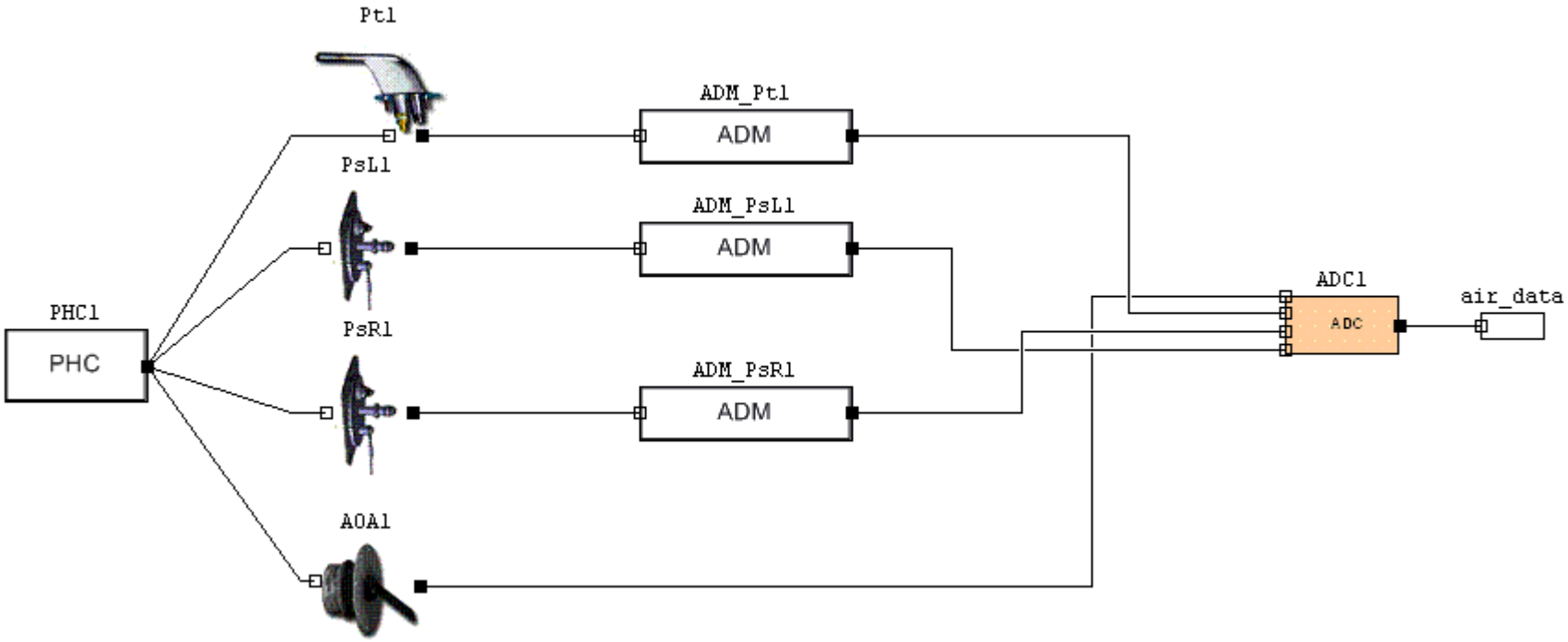
- Mix complexity of the modelling
  - Easy for the primary reference :
    - 3 linear quasi identical chains
  - Complex for the CDS :
    - logic of reconfiguration
    - 3 stages of integrity monitoring : two at equipment level, one at system level (feedback cross-comparison)
- Problematic linked to a common modelling of input and terminal system is tackled
  - Providing of several data which depend on different sensors (speed, altitude, AoA)
  - Adapted monitoring depending on parameters types

Primary References : 3 air data chains



THALES

Air Data Chain



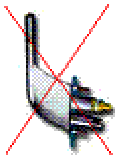
THALES

Formalism of component states

Icons :

- Operative component
  - ex : Pitot probe

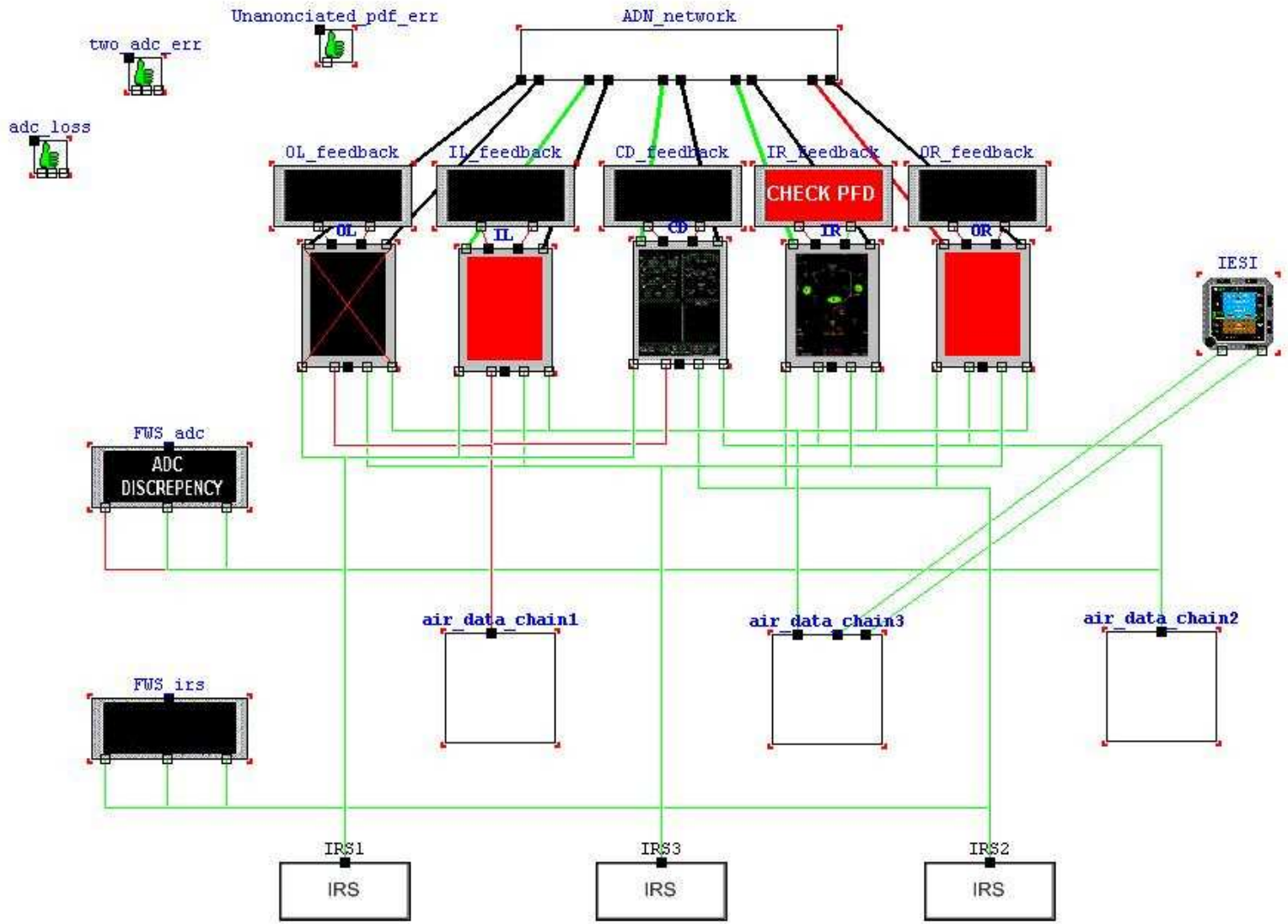
- Faulty component
  - ex : loss of Pitot probe



  - ex : Undetected erroneous functioning of Pitot probe

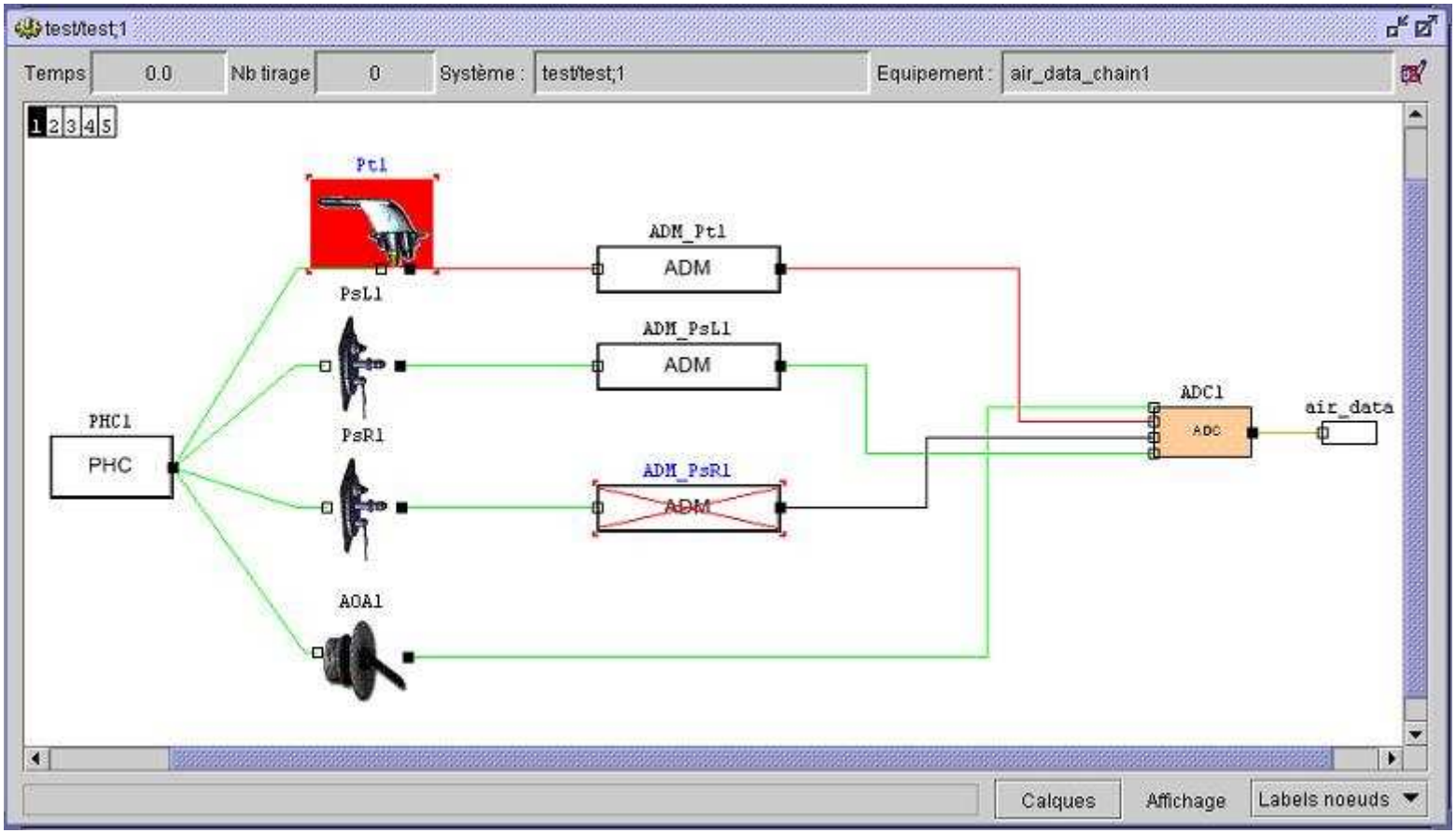
Failures propagation (1/2)

« Air data display » function : impact of failures & monitoring



Failures propagation (2/2)

« Air data chain » : impact of failures & monitoring



THALES

Results

- **Minus :**
  - Use of a preliminary OCAS version
    - Interconnection with Aralia is currently not self evident
    - Plug-ins (model-checkers) are not all DS proprietary
  - Output results generation :
    - FTA generation only possible if model is static (high restriction of the modelling capability : equivalent to FT representation through model)
    - Sequence generation always possible (but problem to sell the “cutsets” without associated FT to our customers)
  - Combinatory explosion
    - Optimisation of the model may request high experience on modelling
    - One way to limit the phenomena : use of attributes ?

- **Plus :**
  - Level of modelling seems adequate with the need of demonstration
  - Reusability of model is easy
  - Preliminary results (early validation) may quickly be obtained

Synthesis / Further investigations

- **Synthesis :**
  - Use of OCAS (dynamic models) for A/C certification ?
  - Deployment within a company requests an important investment (licence price, training, development of an administration tool, etc.)
  - Further investigations requested through a new course training / partial deployment on new program / advance studies (MISSA)

- **Furthers investigations :**
  - Application to Modular Avionic architecture : modelling of functions sharing common hardware resources
  - Time within the demonstration :
    - use of risk time (low reliability systems) & exposure time (dormant failures),
    - functional system behaviour dependent on flight phase (like Auto-Pilot)
  - Generation of System FMEA : complete modelling of a component (not in regard to FHA safety objectives) vs. model complexity
  - Validation of Testability / Diagnostic logics
  - Sharing lesson learnt with other tool users