MISSA Project: focus on Model-based safety assessment for the three stages of refinement of the system development process in ARP4754A

**Airbus:** Matthias Bretschneider, *Chris Papadopoulos*

**Alenia Aeronautica SpA:** Antonella Cavallo

**Cassidian-APSYS:** Jean-Pierre Heckmann, Laurent Sagaspe

**Dassault Aviation:** Valerie Sartor

**Foundation Bruno Kessler:** Marco Bozzano

**ONERA:** Pierre Bieber, Rémi Delmas, *Christel Seguin*

**OFFIS:** Eckard Boede

**Prover Technology AB:** Johann Deneux

**University of York:** Oleg Lisagor

**Thales:** Marion Morel
MISSA project

- More Integrated System Safety Assessment
  - FP7 EU project 2008-2011 project
  - coordinator Airbus

- Scope: safety assessment at complementary design stages
  - From specification of aircraft function
  - To design of aircraft system architecture
  - Until detailed design of systems
MISSA approach:
- Safety assessment based on formal simulation models (cf new ARP 4761)

Talk focus:
- support of:
  - PASA/PSSA
  - Safety requirement allocation
  - SSA
Need: Assess preliminary design against safety requirements

- Ex: A failure condition (FC) severity and derived requirements
  - FC: Unannounced loss of deceleration capability on ground is CAT
  - Quant. Req.: The FC occurrence probability shall be less than 10^-9/F H under hypothesis about system check interval
  - Qual. Req.: No single failure shall lead to the FC
  - DAL Req.: Development Assurance Levels (DAL) of functions/items shall be compliant with ARP4754A rules.
Approach

- **Scope:** Aircraft functions, mono / multi ATA systems
- **Build abstract models of failure propagation in the system**
  - Use automata-like + Boolean modeling languages,
  - Model the dynamic of each system component
  - Connect the component to reflect the system architecture
  - Add observers of system FC
- **Assess the model against safety requirements with available tools**
  - Extract from the models fault trees / cut sets of FC with model dedicated tools
    - => check of Qual. Req and DAL
  - Apply traditional tools to cut sets / tree for quantitative assessment
Experimental feedback

- Need for user's modeling guideline
  - Failure Logic Modeling: close to fault tree style
  - Vs Failure Effect Modeling: close to design model style

- Tools are available
  - Mature enough for 1 ATA assessment
    - e.g. Cecilia OCAS from Dassault Aviation
  - Encouraging results both for
    - models of aircraft functions
    - Multi-ATA models
MISSA integrated case study
### MISSA assessment results

<table>
<thead>
<tr>
<th>System</th>
<th>Organisation Responsible</th>
<th>Model Features</th>
<th>Analysis Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wheel Braking System</td>
<td>Airbus (UK)</td>
<td>FEM</td>
<td>517</td>
</tr>
<tr>
<td>Ground Spoilers &amp; Thrust Reversers</td>
<td>EADS APSYS</td>
<td>FEM</td>
<td>111</td>
</tr>
<tr>
<td>Weight on Wheels</td>
<td>Dassault Aviation</td>
<td>FEM</td>
<td>35</td>
</tr>
<tr>
<td>Integrated Modular Avionics</td>
<td>THALES</td>
<td>FEM/FLM Hybrid</td>
<td>80</td>
</tr>
<tr>
<td>Electrical Power Distribution</td>
<td>Alenia Aeronautica</td>
<td>FEM/FLM Hybrid &amp; ‘pure’ FEM</td>
<td>~30</td>
</tr>
<tr>
<td>Hydraulic Power Distribution</td>
<td>Airbus (Germany)</td>
<td>FEM/FLM Hybrid</td>
<td>78</td>
</tr>
</tbody>
</table>
Need: Assess detailed design against safety requirements and functional safety requirements

Approach
- Use existing design model (e.g. Simulink / Scade models)
- Inject failure modes
- Use previous assessment tools + model checkers

Experimental feedback
- Detailed models are not easily "provable"
  - Hybrid models mixing discrete and continuous time evolution laws
  - Timed models, to reason about system delays
- Tools developed in MISSA
  - Encouraging results: application to toy industrial case studies
Safety requirement management - 1

- Need 1: verify / generate the safety requirements allocation
  - Input =
    - Initial system safety requirements
    - System model or cut sets leading to the system FCs
    - User optimization criteria
  - Output = valid safety requirements applicable to the component of the system
    - failure rates, check interval, FDAL, independence groups

- Approach: two tools solving problems of optimal allocation
  - Opt-Alloc: preliminary design exploration taking into account various user criteria (weight, cost of equipments, ...)
  - DAL-calculator: allocation of average risks and FDAL taking into account standard recommendations
Experimental feedback for DALculator

- From small examples …
  - Performances: DAL, Probability (<1 sec)
    - Data display
    - Nbr of Mincuts: From 11 to 51 (order 3 to 9)
    - Deceleration function
    - Nbr of Mincuts: From 4 to 68 (order 2 to 4)

- … to larger examples
  - Electrical System
    - Nbr of Mincuts: from 300 to 1800 (order 3)
    - Performances: DAL(< 10 sec), Probability (from 5 min to 40 min)
      - MISSA Common Case-Study
        - Nbr of Mincuts: 3000 (order 3)
        - Performances: DAL(< 5 min)
Safety requirement management - 3

- Need 2: reason on "safety contract"
- Approach: tools to assess design following contracts paradigm
  - Assumptions
    - Reflect current degree of knowledge of anticipated design context
    - Determine boundary conditions on actual design context
  - Guarantee
    - Is guaranteed if component is used in assumed design
- Experimental feedback
  - Applied to ARP4754 braking systems
Conclusion

- MISSA provided a comprehensive set of methods and tools to assist
  - Safety requirement management
  - Requirement assessment on formal models
  - At various design stages: from aircraft function to system design
- All proposals have been tested on industrial case studies
  - Good maturity level of PSSA by existing tools
  - More experiments are needed for other promising tools
- For more details http://www.missa-fp7.eu/