MBSA process for airworthiness of aeronautical systems: application to IMA, stakes and benefits
Emmanuel Arbaretier, APSYS, France

GOSNIAS - 3rd International Conference «Integrated Modular Avionics and CNS/ATM.
State and prospects of development»
August 27, 2015 Moscow
1. Model Based Approach

2. Modelling for IMA

3. SIMFIA workbench

4. Model Based Architecture Optimization

5. Conclusion
Classical Approach

Design documents
- System description
- Documents
- Architecture diagram
- …

Understanding of system behaviour

Current process limitations
- Increased complexity of avionic systems
  - Combinatorial explosion in the number of failures
  - leading to a feared situation
  - Complex management of shared resources
  - Ensure held assumptions
  - Safety verification is time consuming
- Difficulty to adapt during the prototyping phase
  - During design phase, safety assessment is performed after each change
- Fault tree size (hundreds pages) unreadable

Conventional avionics
Loss of LRU=loss of a function of one system

Avionics Modules
Loss of LRM=loss of several functions of several systems

Safety analysis results
- Dependence diagram
- Fault tree
Model Based Approach

Design documents
- System description
- Documents
- Architecture diagram
- ...

Understanding of system behaviour

Improvement of safety process

Added value:
- Verification of good understanding
- Hierarchical view
- Common support to share data between design, safety and operational teams.

Formal model

Analysis result Model

Complete list of failures

Exploitation of results

Automatic analysis

Fault tree representation
**Principle:** Incremental development consists in:

1. Developing a platform: the platform is composed of various HW and SW resources + Operating System, embedded in one cabinet. (Nota: a platform may be composed of several cabinets)

2. Individually developing each hosted application in the frame of a usage domain defined in the platform environment

3. Identifying all functional configuration (system integration)

**Advantages:**
- Factorize development efforts of the platform for multiple applications and configurations
- Limit integration / re-qualification efforts for a change of the platform or application
- Propose a standardized framework for multi-supplier development

**Issue:** This concept allows as many different safety configurations as possible combinations of independent resources, what makes safety analysis difficult to achieve, difficult to model.
IMA vs « classical system » safety approach

For 1 system (ARP4754 approach)

Equipment design: FMEA/FMES HW/SW

Integration:
System FMEA/FMES / FTA

ASA Aircraft safety assessment
IMA vs « classical system » safety approach

IMA => multi-resources system

IMA Safety process

* Generic : without system consideration
Top Down Approach for IMA

- Top Level Functions
- System allocation / mapping
- Technological implementation

Different View
MODELLING FOR IMA

SOW → requirements → Top Level Spécification

level 1  
Functional

 Functional Design

level 2  
Physical

 Physical Allocation

level 3  
Technology

 Implementation → Product

SIMFIA model based approach for IMA
Requirement driven Design for IMA

Different levels of abstraction

Service

Level 1

Level 2

Level 3

Level 4

Top level Requirements

Refinement

Models 1

Models 2

Models 3

Models 4

SIMFIA model based approach for IMA
IMA process of Functional Mapping

Step 1: Specification

Step 2: Functional View

Step 3: Physical View

Step 4: Implementation

SOW

requirements

F1

F2

Hard

Soft
Inherent dual point of view for IMA

• Design Tree: dual point of view of Work Breakdown Structure
• Functional / Physical dual mapping
  - Depending on the level of progress of the project
  - Depending on the level of detail in the Work Breakdown Structure
  - Depending on the point of view to be developed:
    - Functional reference,
    - Physical reference.
MBSA with SIMFIA

• **SIMFIA** is a software package which, based on the acquisition of knowledge from the **functional analysis** of the equipment, product, or process, can be used to **analyze and simulate global behavior of a system and automate R.A.M.S.** studies using the principles of Artificial Intelligence.

• SIMFIA, thanks to the integration of **AltaRica Dataflow** language, enables **behavioral modeling** and more **sophisticated computations** based on the Monte Carlo simulation (Stochastic Simulation and generation of sequences).
• SIMFIA software is a structured set of **modules** organized around a kernel constituting the data core of the software.

• SIMFIA use process can be applied to **different areas of activity**.
SIMFIA Architecture

FMECA

- Failure Modes, Effects and Criticality Analysis
- FMECA format customization
- Static/Dynamic FMECA generation

SAFETY

- Cause Tree generation
- Computation (Q, W, $\lambda_{eq}$)
- Failure rates allocation

RELDIAG

- Reliability diagrams
- RAMS computations

SIMUL

- Step by step simulation
- Stochastic computation
- Sequences generations

Model File

Model Validation

- Failure Propagation
- Consistency checks
- Functional analysis
Modelling with SIMFIA

- Modeling process is based on the principle of Structured Analysis methods.
- It is supported by an intuitive graphical interface to build models in a:
  - simple,
  - quick,
  - ergonomic,
  - autonomous way.

![Diagram of input and output with a transformer model]
Model validation

- Any model based demonstration requires absolute confidence in model representativeness.

- SIMFIA integrates the concept of support to **model validation to ensure the robustness of the model** against:
  - System architecture: **Table of functional analysis**
  - Behavior: **Propagation of failure step by step**
  - Modeling process and model updating control: **Model comparison**
SIMFIA Modules

- FMECA Module
- SAFETY Module
- RELDIAG Module
- SIMUL Module
FMECA module

- Specify and define an FMECA format
- Automatically generate a static FMECA
- Automatically generate a dynamic FMECA

<table>
<thead>
<tr>
<th>Failure</th>
<th>Lambda failure</th>
<th>Local effect</th>
<th>Intermediate effect</th>
<th>Final effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batterie:abs</td>
<td>1.0E-6</td>
<td>s:failed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pompe:defaillance pompe</td>
<td>1.0E-6</td>
<td>output_Pompe:failed</td>
<td>S_HP:failed</td>
<td></td>
</tr>
<tr>
<td>Pompe2:defaillance pompe</td>
<td>1.0E-6</td>
<td>s:failed</td>
<td>S_HP:failed</td>
<td></td>
</tr>
<tr>
<td>Switch_alim:abs</td>
<td>1.0E-6</td>
<td>s:failed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch_alim:abs</td>
<td>1.0E-6</td>
<td>s:failed</td>
<td>S_Alim:failed</td>
<td>Extraction_train:failed</td>
</tr>
<tr>
<td>Train_atterrissage:abs</td>
<td>1.0E-6</td>
<td>Extraction_train:failed</td>
<td>Extraction_train:failed</td>
<td>Extraction_train:failed</td>
</tr>
<tr>
<td>Transfo:abs</td>
<td>1.0E-6</td>
<td>s:failed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valve:ftite valve</td>
<td>1.0E-6</td>
<td>output_valve:failed</td>
<td>S_HP:failed</td>
<td></td>
</tr>
<tr>
<td>Valve2:ftite valve</td>
<td>1.0E-6</td>
<td>s:failed</td>
<td>S_HP:failed</td>
<td></td>
</tr>
</tbody>
</table>
SAFETY Module

- Automatically generate Fault Tree related with a dreaded event
- Produce Minimal Cutset List associated with a dreaded event and their contribution
- Compute probability of a dreaded event (Q), its frequency or unconditional intensity (W) and its occurrence rate ($\lambda_{eq}$)
- Compute sensitivity factors
RELDIAG Module

- Generate automatically reliability diagram corresponding to one phase of mission
- Compute RAMS performance indicators on a transient or steady state mode
- Draw time dependent reliability, maintainability or availability curves
SIMUL Module

- Model system dynamic behaviour
- Perform Monte-Carlo simulation
- Generate sequences of events
- Perform step by step simulation
Model processing for IMA in SIMFIA

Model Processing
- consistency check
- completeness check
- scenario simulations

Data / Information / Model Patterns

System Engineering Tool / Workbench Framework

RAMS Information Data Bases

Design Information Repository

Simulation/ Diagnosis
Safety analysis
RAMS analysis
Functional/Hazard analysis

Datasheets for Reports
IMA Project / System Information
- Classification
- DAL
- Localisation
- Equipements types

Model Information
- Equipements, composants, leurs événements
- Code Altarica
- Familles

Results
- Failures ⊂ Cuts ⊂ Observers

Correspond to

Is linked to

SIMFIA model based approach for IMA
<table>
<thead>
<tr>
<th>Failure Condition</th>
<th>Phase</th>
<th>EFFECT OF FAILURE CONDITION ON AIRCRAFT/CREW</th>
<th>Classification</th>
<th>Reference to supporting material</th>
</tr>
</thead>
<tbody>
<tr>
<td>To decelerate the aircraft using the braking system</td>
<td>Unannounced loss of braking system</td>
<td>Crew detects failure when braking is launched. The Crew/Aircraft is in exit ramp phase. Crew ensures some braking via flight controls and/or thrust reversers</td>
<td>CATASTROPHIC</td>
<td>Procedures to prevent loss of normal, emergency or parking mode</td>
</tr>
<tr>
<td>To decelerate the aircraft using the braking system</td>
<td>RTO</td>
<td>Crew detects failure when braking is launched. The Crew/Aircraft is in exit ramp phase. Crew ensures some braking via flight controls and/or thrust reversers</td>
<td>CATASTROPHIC</td>
<td>Procedures to prevent loss of normal, emergency or parking mode</td>
</tr>
<tr>
<td>To decelerate the aircraft using the braking system</td>
<td>Announced loss of braking system</td>
<td>Crew warns their passengers and control tower of the failure. Crew ensures some braking via flight controls and/or thrust reversers. Airport prepares the landing route by using foam to decelerate.</td>
<td>HAZARDOUS</td>
<td>Do this kind of scenario in tests to improve reactivity and minimize this kind of event.</td>
</tr>
</tbody>
</table>

Model 1

Model 2
IMA architecture tradeoff analysis

High level information:
- FC
- DAL etc.

Model 1

Results comparison / Analysis
- Report generation

Results 1

SIMFIA model based approach for IMA

27/08/15
Benefit of MBSA for IMA

- With MBSA approach, you can assess safety performance of an IMA architecture

- A configuration management integrating those models and results can help keeping tracks all along the project

- The ability to keep the information coherent at each level of abstraction (functional, physical, technological) is the key issue for certification
Only MBSE / MBSA approach can manage IMA level of complexity

Multiple Logics of Functional / Physical / Technological IMA Mapping Systems can only be encompassed and mastered through MBSE / MBSA approach

All design opportunities offered by IMA can be assessed in the framework of MBSA techniques and methods

SIMFIA is a rather complete MBSA environment for IMA design because it is open to all computing processes required by Safety Analysis and Airworthiness report production
The software
simLog & simFia

They trust us

AIRBUS DEFENCE & SPACE
AIRBUS HELICOPTERS
DASSAULT AVIATION
cnes
DCNS
Rolls-Royce
SAFRAN AEROSPACE · DEFENCE · SECURITY
THALES
BAE SYSTEMS
cea
EDF
PSA PEUGEOT CITROËN
SNCF
GDF SUEZ
Alcatel-Lucent
RATP
VINCI ENERGIES
Schneider Electric
MBDA
ZODIAC AEROSPACE
NEXTER SYSTEMS
DGA
ACTIA SODIELEC
Thank you for your attention!

Emmanuel Arbaretier : Head of Software tool department  
emmanuel.arbaretier@apsys.eads.net

Michel Oberlé : Export Director  
michel.oberle@apsys.eads.net

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.