System safety assessment based on formal models

Lessons learnt by Alenia Aeronautica

Presented by Antonella Cavallo
Toulouse, 9th February 2010
• Introduction
• Safety assessment based on formal models
  – Premise
  – Models developed by safety engineer
    • Verification of architectural alternatives
    • Incremental modeling and assessment
  – Models developed by design engineer
• Method extended to cover other safety related aspects
  – Premise
  – Mission Analysis
• Conclusion
Introduction

• The issues presented in the following derive from the experience matured in the following research projects:
  – ESACS (Enhanced Safety Assessment for Complex Systems, FP5)
  – ISAAC (Improvement of Safety Activities on Aeronautical Complex Systems, FP6)
  – MISSA (More Integrated Systems and Safety Assessment, FP7)

• The results of the experience will be presented in terms of:
  – Examples of systems types considered
  – Approach followed for modelling and analysis
  – Considerations

• Two main tools chains were used for formal modelling and analysis:
  – OCAS (Dassault tool)
  – STATEMATE (IBM tool) including STSA (OFFIS STatemate Safety Analysis module)

• Other tools used:
  – COMPARE tool by FBK
  – Fault Tree Plus tool by Isograph
Safety assessment based on formal models

- Premise

- Models developed by safety engineer
  - Verification of architecture alternatives
  - Incremental modeling and assessment

- Models developed by design engineer
• The safety process is parallel to the design development (ref. to ARP 4754)
• The assessment is performed at major stages of the development that are related to different levels of detail
• An approach based on “formal” system models and verification techniques is used for the assessment (to find paths leading to violation of safety requirements)

• Two main kinds of models are considered:
  – models developed by safety engineer
  – models developed by design engineer
Safety Analysis

Failure modes:
- Stuck-at Failure
- Random Failure
- User-defined Failure
- Delay Failure
- Ramp-down Failure
- Noise-Failure

SR1: Utilities to not go under the 20% in case a PTO failure occurs

Requirement

Simulation trace
• The safety engineer builds models at different stages:
  – in the initial development stage, architecture models that may be used to verify design alternatives
  – in the following stages, incremental models i.e. including new components, more failure modes, more detailed behaviour used to verify compliance with safety requirements
The experience presented in the following is relevant to an Electrical system of an Airbus A/C developed by OCAS tool.

Purpose of the case study:
- to apply the model-based approach to safety analysis for proposing some changes in an existing model architecture and verifying them
- this to “reproduce” what could be a real process when a first architecture is analysed, a suggestion for safety improvement is done and its benefit is verified.
Model

- A previous model developed by ONERA is the basis of the job.
- This “Reconfiguration Model” describes the behaviour of the Electrical system components and contains a reconfiguration logic implemented by opening or closing various switches. The failure mode (FM) taken into account is the loss of voltage. (Short circuit is not considered).
- The model uses a library of components.
- There are three inputs: two engine status and one hydraulic line status, and six outputs relevant to the status of provision of voltage of three DC and AC bus bars.
• At System Level, the modified Reconfiguration Model has four inputs, instead of three, that are: two engine status, one hydraulic line status and one APU status.

• The six outputs relevant to the status of provision of voltage of three DC and AC bus bars remain the same of the original model.

New Input: APU Power Supply
The introduction of an additional generator (the APU generator) has needed the addition of other new components (the APU contactor, a joint connector).

Moreover, the logic of the AC, DC and Generator Controllers was modified in order the logic takes into account the presence of a third generator.
Physical Layer

New Components Instances
Physical & Controller Layers

Modified Controllers Components
Analyses

• The Minimal Cut Sets have been generated for the following 12 Failure Conditions (FC):
  
  – 6 “Minor” FC relevant to the loss of voltage of one bus bar (AC1, AC2, AC_ESS, DC1, DC2, DC_ESS)

  – 4 “Major” FC relevant to the loss of voltage of two bus bar, that are: loss of two AC, loss of two DC, loss of AC1 and AC2, loss of DC1 and DC2

  – 2 “Catastrophic” FC relevant to loss of three bus bars, that are: total loss of AC bus bars and total loss of DC bus bars.
Analyses & results

Failure Conditions: loss of...

**Original Reconfiguration Model**

<table>
<thead>
<tr>
<th></th>
<th>AC 1</th>
<th>AC 2</th>
<th>AC ESS</th>
<th>AC Double</th>
<th>AC Total</th>
<th>AC1 &amp; AC2</th>
<th>DC 1</th>
<th>DC 2</th>
<th>DC ESS</th>
<th>DC Double</th>
<th>DC Total</th>
<th>DC1 &amp; DC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>single</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>double</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>6</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>triple</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>18</td>
<td>18</td>
<td>24</td>
<td>21</td>
<td>34</td>
<td>25</td>
</tr>
</tbody>
</table>

**Modified Reconfiguration Model**

<table>
<thead>
<tr>
<th></th>
<th>AC 1</th>
<th>AC 2</th>
<th>AC ESS</th>
<th>AC Double</th>
<th>AC Total</th>
<th>AC1 &amp; AC2</th>
<th>DC 1</th>
<th>DC 2</th>
<th>DC ESS</th>
<th>DC Double</th>
<th>DC Total</th>
<th>DC1 &amp; DC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>single</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>double</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>triple</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>16</td>
<td>16</td>
<td>18</td>
<td>18</td>
<td>27</td>
<td>22</td>
</tr>
</tbody>
</table>

The introduction of an additional power source (APU) improves all the minimal sequences leading to the considered Failure Conditions, i.e. decreasing the minimal cut set (MCS) order.
Considerations

- The OCAS tool allows easily modifying a given architecture thanks to a modular approach based on components library.
- The Sequences Generation for architectural models (only boolean variables without a complex dynamic) is very fast.
- The previous characteristics allow to quickly test changes in a given safety architecture e.g. in order to find the best compromise between system’s safety, design and cost.
- The model-based approach to safety analysis can be a valuable support in the process, especially in the architectural phases.
• The experience presented in the following is relevant to an Electrical system of an Alenia Aeronautica A/C developed by STATEMATE tool chain.

• Purpose of the case study:
  – incremental modeling and assessment
  – monitoring of analysis complexity issues and identification of remedy
  – verification of models using compositional analysis
Models

- The Electrical System of an Alenia aircraft is the basis of the job (2 Generators and 1 APU; AC, DC, emergency bus bars; Controllers managing the reconfiguration logic)
- The scheme considered is showed below
• An incremental approach is undertaken with production of models with increasing complexity (addition of failure modes, system components and behaviours)

• Only simple variables (e.g. boolean)

• User defined failure modes

• Schematic way for system components behaviour (GOOD and LOST charts)
Failure mode variable
Electrical system of an Alenia A/C

- Models typologies (with incremental complexity):
  
  a) Basic reconfiguration logic. No FMs on Controllers, no FMs and behaviour for short circuit
  b) Addition of FMs on controllers relevant to the system behaviour without short circuit
  c) Addition of FMs, system components and behaviour for short circuit (this kind of models are interesting for “failure propagation”)
Analyses

- Failure Conditions as “total loss of AC” and “total loss of DC” where considered.
- Compatibility proofs were performed between models of increasing complexity. The COMPARE tool was used (*).
- COMPARE tool was also used to identify new cut-sets from a model of an higher level of complexity (model “x+1”) in respect to a low level model (model “x”).
- A scenario for “composition” was developed. A proof on a FC was logically decomposed into several sub-proofs. The results (cut-sets) of the sub-proofs performed with the OFFIS tool were added to the leaves of a tree that represents the global FC (built by Fault Tree Plus tool). The cut-sets of the “composed” tree were compared with the results of the complete proof of the global FC performed with the OFFIS tool.

(*) COMPARE tool: allows the comparison of two sets of MCS finding the differences
Results

- Models with higher level of complexity can not be examined globally in a proof. For this reason the analyses have to be performed on subsets of Failure Modes
- Where possible, results were compared with those of traditional analysis and they match
- Comparations using COMPARE tool provided positive results
- The composition scenario provided consistent results
Considerations

- Higher level models (with short circuits) allowed to evidence some complexity points that make difficult the analysis: e.g. “loops”, “reverse flows” from the bus bar that experienced the short circuit towards the power source, presence of “timing” issues. These are tool independent problems that need to be investigated.
- Incremental modeling promises to be a valuable approach to safety analysis in a real process.
- “Comparation” of different sets of results is useful.
- For large or complex models “composition” could be an help to conduct the analysis and to can find results that can not be obtained with “global model” analysis. Nevertheless it has to be evidenced that not always it is easy to build a logical tree that is comprehensive of all possible cases. The methodological investigation has to be further developed.
• The design engineer builds models that usually:
  – contain high level of detail
  – contain maths functions
  – use almost all the features of the modeling tools
Models developed by design engineer

• The experience was based on the use of design models in STATEMATE

• Two kinds of systems models were considered:
  – “logic” models mainly aimed to interlock functions management
  – models including continuous “math” functions aimed to perform specific mathematical computation
Models developed by design engineer

- Models demonstrated to be too complex to be analysed by means of verification techniques
- For this reason, the models needed some adaptation/simplifications, e.g.:
  - reduction of the number of activities, states and variables. This means to identify the functions “safety relevant” and export them in a new model that will be specifically used for formal verification and safety analysis
  - simplification of the structured data items, when possible
  - rescaling of long timers
  - reduction of variable range/resolution
  - simplification of math computations
Models developed by design engineer

Considerations

- design models, being constructed to verify the system real behaviour and performance, are too complex for safety verification
- in order to be considered for the safety assessment model-based approach they need to be re-arranged (simplified, abstracted from details, split into sub-parts whose results need to be composed, etc.)
- this activity is costly
- in conclusion, design models seem to be more adapt to be studied by means of “what-if simulation”
- models built by safety engineers, even if detailed, seem to be preferable for safety analysis purpose
Method extended to cover other safety related aspects

- Premise
- Mission Analysis
• Model-based approach can be also used to study other safety related aspects, like e.g.:
  – operational aspects: e.g. to answer to the question “is it possible to continue the planned mission in a failed configuration or to revert to another mission profile?” (Mission Analysis)
  – testability aspects: e.g. to answer to the question “is it possible for a fault to occur undetected?” (Fault Detection Analysis), “for a warning message, which are the faults that raise it” (Fault Isolation and False Alarms Analysis)
  – crew interface related aspects: e.g. to answer to the question “will an erroneous procedure lead to a safety critical situation?” (Human Errors Analysis)

• In this perspective, it is necessary to introduce in the model other “items” in addition to the system components, like e.g.:
  – mission profiles and requirements for mission phases
  – failure detection components and messages management functions
  – interface components and pilot procedures
Mission Analysis

- The experience was performed on a “Secondary power system” that has the function to drive the A/C utilities (electrical and hydraulic) taking the power from the engines

- The tool used was STATEMATE
Mission Analysis

Models and analyses

Type A (used when considering only some behaviour for some mission phases):

- A new chart “Mission Manager” was added in order to describe the mission profile
- Observables were defined in order to observe when (mission phase) the FMs occur and lead to a mission unsuccess defined by means of requirement
- These observables are used by the verification - analysis tool (STSA) in order to construct the Mission Fault Tree by grouping the cut-sets depending on when the failures occurred.

Type B (used when considering all system behaviours in all mission phases):

- Other charts were added, in respect to type “A”: “Frame Controller” and “Fault Manager”
- The new frame was used to conduct simulation tasks where several missions are simulated (managed by the “Frame Controller”) in which failures are injected (by the “Fault Manager”). The output in this case “B” is a file containing information about the missions runs.
Mission Analysis

Planned Mission

M0 starts

Mission branches

@Fault_Manager

@Frame_ctrl

Number of missions = 1000
Number of failed missions = 2
Number of reverted (limited) missions = 1

Mission n. Failed mission time Phase
19 59 3

...
Considerations

- Model-based approach can be also used to study other safety related aspects
- Guided-simulation techniques can be useful to investigate the system in case of complexity. In the mentioned case the complexity was due to the presence of several behaviours corresponding to several mission phases.
Conclusion (general)

- The model-based approach to safety analysis can be a valuable support in the process. The possibility to have a system model that can be simulated and verified facilitates the discussion and interaction with the design engineers with the target to early detect the system weak points.

- A modular approach based on components library allows to quickly test changes in a given safety architecture e.g. in order to find the best compromise between system’s safety, design and cost.

- Incremental modeling is useful to follow the evolution of the system design and perform assessment at the various stages.

- For the purpose of safety verification, models built by safety engineers seem to be preferable in respect to the models of the design. The abstraction from details, reduces the complexity, therefore facilitates the analysis task.

- Design models seems to be more adapt to be studied by means of “what-if simulation” and are useful to make a comparison and maintain traceability with safety models.

- Model-based approach can be also used to study other safety related aspects, like e.g. operational aspects, testability aspects, crew interface related aspects. In this perspective, it is necessary to introduce in the model other “items” in addition to the system components.
• The fundamental point in a model based approach to safety assessment is to identify the adequate level of detail of the model, ie. to determine the best compromise between model complexity (related to task analysis complexity) and the possibility to obtain useful and significant results for the purpose of safety properties verification.

• There is the need to investigate means to address issues related to model complexity. Composition and guided-simulation techniques could be considered to this purpose.