Model Based Risk Assessment of Procedures and Systems for Aircraft Trajectory Management

Lucia Sanz, Andra Tonie, Christel Seguin, Rémi Delmas, Pierre Bieber, Patrick Fabiani

Model Based Risk Assessment of Procedures and Systems for Aircraft Trajectory Management

Lucia Sanz, Andra Tonie,
ISAE
Toulouse, France
Lucia.SANZ-SANCHEZ-INFANTE@etu.isae.fr
Andra-teodora.TONIE@etu.isae.fr

Christel Seguin, Rémi Delmas,
Pierre Bieber, Patrick Fabiani
ONERA
Toulouse, France
name@onera.fr

***Abstract*— Modern Air Traffic Management (ATM) concepts of operation require a strong interaction between agents such as human operators (pilots, air traffic controllers) and information technology systems (either on-ground or on-board). Although risks shall jointly be managed by all these agents, current risk assessment techniques are usually dedicated to only one class of agents (either human operators or IT systems). This paper addresses this issue. It proposes to extend Model Based Safety Assessment (MBSA) techniques originally developed to assess complex systems. This MBSA extension enables to assess how risk can be jointly managed by procedures and systems. The paper shows the methodology used and it presents lessons learnt from an aircraft trajectory management case study.**

Keywords— Safety assessment; Air Traffic Management;

I. INTRODUCTION

Modern Air Traffic Management (ATM) concepts of operation such as the one developed within the SESAR programme [4] require a strong interaction between agents such as human operators (pilots, air traffic controllers) and information technology systems (either on-ground or on-board).

Although risks shall jointly be managed by all these agents, current risk assessment techniques are usually dedicated to only one class of agents (either human operators or IT systems).

This paper addresses this issue. It proposes to extend Model Based Safety Assessment (MBSA) techniques originally developed to assess complex systems. This MBSA extension enables to assess how risk can be jointly managed by procedures and systems.

The paper shows the methodology used and it presents lessons learnt from an aircraft trajectory management case study.

II. TRAJECTORY MANAGEMENT

The management rules of aircraft trajectories are specified in ICAO's *Annex 2 – Rules of the Air* [1]. We focus on the collision avoidance procedure applicable in the following case. Collision avoidance involves two aircrafts: one aircraft and another one that we will call the intruder aircraft. Both are in cruise phase and are converging approximately at the same flight level. The aircraft is flying in one sector, and it is flying in radar controlled airspace in instrumental flight conditions.

According to ICAO specifications, the main actors of the Trajectory Management system of this scenario are :

- *Pilot:* In clear airspace the pilot can visually detect the appearance of an intruder; if this happens, the pilot shall ask the ATC for a route change.
- *Air Traffic Controller(ATC)*: If the airspace is not clear, or due to workload, the pilot cannot visually detect the intruder then the ATC in charge of that airspace sector shall inform the pilot and assist him during all the avoidance operation. The controller has access to some control panels where the radar tracking (ATCRBS – ATC Radar Beacon System) can be visualized, as well as VHF radios for oral communications and ADS (Automatic Dependent Surveillance) data-link communications.
- *Traffic Collision Avoidance System (TCAS)* [6]: If both the pilot and the ATC fail in a prompt detection of the intruder, the TCAS equipment shall first announce the appearance of the intruder. It shall also provide the pilot with traffic advisories (TA) and resolution advisories (RA) depending of the distance between the two aircraft. When the RA is issued, the controller is no longer responsible for the separation of the aircraft until the conflict is terminated.

Experience returns have proven the robustness of this procedure. However, incidents highlighted also its limits especially when equipment failures are combined with human inadequate performances. So we propose to conduct an integrated safety assessment of all the actors (human and equipments) to deal with such issues.

III. PROPOSED SAFETY ASSESSMENT PROCESS

The goal of safety assessment is to determine that every possible hazards (failure conditions) of a system were considered and that they were properly addressed. The first

step of the safety assessment is the identification of failure conditions of interest and their classification according to their severity (ranging from Minor to Catastrophic). In this paper we focus on one catastrophic failure condition: aircraft collision due to total loss of conflict detection means. Quantitative and qualitative safety requirements are associated with the failure condition. For a Catastrophic failure condition, we consider the following qualitative requirement: "*no combination of strictly less than 3 failures shall lead to the failure condition*".

The system safety assessment examines the proposed architecture to determine how failures can cause the identified failure conditions. This assessment aims at showing that the qualitative and quantitative requirements are satisfied. Moreover, in case of aircraft systems, this assessment also establishes new safety requirements such as requested independence between component failures and requested minimal Development Assurance Level (DAL). We propose to apply the same principles to all the actors of the trajectory management systems.

We have used two different tools to assess the safety of the trajectory management:

- Cecilia-OCAS workbench from *Dassault Aviation* was used to model in AltaRica [9] trajectory management and to study sequences of events leading to the catastrophic failure condition.
- DALculator tool [8] was used to generate independence, resource allocation and DAL requirements.

Usually these tools are used to model and analyse technical systems [7] and not human actors such as the aircraft crew or the air traffic controllers. The functioning modes of the technical systems of our simplified case study are modelled by a boolean variable *ok* that is true when the system is working correctly and its results are reliable and false otherwise. We have extended the modelling approach to deal with human actor failures. Since in trajectory management the main role of human actors is to detect the intruder aircraft we have introduced modes that degrade their capability to correctly detect the intruder

- in mode *ok*, the actor correctly detects the intruder.
- in mode *positive,* the actor always believes that there is an intruder, even if there is not.
- in mode *negative ,* the actor always believes there is not an intruder, even when there is.
- in mode *lost,* the actor believes are undefined

The model describes all the actors of the trajectory management scenario and their interaction. The model also includes an aircraft node that observes all the actions that could take place and lead to a collision. This node is used to generate automatically the sequences of failure events that lead to a collision.

IV. RESULTS OF THE RISK ASSESSMENT

To analyse the model, we first used the *Sequence Generation* of the Cecilia tool. We found 34 sequences of events leading to the total loss on the conflict detection means. We used these sequences in the following ways.

First, these sequences were used to check qualitative requirements. Two sequences of size equal to 2 contradict the qualitative requirements:
{copilot_detection.fail_loss, pilot_detection.fail_loss},
{ ACFT.TCAS_fail, ATC_detection.fail_negative}
However, the tolerance to two faults is a requirement justified by good practices of technical system design. Here, only the behaviour of the pilot, the co-pilot and controller play an important role that leads to a collision risk in these sequences. Indeed, only "single fault tolerance" is mandatory for the whole aircraft operation. Moreover, if fault tolerance issues can be solved by adding redundant equipments in the aircraft or in ground ATC station, we cannot easily have three pilots on board or two controllers working in the same stand. In conclusion, we made an exception and continued the analysis.

Then the sequences were used to generate independence requirements. The rationale is the following. If we want to ensure that no single/double failure leads to a catastrophic failure, we shall also require that events which occur in sequences of size 2/3 are independent two by two. In our model, there are several sequences of order 3. According to this, their segregation was not studied by hand but with the help of the tool DALculator.

DALculator proposed to require the independency of the items given in the table below. Independency implementation requires diversification of components. The table discusses also the diversification issues in our study case.

Independent components	**Why can they be independent?**
pilot_detection copilot_detection	Commonly is said that "there are not two people alike". Pilot and co-pilot are independent because their decisions come from their inner professional criteria.
ATC_detection TCAS	The most obvious of the independences is between the different technologies human and systems are made of.
processing_equipment_1 processing_equipment_2	The independence between these two items may be the most difficult to achieve, two processing equipment with different software are needed.
processing_equipment_3 TCAS	As these two components have very different functions, they do not share common software computation.
signal_comparator_1	Idem to the explanation above

TCAS	for the processing equipment and the TCAS.

Table 1. Item Development Independence.

Independency implementation also requires installing the items in different zones. DALculator tool also established the minimum physical zones where the components can be located. In our case at least two zones per group of components is needed:

- *Crew on board*: pilot and co-pilot have different positions in the cockpit, with independent displays and flight controls; however it is impossible to place them in different zones of the aircraft, both of them need to be in the cockpit. Once again in this paper, we can highlight the differences between systems and humans. While a leakage of a pipe ("system_failure") can lead to a catastrophic failure if it is over navigation wires; if the pilot cries ("pilot_belief=undefined"), the co-pilot will not be affected ("copilot_belief=ok"), maybe distracted and stressed, but capable to do his functions.
- *Controllers on ground*: Their allocation behaviour is similar to the pilot and co-pilot situation. Various controllers share air traffic control centre but have separate stands, equipment and moods.
- *Systems on board*: In this case study we only considered as on board equipment the TCAS and the VHF components. The results from the DALculator mean that the TCAS has to be allocated in a different place than the processing equipment and the signal comparators of the ATC radar. This is accomplished by the fact that all these components are on ground while the aircraft is cruising. According to the VHF system, results about the on board radio are not found with DALculator because they do not even appear in the Minimal Cut Sets done for order 6 with Cecilia tool, which means that these components are not critical and their malfunction does not lead to a real collision risk.
- *Systems on ground*: we considered two big groups of systems: controller VHF radio and controller radar. Neither the controller's radio nor some sub-systems of the radar (ATCBRS transponders and control panel displays) affect catastrophically in the scenario presented; but for the other radar's sub-systems: one of the processing equipment shall be mounted apart from the others. The signal comparators can be in the same zone, as their function is just check the processing equipment results.

Finally, after identifying feasible independence requirements, we used the generated sequences to perform the DAL allocation with the DALculator.

The Development Assurance Level (DAL) classifies the level of development of the equipment in order to prevent or eliminate design errors with more or less care. Depending of the level of severity of the failure conditions, a different DAL will be required. As we are working with a model for catastrophic failure, the overall conflict detection function shall have a functional DAL (F-DAL) A. However, the DAL of the system items (I-DAL) can be lower. New DAL allocation rules introduced in *ARP4754A* allow downgrading some components that appear in the minimal cut sets. This downgrade is possible for independent components and considering that the local degradation of the DAL will not lead to a safety problem. The interest of downgrading some of the components is due to the inverse relation between severity level and development costs: as higher is the severity level, higher is the cost; so with the DAL study the purpose is to have a trade-off between these two agents.

With DALculator the downgrade DAL can be obtained following two different approaches, both certified by international Authorities, so both valid. The final election between which one to choose will be made in order to optimize the development costs while preserving the feasibility. For instance, some too complex software cannot be currently certified at level A.

Several allocations have been generated. A first DAL allocation was computed by selecting "Option 1" solver and constraining the TCAS to a DAL equal to C (its current usual DAL). This makes some other components to become class A. In particular for the co-pilot and the controller what this solution means is that, they have to be very reliable, so when they are needed, they are fully capable to avoid the intruder. The dependability on them also concerns their availability and continuity at work. In terms of safety, it is not interesting to workload the crew; however there is a positive point, there is not an increment of the development cost. .

A second proposed "Option 1" allocation sets TCAS to DAL A. In this case, most of the components can be downgraded to DAL C. We also can observe that the crew on board and the controllers on ground are less needed, as they dependability decreases. Only the co-pilot has DAL A classification, he/she represents the last chance for visual detection.

The tool shown also that "Option 2" is not feasible when TCAS DAL=C. "Option 2" when TCAS DAL=A is feasible. There is only one item with DAL A, the controller, as it is a human resource he/she is not an additional cost.

Finally we did also the analysis for the combination of the two options and with the TCAS set to A. We got the following results:

DAL	**Component**
A	TCAS
B	pilot_detection
	copilot_detection
C	ATC_detection
	coATC_detection
	processing_equipment_1

processing_equipment_2
processing_equipment_3
signal_comparator_1
signal_ comparator_2

D The remaining components of the system.

This last result seems optimal. However, it requires developing TCAS at DAL A..

V. LESSONS LEARNT

One challenges of this work was to model the faulty behaviour of human actors and their interactions with the systems. We modelled the scenario for collision avoidance established by ICAO's *Rules of the Air* in the AltaRica language. Another issue was to also to define requirements applicable to all actors of the system. We proposed to apply the approach defined for complex aircraft systems in ARP 4754 and we discussed the interpretation of fault tolerance, independence and DAL requirements in the integrated analysis.

The safety analysis allowed determining the principal differences between the components and the human actors involved in the collision avoidance procedure. These differences are:

- *Redundancy*: In order to make more robust the procedure, we can have redundant equipment, but we cannot have a higher crew redundancy. We have to trust that the only two available pilots and the controller are able to do their work correctly.
- *Independence*: The independence for components and human actors was studied with the same tool (DALculator), but the results have to be interpreted differently. Independence between two components means to have different development technologies between them to assure that the output data is reliable. While, independence between members of the crew is assured because it is intrinsic to human's nature.
- *Zonal allocation*: To determine the relative physical allocation of the items we also used DALculator tool. The allocation constraints are essential to place correctly the redundant and independent equipment; in order to avoid that a single failure is transmitted to other essential equipment for the avoidance.
- *DAL allocation*. Currently highly qualified human actors are requested to recover lower DAL of TCAS. If TCAS can be qualified at a higher level, the balance could be fruitfully re-equilibrated.

Finally, it can be considered that this study – that models the nowadays collision avoidance procedure – propose a framework which can be applied for the analysis of the next concept for collision avoiding, defined by the SESAR programme.

REFERENCES

[1] ICAO Annex 2 – Rules of the Air, July 2005

[2] SAE ARP4761 – Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment December 1996

[3] EUROCAE, ARP4754 – Certification considerations for highly-integrated or complex aircraft systems, November 1996

[4] SESAR, http://www.sesarju.eu

[5] RTCA, Minimum Operational Performance Standards for Air Traffic Control Radar Beacon System (ATCRBS) Airborne Equipment, 2008

[6] FAA Introduction to TCAS II Version 7, November 2000

[7] P. Bieber and C. Seguin,Safety Analysis of the Systems Embedded with AltaRica. In "Industrial Use of Formal Methods: Formal Verification", J.-L. Boulanger Editor, Wiley, April 2013

[8] P. Bieber, R. Delmas and C. Seguin, DALculus – Theory and Tool for Development Assurance Level Allocation in Safecomp proceedings, 2011

[9] Arnold-al , The AltaRica Formalism for Describing Concurrent Systems, 2000

[10] L. Sanz, A. Tonie, Safety Assessment of the SESAR management of the aircraft trajectories, ISAE M. Sc. Thesis, June 2013