



HAL
open science

AIRCRAFT SAFETY MODEL DEVELOPMENT AND INTEGRATION IN A RISK OBSERVATORY

Pierre Bieber, Sylvain Metge, Marion Morel, Julien Ple

► **To cite this version:**

Pierre Bieber, Sylvain Metge, Marion Morel, Julien Ple. AIRCRAFT SAFETY MODEL DEVELOPMENT AND INTEGRATION IN A RISK OBSERVATORY. EASN International Conference on Innovation in European Aeronautics Research, Sep 2017, Varsovie, Poland. hal-02078264

HAL Id: hal-02078264

<https://hal.science/hal-02078264>

Submitted on 10 Apr 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

AIRCRAFT SAFETY MODEL DEVELOPMENT AND INTEGRATION IN A RISK OBSERVATORY

PIERRE BIEBER

*ONERA, 2, avenue E. Belin
Toulouse, 31055 France
Pierre.Bieber@onera.fr*

SYLVAIN METGE

*AIRBUS Operations S.A.S., 316 route de Bayonne
Toulouse, 31060 France
Sylvain.Metge@airbus.com*

MARION MOREL

*Thales Avionics, 105 avenue Gen. Eisenhower
Toulouse, 31100 France*

JULIEN PLE

*NAVBLUE, 1 rond-point Maurice
Blagnac, 31707 France
Julien.Ple@navblue.aero*

Abstract

The Future Sky Safety project 4 (FSS P4) aims at developing a prototype Risk Observatory (RO) that will assist in the safety assessment of the total aviation transport system. The Risk Observatory is based on the interaction between safety models covering various domains of the aviation transport system: Aircraft, Air Traffic Management, Airline Operation. In this paper we describe the development of the Aircraft domain safety model and its integration within the RO thanks to the specification and the implementation of a dedicated interface between the Aircraft Operation Safety Model described in this paper and a backbone model developed in cooperation with the other partners of the FSS project.

The main inputs used to develop the aircraft safety model are the Aircraft Functional Hazard Assessment (FHA) and the Standard Operating Procedures (SOP). The FHA is used to assess the impact of the aircraft function failures on the aircraft and its occupants considering existing or assumed mitigation means and derive safety requirements for the aircraft design. In the context of FSS, the FHA is used to infer a severity level for each considered failure scenario and the ensued occurrence probability targets as per the European Aviation Safety Agency regulations. The SOP describes the main actions to be performed by the flight crew during each flight phase in order to ensure a safe flight and landing. The Aircraft safety model computes, for each operation procedure, a qualitative safety performance measure that is based on crew errors, aircraft system failures, safety performance measure of previous relevant procedures and external actor errors.

Integration of the Aircraft Safety Model in the RO is performed via a Backbone model that has been developed with other domains. The Backbone model manages in a consistent way generic contributors and influencing factors like the environmental conditions, leading to a global risk such as Runway Excursion. The Aircraft Safety Model is used to verify that the preliminary aircraft system architecture is able to fulfil the safety objectives resulting from the FHA. The Aircraft Safety Model contributes to refine the aircraft system architectures and flight crew contributors operations. It provides safety outcomes to the Backbone model.

Keywords Safety; Aircraft Safety Modelling; Flight operation procedures; Runway excursion ; Mid-Air collision

1. Introduction

The Future Sky Safety (FSS) project aims at developing a prototype Risk Observatory (RO) that will assist in the safety assessment of the total aviation transport system. The Risk Observatory is based on the interaction between safety models covering various domains of the aviation transport system.

In the following of the paper we first detail the role of the Risk Observatory and we introduce the notion of the Backbone model that federates domain specific models. We then illustrate this notion with the Backbone model developed to assess the possible risk of runway excursion resulting from both ground and airborne system

failures, human errors – i.e. flight crew, air traffic controllers, ground operators and also adverse environmental conditions that may occur in combination. In the following section we explain how we used two documents produced by the Aircraft manufacturer (the Aircraft Functional Hazard Assessment (FHA) and the Standard Operating Procedures (SOP)) in order to develop a new type of Aircraft Safety Model. Finally, we describe how this Aircraft Safety Model can be managed by the backbone model to assess specific risks and provide insights in safety performances to safety analysts using the RO. Such outcomes considering the role of various domains for a given risk, enable to perform a global assessment of the total aviation transport system.

2. Risk Observatory

2.1. Goals of the Risk Observatory

The Risk Observatory (Verstraeten et al., 2016) will acquire, merge and structure safety data and translate it into actionable safety information that should help to identify the combination of the most significant contributors involved in serious incident and accident, and highlight where effort should be put to reduce their probability of occurrence. The core of the risk observatory is formed by a risk assessment framework that integrates safety models covering various domains of the aviation transport system: Aircraft, Air Traffic Management, Airline Operation. The framework is fed by different data inputs: e.g. operation data from the aircraft operator domain (e.g. originating from Flight Data Monitoring (FDM)) and ANSP (Air Navigation Service Providers) domain, but also occurrences data. The risk observatory will offer important insights in safety performance to RO users, which can be used in the risk assessment of new aircraft operations and innovative system architectures and in safety assurance by identifying safety trends, key risk areas, and efficient mitigation measures. Several use cases were defined during the first stage of the project, we detail two of them:

- **Risk Overview:** The RO is used to assess the probability of occurrence and the trend over time of a given risk such as Mid Air Collision or Runway Excursion. In addition, the RO is used to assess the importance of the elements contributing to this risk. An Aircraft manufacturer could use the RO in order to check whether the combination of aircraft-related contributors with contributors from other domains and also external factors can lead to unacceptable risks. The aircraft manufacturer could monitor the sensitivity of contributors from other domains to a given risk in order to check that the assumptions made to assess the aircraft design are realistic ones, i.e. not underestimated, and can be actually used to validate the outcomes of the Aircraft Safety Models.
- **What-if scenario:** The RO is used to estimate the impact of changes (such as the introduction of a new procedure or a new system design) on the assessment of a given safety event. An aircraft manufacturer could use the RO in order to compare the safety impact of such foreseen changes with the current baseline in which no change is implemented.

2.2. Backbone Model

The Backbone model has been developed with other domains. The Backbone model manages in a consistent way contributors and influencing factors leading to a global risk such as Runway Excursion resulting from various causes in combination.

Contributing Factors are elements contributing to the occurrence of a specific safety event. A contributing factor can be a technical causing factor (e.g. airborne or ground equipment failure) or human factor (flight crew, ATCO, ground operator errors). A list of Generic Contributing Factors (GCF) has been drawn up for each risk. These factors are part of the backbone and can be related to different domains. The following table provides the main categories of GCF have been defined for the risk of runway excursion:

Table 1. Categories of Generic Contributing Factors

| Ref. | Generic contributing factors for RWY-EXC Risk |
|------|---|
| 1 | Approach preparation and management by crew |
| 2 | Approach preparation and management by aircraft systems |
| 3 | Air Traffic Control |
| 4 | Unstable approach |
| 5 | Inappropriate flare and touchdown |
| 6 | Inappropriate lateral positioning and steering |
| 7 | Degraded landing gear or braking/ Steering systems |
| 15 | Airborne systems - Runway Excursion Prevention |
| 16 | Ground systems |

The following table provides GCF for the risk of runway excursion included in two categories.

Table 2. Contributors in Categories #1 and #4

| 1 | Approach preparation and management by crew | 4 | Unstable approach |
|-----|---|-----|---|
| 1.1 | Inaccurate weather forecast available at flight preparation | 4.1 | Excessive speed |
| 1.3 | Crew performs inaccurate landing performance check, or fails to perform/revise landing performance check based on available information | 4.2 | Excessive lateral and vertical path |
| 1.4 | Inadequate airport, approach or runway data available to crew (chart, AIP, NOTAM, FMS ...) | 4.3 | Excessive thrust |
| 1.5 | Crew performs inappropriate approach preparation (Non-compliance SOP) | 4.4 | Late or inappropriate flaps/gear configuration |
| 1.6 | Crew fails to revise approach strategy, following ATC change request | 4.5 | Inappropriate use of automation during approach |
| | | 4.6 | Absence of go around when unstable approach |
| | | 4.7 | Late destabilization of the approach |

Influencing Factors (IF) are elements that may affect the frequency of occurrence or the potential consequences of one or several contributing factors. A common list of Influencing Factors is shared by all specific domain risk models and the backbone model. They can be applied to various risks according to their relevance. The influencing factors can be computed by the Domain Specific safety models but also at the level of the backbone model.

Their characterisation is based on average industry values (for aircraft performance and characteristics) or on international standards for aircraft and airport operations. Criteria used are based on official sources (EASA, ICAO...), Aircraft manufacturer internal sources (operational procedures, Aircraft manufacturer average landing performance effect) and Flight crew experience.

In the experimental stage of FSS, we have assigned each IF a weight and also an estimated probability of encountering such an Influencing situation during a flight phase like the final approach or landing.

The weight of an influencing factor reflects its influence (negative or positive one) on the sequence of contributing factors that will lead to a risk. This weight is directly linked to the characteristics of the influencing factor. A weight equal to 1 is used to indicate that the IF has no influence while a weight greater than 1 reflects a negative influence. For example a 'Good' runway surface quality is assigned a weight of 1.

The weight associated to some specific influencing factors like for example the runway length (short, medium, long) may depend on the category of aircraft (light/ medium propeller A/C, Light jet A/C, ..., Heavy & Super jet A/C). The shorter is the runway the higher will be the weight given the increase of a possible risk of runway excursion for a given A/C ground speed.

Examples of influencing factors with attributes are given below:

- Traffic density and complexity: High, Medium, Low
- Runway surface: Dry, Dump, Wet, Contaminated
- Wind: Direction x strength: {Tailwind, cross wind, headwind} x {moderate, strong}.

The wind strength has been defined according to EASA certification standards for aeroplanes (see AMC AWO 131 § 3.1, (EASA, 2003)), it is summarized in the following table.

Table 3. EASA Classification of wind strength

| WIND | Moderate | Strong |
|-----------|-----------------|-----------------|
| Headwind | Less than 25 KT | More than 25 KT |
| Crosswind | Less than 18 KT | More than 18 KT |
| Tailwind | Less than 10 KT | More than 10 KT |

Probabilities assigned to each IF are much difficult to define. There is today no actual agreed values except for some of them like for example the wind. For this specific IF the probability comes from an official certification source (Specifications for All Weather Operations (AWO)) and is already used in Aircraft System Safety Assessment. This probability is applicable to the whole A/C flight duration.

Table 4. Probabilities of strong wind according to AMC AWO 131 § 3.1

| | |
|-------------------|--------------------------------|
| Strong Head wind | 8×10^{-3} (per cycle) |
| Strong Tail wind | 8×10^{-3} (per cycle) |
| Strong Cross wind | 1×10^{-2} (per cycle) |

The initial values of the weight and probability of occurrence are set in the risk observatory and can be modified by the RO user based on statistics from its own database.

It is worth noting that such a notion of Influencing Factor has been introduced in the frame of the project and has not been validated nor approved by the industrial partners, airlines and EASA. Therefore the safety performance indicators resulting from this modeling activity performed by using the RO shall not be considered as trustworthy outcomes.

2.3. Runway Excursion Backbone Model

The backbone model used for assessing the risk of Runway Excursions is based on the Accident Incident Model relying on barriers that prevent failures/ errors to propagate and lead to the risk (see Eurocontrol (2006)).

The main elements of the backbone models are the ‘precursors’ and the ‘barriers’.

- Precursors represent a hazardous situation that acts as the exposure to a barrier and also as the result of barrier failure.
- Barriers represent the safety function designed to prevent the occurrence of the risk (e.g. runway excursion). Each barrier has a fault tree associated with it, which represents the logically related elements from the relevant domains contributing to its failure.

The elements that constitute the backbone model are the generic contributing and influencing factors, presented in the previous section. The generic contributing factors have been specified for the design of the RO to enable the link with other specific domains.

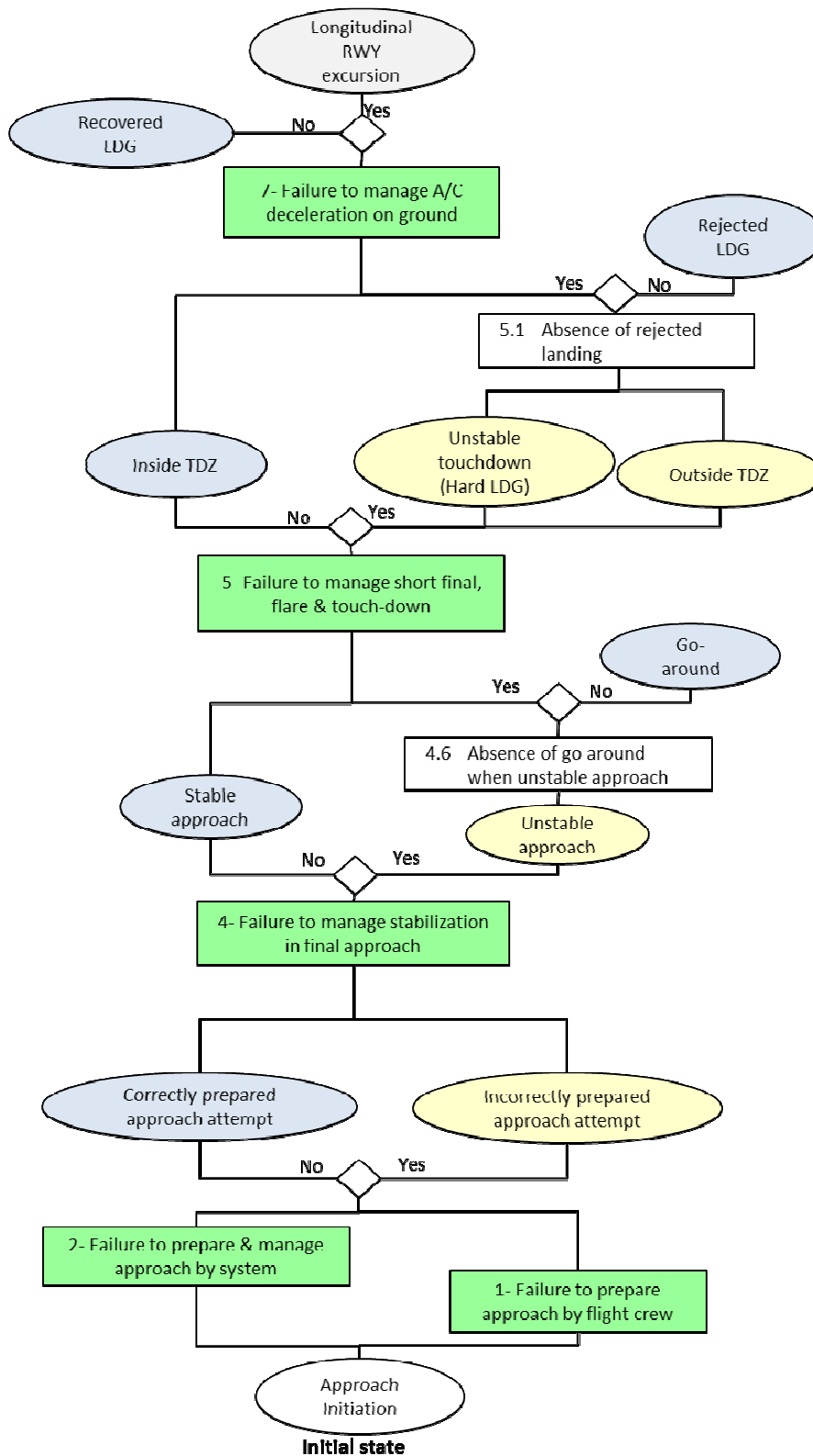


Fig. 1: Backbone model for longitudinal Runway Excursion – Barriers

The backbone model built to model the risk of a Runway Excursion depicts how the different contributing factors interact with each other and what impact they have on the overall risk. Fig. 1 is a simplified graphical

representation of the backbone model related to the risk of longitudinal runway excursion with the associated barriers to mitigate the risk.

This backbone model has been built according to a bottom-up approach. The starting point is the “Approach initiation” as depicted by the white oval shaped drawing. The light grey oval shaped drawing (Longitudinal RWY excursion) is the final unsafe state that will be the consequence of the inefficiency of all barriers against all contributing factors and influencing factors involved in the risk.

The graphical elements of this model are explained below:

- The light yellow and light blue oval shaped drawings in the next figure below depict intermediate steps. Light blue oval shaped drawings can either be a nominal state / situation (Stable approach) or a recovered action (rejected landing) corresponding to an expected flight crew action. The light yellow oval shaped drawings represent a failed state / situation as for example ‘Unstable approach’ or ‘landing outside Touch down zone’. Failed state / situations are the result of a series of individual contributing factors or several ones in combination.

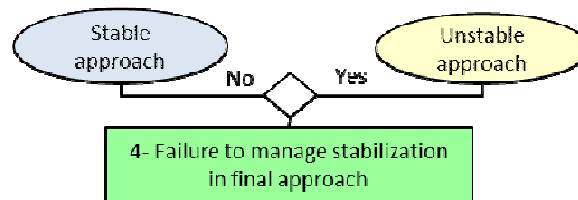


Fig. 2: Backbone model for longitudinal Runway Excursion – Link between factors and Barriers

- The next figure shows how a failed state / situation is modelled by a simple logic-OR Boolean combination of several contributing factors. The influencing factors that may aggravate the situation are indicated in the model. In the example of the figure below, flight crew performance (IF 503) and a low visibility / ceiling (IF 501.5) have been considered as relevant IF's.

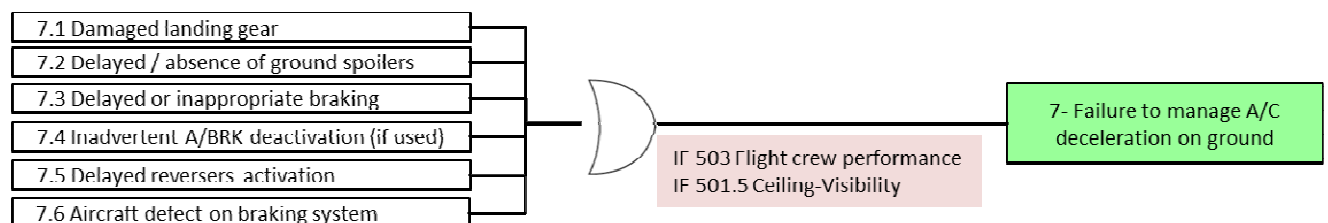


Fig. 3: Backbone model for longitudinal Runway Excursion – Link between factors and Barriers

3. Development of the Aircraft Operation Safety Model

3.1. Model-Based Safety Assessment of Aircraft Operations

Model Based Safety Assessment (MBSA) approaches have been developed among other things to strengthen the links between system specifications and safety models. These models also enable to automatically find out combinations of failures leading to undesired events for complex systems. MBSA has been successfully applied to assess safety of the detailed design of aircraft systems (see Bieber et al. (2004)). These models describe failure propagation paths inside a system architecture, based on the explicit description of how equipment used in the system architecture may fail and how they behave under failure occurrence. These models usually deal with technical problems of equipment.

More recently, the MBSA approach was also used to assess the safety of systems at an earlier stage of design when the system architecture is not necessarily fully defined. These new models focus on what the system should achieve in terms functions and operations. For instance, see Maitrehenry (2012) for a description of the use of models to support Functional Hazard Assessment. In that case, the effect of the failure of functions is analysed. Other models were used to study the safety of operating procedures such as satellite ground control operations (see Martinie et al. (2016)) or abnormal and emergency procedures, when interacting with the Aircraft systems (see Morel and de Brito(2016)). These models deal with both system functional failures and operator errors seen as deviations from the expected actions described in the Standard Operating Procedures (SOP).

In the frame of the Future Sky Safety project, we proposed to use the MBSA approach in order to build a model of Aircraft operations that can support the assessment of possible risks of runway excursion and mid-air collision. The Aircraft Operation Safety Model should describe the operating procedures considering the relevant function failures, human errors (flight crew, ATC operators) and also the most significant external conditions.

3.2. Structure of the Aircraft Operation Safety Model

The model of Aircraft operations is based on aircraft Standard Operating Procedures* (including Flight Crew Operating Manual (FCOM)) and the Flight Crew Training Manual (FCTM)). The same approach can be used to model any type of significant safety issues/ major risks (e.g. risk of Mid Air collision, CFIT...).

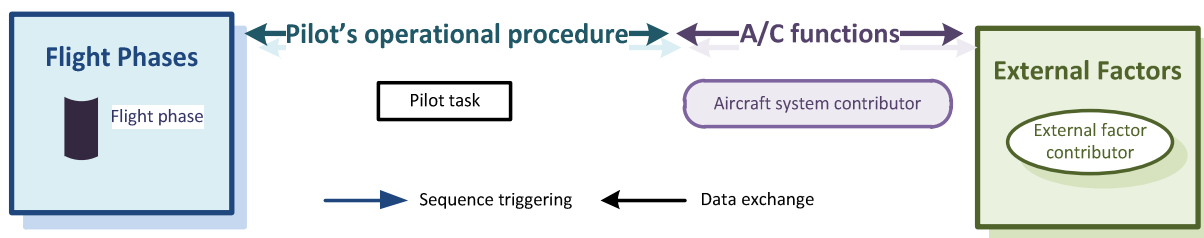


Fig. 4: Structure of Aircraft Operation Model

The model of Aircraft operations is organized according to the previous structure (Fig. 4):

- The sequence of Aircraft Flight Phases and flight levels requiring flight crew actions as indicated in the SOP's (e.g. En-route, 200 ft., 20 ft.) is listed in the left part of the figure.
- Pilot's procedure and associated tasks, required to perform the Aircraft operations during the considered flight phase, are described in the middle of the figure. Only operations that have been deemed relevant regarding to each scenario are considered here: it means that only part of the operational procedure having an influence on the studied risk is analysed. The model also shows Aircraft Functions / Systems used to perform the Flight Crew tasks.
- External Factors that influence the Aircraft operations (e.g. Air Traffic Management ...) are provided in the right part of the figure. Interaction between external actors and the aircraft operations are depicted by arrows (data or status exchanges).

This model highlights the links with generic contributors involved in each scenario: either at the level of a pilot task or Aircraft systems contributors, or at the level of external factors. For example, the following pilot tasks must be performed as descent preparation before top of descent:

* The reference for this study is an Airbus Long Range Aircraft.

DESCENT PREPARATION

Descent preparation and approach briefing should be completed before top of descent.

Ident.: PRO-NOR-SOP-16-A-00012246.0001001 / 28 APR 14

WEATHER AND LANDING INFORMATION.....OBTAIN

Check weather reports at ALTERNATE and DESTINATION airports. Airfield data if any should include runway in use for arrival.

Note: When operating in cold weather conditions, consider altitude correction. Refer to PER-OPD-GEN ALTITUDE TEMPERATURE CORRECTION.

Ident.: PRO-NOR-SOP-16-A-00013713.0003001 / 23 JUN 15

LANDING PERFORMANCE..... CONFIRM

Perform an in-flight landing performance assessment if the landing conditions changed compared with the landing computation at dispatch, or with a previous computation (e.g. runway, weather conditions, in-flight failure affecting performance, diversion).

Fig. 5: Extract from SOP related to Descent preparation and Landing Performance assessment

This is modelled by the pilot task “Revise Approach / Landing Strategy”. This task is linked to the contributing factors # 1.3.b and # 1.6 (Fig. 6). It uses inputs ‘Runway characteristics’ and ‘Weather information’ (external factors), Technical status of aircraft (from Flight Crew Alerting systems) and Charts as well as other Flight Management data (from Aircraft Flight Management system).

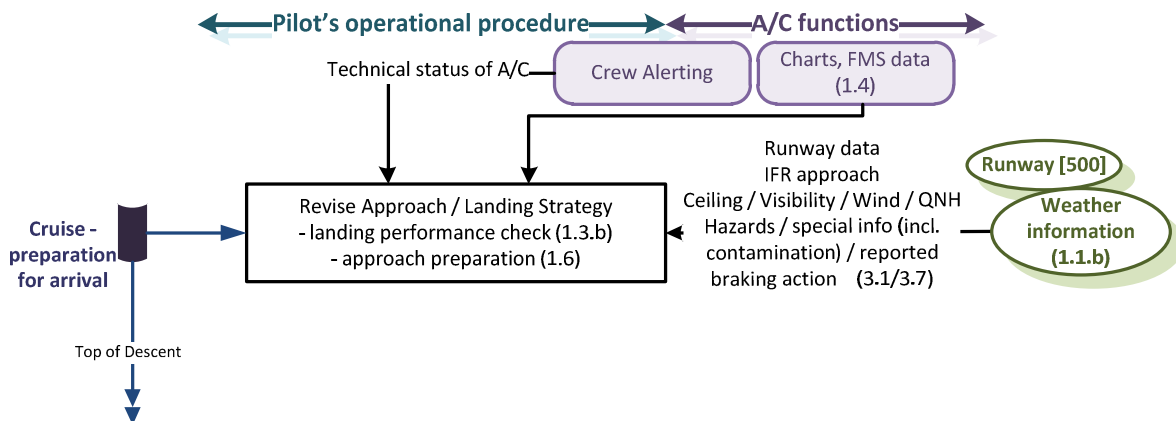


Fig. 6: Aircraft Operation Safety Model for Runway Excursion – Landing Preparation Phase

The next figure gives the part related with the Landing phase of the Aircraft Operation Safety Model. To validate this model, a selection of Runway Excursions described in accident reports from official bodies as NTSB, ATSB, was analyzed. We checked that contributing factors identified in the investigation reports were correctly considered in the Aircraft Operation Model. For instance, we highlighted in dark red in the previous picture all the factors that appeared in the accident report of a runway excursion that occurred in Paris Charles de Gaulle in 2004 (BEA, 2004). In that incident, the flight crew did not decide to reject landing despite an excessive final approach speed, they did not properly monitor the Touch Down zone leading to a long flare and they did not use the Thrust Reversers. Furthermore, there was a tailwind of around 5 KT during the landing.

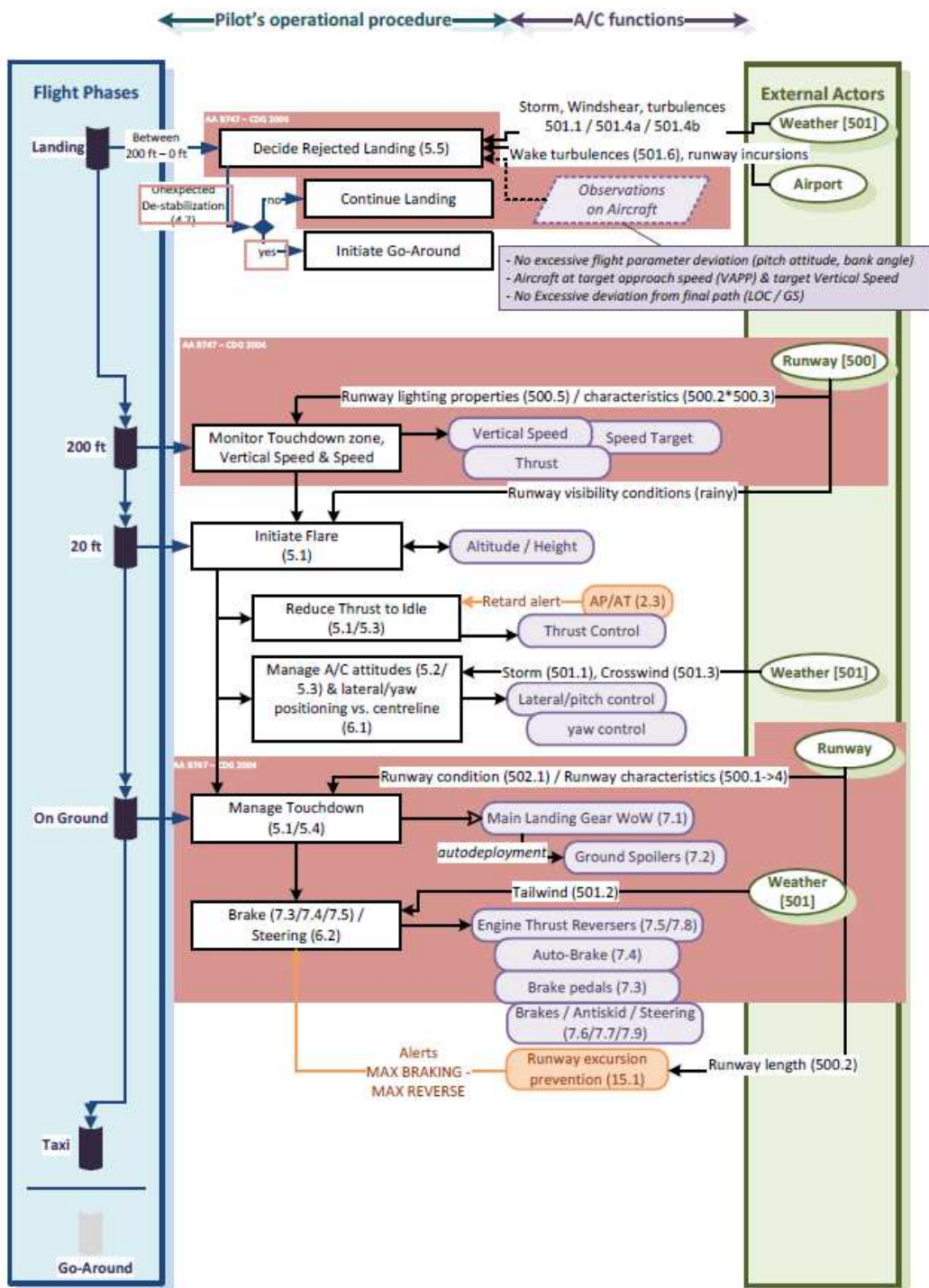


Fig. 7: Aircraft Operation Safety Model for Runway Excursion – Landing Phase

3.3. Detailed Modelling with AltaRica

We used the AltaRica language (Arnold et al. (2000)) to describe the Aircraft Operation Safety Model. Each component (flight phase, operating procedure step, system functions, ...) of the Aircraft Operation Safety Model is described by a node that is selected from a pre-existing library. Fig. 8 shows a node corresponding to a processing function. This node has three states in its automaton (shown in the figure):

- SAFE : nominal state

- LOST: degraded state when the function is lost or it has an obviously internally detected erroneous behaviour
- ERR: degraded state when the function has an undetected ERRoneous behaviour (i.e. undetected internally – even if this state may be detected by others system monitoring either during the flight or through pre-flight tests)

The node has two failure events Loss and Undetected Erroneous Functioning (UEF) that trigger the state changes. When available, a probability of occurrence is associated with these events.

Furthermore, the node has one input and one output that propagate information about the correctness of the outcome of the function. Three values are used:

- OK: the function outcome has the expected value
- Invalid: the function outcome is either not produced or it is detected as an invalid by other functions using this outcome
- Corrupted: The outcome is considered valid and it is not detected as faulty by other functions using this outcome.

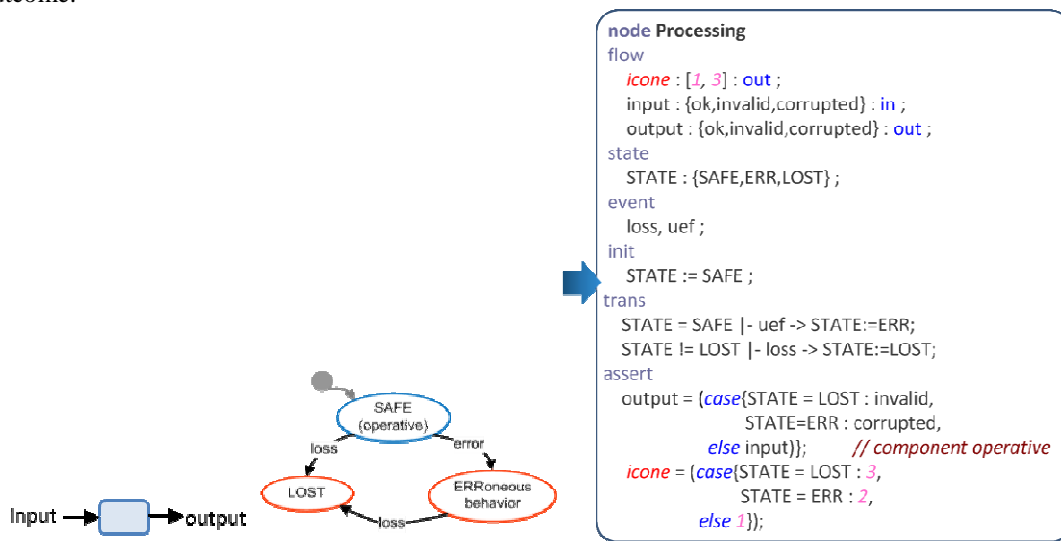


Fig. 8: Node State Automata, with translation into AltaRica code

This AltaRica node was used several times when we built the Aircraft Operation Model. The following figure contains an extract of this model, it shows two instances of the processing node: AC_VSpeedControl and AC_SpeedControl that model functions that control vertical speed and speed of the Aircraft. We used other types of AltaRica nodes that describe steps of operating procedures such as Op_MonitorRejectLanding (instance of a monitoring task), Op-DecideRejectedLanding (instance of a decision task), Op_ManageVerticalSpeedandSpeed (instance of a management task). As in the case of the processing function, an operating step is not always performed correctly. In particular, we consider that tasks can be partially performed, not performed or erroneously performed. The library of nodes describing operating procedures is explained in more details in (Bieber et al., 2016).

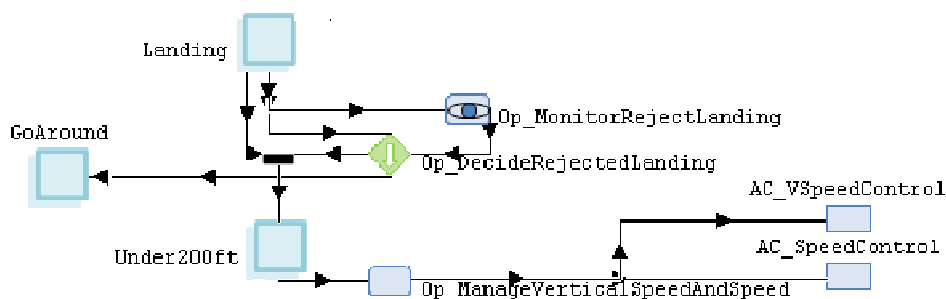


Fig. 9: Extract from the Aircraft Operation safety Model in AltaRica

We also used nodes that model the active flight phase (Landing, Under200ft, and GoAround). They are mainly used to activate relevant operating procedures. For instance, during landing under 200 ft, the flight crew has to manage the vertical speed and the speed of the aircraft. Consequently the link that goes from node Under200ft towards node Op_ManageVerticalSpeedAndSpeed is used to activate this operating procedure step when the flight phase is active. Conversely, some operating procedure steps may activate a flight phase. For instance, task Op_DecideRejectLanding can activate the Go Around flight phase.

3.4. Safety Assessment Results

Minimal Cut Sets (MCS) (e.g. minimal combinations of node events leading to an observed situation) can be automatically computed from the AltaRica model. For instance, the 5 following MCS were generated using Dassault Aviation Cecilia tool for AltaRica. They all lead to a situation where the Aircraft Speed is excessive at Touch Down:

```
{Op_ManageTouchDown.UEF}
{AC_SpeedControl.UEF, Op_MonitorRejectLanding_Under20ft.Loss}
{AC_ThrustControl.UEF, Op_MonitorRejectLanding_Under20ft.Loss}
{Op_ManageVerticalSpeedAndSpeed.UEF, Op_MonitorRejectLanding_Under20ft.Loss}
{Op_ReduceThrustToIdle.UEF, Op_MonitorRejectLanding_Under20ft.Loss, }
```

Each of the 5 previous lines is a MCS that gives the name of one or several nodes of the model and the related event leading to an excessive speed. The first line is a single event MCS representing an error of the flight crew when managing Touch-Down. The two following MCS combine a technical failure (erroneous behaviour of either the functions that control aircraft speed or the engines) and human error (the crew does not reject landing). Finally, the two last MCS are combinations of human errors (erroneous management of speed or thrust and the crew does not reject landing). It could also be the case that a MCS is exclusively made of technical failures or that the MCS contains some external events such as the loss of GPS satellites.

This safety outcome can be used to demonstrate that the aircraft meets qualitative and quantitative safety requirement. With respect to qualitative requirements, we could for instance review the MCS in order to check that no single safety event can lead to a situation that has a catastrophic effect. With respect to quantitative requirement the MCS can be used in conjunction with information about the probabilities of the node events in order to compute the probability of a given situation such as excessive speed at touch-down.

The aircraft manufacturer can provide the probabilities of the occurrence of function failures and of some external events but human errors are not usually quantified in the safety model built by the Aircraft manufacturer and systems provider since this is not requested by the EASA. So it might be difficult to check quantitative safety requirements of aircraft operations without information from other domains such as airline operators or ATM National Service Providers.

4. Integration of the Aircraft Safety Model into the Risk Observatory

The Aircraft Operation safety model can provide qualitative and quantitative information for the backbone model. For a given Generic Contributor of the Backbone model, an observer node is created in the AltaRica model. This observer node is used to automatically compute the list of all minimal cut sets leading to a state where the Generic Contributor has occurred. One minimal cut set is a combination of domain specific contributors leading to the occurrence of the Generic Contributor.

Let's consider the generic contributor 4.1 "*Excessive Speed*" of the Backbone model. It is a contributor that leads to the failure to manage stabilization during the final approach. As explained in the previous section we use the Aircraft Operation Safety Model in order to generate MCS for the situation "Excessive Speed at 20ft". We can use the combinations of technical faults and human errors of the MCS in order to refine contributor 4.1 of the

Backbone model. A similar approach can be used for all Generic Contributors that can benefit from information contained in the Aircraft Operation safety model (e.g; aircraft function failures and operating procedure errors).

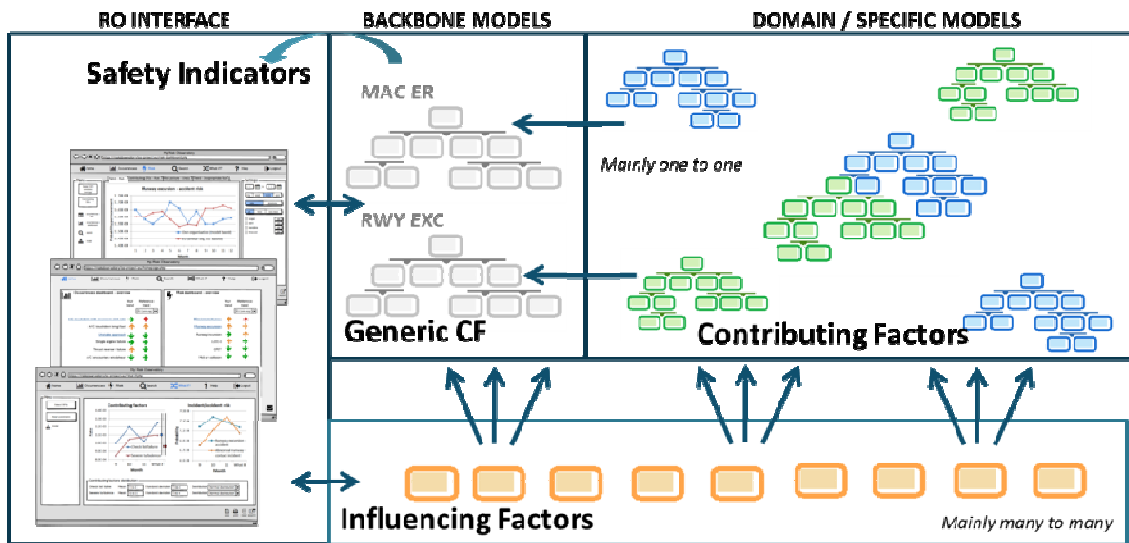


Fig. 10: Relationship between domain specific models, backbone models and RO interface

We can also provide the occurrence probability of technical failures managed by the Aircraft manufacturer. If the backbone model also contain probability of human errors provides by aircraft operators and ANSP then it should be possible to compute the probability of the all Generic Contributors and of overall risk (Runway Excursion, Mid-Air Collision, ...).

5. Conclusion

Future Sky Safety project aims at developing a total system approach to aviation safety. This European R&T project has demonstrated the added value and potential of developing a Risk Observatory formed by high-level modular framework that connects safety risk assessment models of the different domains in aeronautics. With this purpose, FSS partners agreed to elaborate a shared backbone model enabling to federate outputs from various domain specific safety models.

This paper has highlighted how a safety model developed by aircraft and system manufacturers can produce relevant safety outcomes usable by a backbone model thanks to an appropriate interface structure, in order to produce relevant safety performance indicators available in a Risk Observatory.

5.1. Lessons learnt

One of the difficulties we had to face with, in the frame of Future Sky Safety, is the lack of uniformity between the risk classification scheme used by the aircraft manufacturers and the Air Navigation Services Providers, both being partners of this project. The safety models related to the first domain use the CS25-1309 certification specification for Large Aeroplanes (EASA), while each ANSP uses its own Risk Classification scheme agreed with their local/ national regulatory bodies.

From a qualitative point of view there are yet similarities in the two domains: Both Risk Classification Schemes refer to five fairly equivalent levels of severity (from No Safety Effect to Accident / Catastrophic worst case) and five categories of frequencies (from 'very frequent' up to 'rare' events for ANSP based on targeted frequencies of occurrences per year and from 'probable' up to 'extremely improbable' for the aircraft failures where the quantified objectives are expressed in failure rate per flight hour); see (EASA, 2015).

Recently EASA took the initiative to build a safety plan aiming at standardizing the risk classification used by each ATC national regulatory body (see EU No 376/2014, 2014). This work is in progress. In the experimental stage of FSS, we will propose a common Risk Classification Scheme with coherent target probabilities that would enable the RO to produce safety performances indicators.

A bottleneck is the collection of data in a standardized and secure way due to the large variety in which operators collect and process their data. A particular challenge for Europe is the involvement of organizations from different countries with different cultures and legal systems. In the coming years exchange and cooperation is foreseen with similar initiatives aiming for a successful Risk Observatory for total system risk management.

5.2. Further Work

The development of risk models will be improved by:

- Further developing human response modelling. There is a need to get a better understanding of the relationship between qualitative generally understood notions and the translation of these in real observable and quantifiable influences on risk and risk reduction;
- Selecting the appropriate level of detail of the model. This selection is strongly dependant on the use and users of the model;
- Assessing the availability of representative datasets and improving the integration of Data (FDM, ADS-B, accident reports, ...) into the RO in order to improve the accuracy of safety performance indicators resulting from the models assessment ;
- Using the Influencing Factors in the quantitative assessment ;
- Analysing common causes across domains ;
- Reinforcing the partnership between the different types of stakeholders e.g. airlines and manufacturers in order to refine the multi-domain safety model assessment of risks in aeronautics.

References

- A. Arnold, A. Griffault, G. Point, A. Rauzy (2000). The AltaRica formalism for describing concurrent systems. In: *Fundamenta Informaticae* p109-124.
- BEA Bureau Enquête Analyse , Rapport Incident survenu le 4 novembre 2004 à Paris Charles de Gaulle (95) au Boeing 747-300 immatriculé D2-TEB exploité par TAAG
- P. Bieber, C. Bognol, C. Castel, J.-P. Heckmann, C. Kehren, S. Metge, C. Seguin, (2004) "Safety Assessment with AltaRica - Lessons learnt based on two aircraft system studies" 18th IFIP World Computer Congress, Topical Day on New Methods for Avionics Certification, August 26th, 2004, Toulouse (France).
- P. Bieber, C. Seguin, V. Louis, F. Many (2016), Model Based Safety Assessment of Concept of Operations for Drones, in proceedings of Congrès Lambda Mu 20 de Maîtrise des Risques et de Sûreté de Fonctionnement, Saint-Malo, 2016
- EUROCONTROL (2006). Main report for the 2005/2012 Integrated Risk Picture for Air Traffic Management in Europe, EEC Note No. 05/06, Eurocontrol Experimental Centre, Brétigny-sur-Orge, France.
- S. Maitrehenry, S. Metge, Y. Ait-Ameur, P. Bieber (2011), "Towards Model-Based Functional Hazard Assessment at Aircraft Level", ESREL 2011, Troyes, September 2011
- C. Martinie, P. A. Palanque, R. Fahssi, J.-P. Blanquart, C. Fayollas, C. Seguin (2016), Task Model-Based Systematic Analysis of Both System Failures and Human Errors. *IEEE Trans. Human-Machine Systems* 46(2): 243-254
- M. Morel, G. de Brito,(2016), Approche basée « modèle » pour l'analyse Safety de systèmes avioniques critiques et des erreurs humaines, in proceedings of Congrès Lambda Mu 20 de Maîtrise des Risques et de Sûreté de Fonctionnement, Saint-Malo, 2016
- EU (2016), REGULATION (EU) No 376/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU) EASA(2003), Certification Specifications for All Weather Operations, ED Decision 2003/6/RM, Final 17/10/2003
- EASA (2015), Risk Analysis Tool – RAT Guidance material, issue 2.0 dated 04/12/2015 – EASA deliverable
- Verstraeten, J., Van Baren, G., Wever, R.. (2016). The Risk Observatory: Developing an Aviation Safety Information Sharing Platform in Europe. *Journal of Safety Studies*. 2. 91. 10.5296/jss.v2i2.10443.

About the authors

Pierre BIEBER (Pierre.Bieber@onera.fr) is a research engineer working for ONERA, the French aerospace lab. He is interested in the application of innovative safety and security assessment techniques to aerospace systems. He heads the “Modelling and Analysis of Global Systems” research unit.

Sylvain METGE (Sylvain.Metge@airbus.com) Sylvain METGE is an aircraft safety manager working in the Engineering Dpt of Airbus since 15 years. He has spent nearly 30 years in dependability activities dedicated to R&T, including software and systems modelling activities. He has been involved in various air transport & space R&T projects and design development of complex dependable architectures. Sylvain Metge worked in various major companies and Research labs, in particular the French Laboratory for Analysis and Architecture of Systems – LAAS-CNRS, the Department of the Air Navigation and Services attached to the French Civil Aviation Authority, Eurocontrol and more recently, Airbus Operations S.A.S.

Marion MOREL previously worked as a safety specialist at Thales Avionics where she participated to the Future Sky Safety project.

Julien PLE (Julien.Ple@navblue.aero) is an aeronautical engineer and project manager at NAVBLUE (Airbus Flight Operations Services company) specialized on Flight Data Analysis solutions and services. He is a former Flight Operations Support Senior Engineer on A320 and A330/A340 programs at Airbus, and project manager for GPS-based approach solutions at Quovadis. Over 4 years, he has coordinated several programs in airlines to assist the implementation of Safety Management Systems, and Flight Data Analysis solutions, and has recently been nominated to lead the development of NAVBLUE’s new FDA software solution within Airbus’ wider SKYWISE data analytics programme. He also has a commercial pilot license with instrument rating and a flight instructor rating.

Acknowledgement

This project has received funding from the *European Union’s Horizon 2020 Research and Innovation Programme* under Grant Agreement No 640597.