Integrated Risk Assessment Framework

S. Metge (AI-F), B. Hickling (EUROCONTROL), P. Bieber, J. Morio, X. Olive (ONERA), F. Kaakai (TR6), J. Plé (NAVBLUE), C. Sannino (TAV), W.F.J.A. Rouwhorst, Bas van Doorn (NLR), F. Oliveira and R. Peixe (CEiiA)

Short abstract: Future Sky Safety is a Joint Research Programme (JRP) on Safety, initiated by EREA, the association of European Research Establishments in Aeronautics. The Programme contains two streams of activities: 1) coordination of the safety research programmes of the EREA institutes and 2) collaborative research projects on European safety priorities.

This deliverable (D4.7) is produced by the Project P4 “Total System Risk Assessment”. The main objective is to integrate the domain-specific risk assessment models into an integrated risk assessment framework and to perform framework verification.

Programme Manager	M.A. Piers , NLR
Operations Manager	L.J.P Speijker, NLR
Project Manager (P4)	W.F.J.A. Rouwhorst, NLR
Grant Agreement No.	640597
Document Identification	D4.7
Status	Approved
Version	2.0
Classification	Public

This page is intentionally left blank

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Contributing partners

Company	Name
EUROCONTROL	Brian HICKLING
Airbus (AI-F)	Sylvain METGE
CAA-UK	Matthew WEEKS
CEiiA	Fabio OLIVEIRA, Rui PEIXE
NAVBLUE	Mathieu TERRISSON, Julien PLE
ONERA	Pierre BIEBER, Jérôme MORIO, Xavier OLIVE
Thales Air Systems (TR6)	Fateh KAAKAI
Thales Avionics (TAV)	Christian SANNINO
NLR	Wilfred ROUWHORST, Bas van DOORN

Document Change Log

Version	Issue Date	Remarks
1.0	25-04-2019	First formal release
2.0	29-04-2019	Second formal release

Approval status

Prepared by: *(name)*	**Company**	**Role**	**Date**
Sylvain METGE	Airbus (AI-F)	Author	24-04-2019
Fabio OLIVEIRA / Rui PEIXE	CEiiA	Author	24-04-2019
Pierre BIEBER	ONERA	Author	24-04-2019
Bas van DOORN	NLR	Author	24-04-2019
Checked by: *(name)*	**Company**	**Role**	**Date**
Alex RUTTEN	NLR	Quality Assurance	29-04-2019
Approved by: *(name)*	**Company**	**Role**	**Date**
Wilfred ROUWHORST	NLR	Project Manager (P4)	24-04-2019
Lennaert SPEIJKER	NLR	Operations Manager	29-04-2019

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Acronyms

Acronym	Definition
ACARE	Advisory Council for Aviation Research and Innovation in Europe
ACAS	Airborne Collision Avoidance System
ACS	Area Control Surveillance
AGL	Above Ground Level
AltaRica	A high-level language designed for the modelling of systems
AIM	Accident Incident Model / Aeronautical Information Management
AMC	Acceptable Means of Compliance
Amdt	Amendment
ANSP	Air Navigation Service Provider
API	Application Programming Interface
ATC	Air Traffic Control
ATCo	Air Traffic Controller
ATM	Air Traffic Management
ATS	Air Traffic Service
A/BRK	Auto Brake
A/C	Aircraft
A/THR	Auto Thrust
BALS	Basic Approach Light System
BB	Back Bone
BRK	BReaK
CAPT	CAPTain
CAT	Commercial Air Transport / CATegory
CATS	Causal model for Air Transport Safety
CF	Contributing Factor
CFH	Controlled Flight Hours
CFIT	Controlled Flight Into Terrain
CL	Climb
CNS	Communication Navigation and Surveillance
COND	Condition
CRM	Crew Resource Management
DIE	Data Integration Engine
EASA	European Aviation Safety Agency
EC	European Commission
ECAC	European Civil Aviation Conference
ER	En Route
EREA	The association of European Research Establishments in Aeronautics
ESD	Event Sequence Diagram
EU	European Union
Exc	Excursion

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Acronym	Definition
FDM	Flight Data Management / Flight Data Monitoring
FH	Flight Hours
FHA	Functional Hazard Assessment
FL	Flight Level
FMS	Flight Management System
FSS	Future Sky Safety
F/O	First Officer
GCF	Generic Contributing Factor
GNSS	Global Navigation Satellite System
H	Probability density
HIALS	High Intensity Approach Lighting
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
IF	Influencing Factor
IFR	Instrument Flight Rules
JRP	Joint Research Programme
kt	knots
LOC	LOCalizer / Loss Of Control
LOC-I	Loss OF Control - In-flight
MAC	Mid Air Collision
MCS	Minimal Cut Set
MEF	Model Exchange Format
METAR	METeorological Airport Report
MS	Member States
Nac	Average Number of aircraft controlled by one ATS unit (/or ~one sector)
NALS	No Approach Light System
NOTAM	Notice To AirMen
OAT	Outside Air Temperature
P	Probability
PAPI	Precision Approach Path Indicator
PDF	Probability Density Function
Prc	Precursor
PSA	Probabilistic Safety Assessment
R	Risk value
RA	Resolution Advisory
RE	Runway Excursion
REV	Reverser
RI	Runway Incursion
RO	Risk Observatory
RWY	Runway
SCRAM	S Command-line Risk Analysis Multi-tool

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Acronym	Definition
SMM	Safety Management Manual
SOP	Standard Operating Procedures
SSA	System Safety Assessment
STCA	Short Term Conflict Alerting
SURF	SURFace
TA	Traffic Advisory
TCAS	Traffic Collision Avoidance System
Tf	Average flight time in hours
TMA	TerMinal control Area
TURB	Turbulence
VCS	Version Control System
VFR	Visual Flight Rules
VPG	Visual Path Guidance
WP	Work Package
XFTA	X Fault Tree Assessment engine working on models written in Open-PSA
XML	eXtensible Markup Language
X	Random vector
Xt	Average eXposure time

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

EXECUTIVE SUMMARY

Problem Area

Safety is a dynamic characteristic of the aviation system, whereby safety risks must be continuously mitigated. Furthermore, the aviation system entails the complex interaction of different organizations. Each organization has to implement a safety management system, which should interact to assure effective system-wide safety management. The ICAO Safety Management Manual (DOC 9859, [2]) gives guidelines on safety management fundamentals. A uniform and complete approach should be envisaged at European level. Stakeholder interviews and a literature survey unveiled critical aspects and defined the problem context for the activities in Project P4 "Total system risk assessment" of Future Sky Safety [4]:

- Safety Data Collection and Analysis: there is insufficient safety data available/used (both from the own operation or other operations) to get a full picture of safety risks, this causes uncertainty with regard to current safety performance. Available human resources are mostly used for processing data and reactive analysis based on individual occurrences. Often manual processing is needed, which can be time/effort consuming. Organizations can feel overloaded with data.
- Safety Indicators and Safety Performance Monitoring: there is a need for a uniform approach to safety indicator definitions and safety performance monitoring;
- Hazard and Risk Management: some difficulties emerged in the identification of new hazards when a change in systems or procedures occurs;
- Safety space: the safety information does not give appropriate means to executive management to make informed decisions on resource allocation for safety management. The allocation of excessive resources to protection or risk controls may result in the product or service becoming unprofitable, thus jeopardizing the viability of the organization. On the other hand, excess allocation of resources for production at the expense of protection can have an impact on the safety performance of the product or service and can ultimately lead to an accident. It is therefore essential to provide an early warning, if an unbalanced allocation of resources exists or is developing. The need to balance production and protection has become a readily understood and accepted requirement from a product and service provider perspective.

In light of this context, P4 has identified and further developed risk models in the aviation industry, and explores added value that cooperation between different domains on risk modelling can contribute to.

Description of Work

The objective of this task is to integrate domain-specific risk assessment modules with models representing the interfaces between domains to acquire an integrated risk assessment framework.

The integration of the domain-specific risk assessment models implies the need to characterize events and associated probabilities, as well as the integration of dynamic complex systems into distinct modules. First, these modules are then interconnected though interface modules, which are crucial in the development of the full risk assessment framework. Next, the development of processes for updating the

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

integrated risk assessment framework is considered, playing a critical role in assuring the reliability of the framework. Finally, the verification of this conceptual framework for risk assessment is addressed, by comparing predicted performance indicators with a quantitative verification of the backbone model and a verification of the usability of the frame work. A comparison with real data was found to be non-feasible.

Results & Conclusions

The main results of this study are described below.

- A backbone model approach was used to develop a framework able to integrate risk models from various aviation domains. This task also provided results on implementation of this framework in terms of definition of common formats, conversion rules between aviation domain safety indicators, treatment of influencing factors and common causes, management of the uncertainty on the data used to compute safety indicators, and identification of candidates for safety indicator computation tools.
- In order to assure the reliability of the framework, three update processes are considered, namely: risk scenario creation, allowing the adaptation of the input data to the specific scenario in analysis, while providing an easy way to directly compare different scenarios; model refinement, which is responsible for adaptation of the model to the relevant changes in the risk scenarios in analysis; and model update which shall allow the adaptation of the scenario to quickly changing factors that may influence the risk output. The framework is though in a way that, ideally, can make these processes use as inputs observed data and relevant external systems. Nevertheless, as these systems or connections may be difficult to accomplish, manual processes are also considered.
- The risk results obtained with the quantified Mid Air Collision (MAC) and Runway Excursion (RE) models does not perfectly match the MAC and RE accident probabilities assessed in the actual operation. Important reason for that is that the backbone models are quantified by using various data sources with different scopes in period of time, type of aircraft, type of aircraft operations, geographical reasons, etc. Secondly, the accident probabilities are often quite accurate while lower level (probability) information on contribution and influencing factors inside the backbone models is far less complete and accurate. Many times it is based on engineering judgement. The usability of the MAC and the RE models has been validated at top level only.

Applicability

This report is applicable to Project P4 “Total system risk assessment” of Future Sky Safety [1], [5]. It defines an approach to integrate various aviation risks models and it defines means to implement the approach in the risk observatory.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU’s Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

TABLE OF CONTENTS

Contributing partners 3
Document Change Log 3
Approval status 3
Acronyms 4

Executive Summary 7
Problem Area 7
Description of Work 7
Results & Conclusions 8
Applicability 8
Table of Contents 9

List of Figures 11

List of Tables 13

1 Introduction 14
1.1. The Programme 14
1.2. Project context 14
1.3. Research objectives 14
1.4. Approach 14
1.5. Structure of the document 15

2 Risk assessment framework development 16
2.1. Backbone Model Consolidation 17
2.1.1. Alignment of Backbone Models 17
2.1.2. Influencing Factors 20
2.2. Integration of domain specific risk models into the backbone model 27
2.2.1. Harmonized Formats 27
2.2.2. Conversion Rules 33
2.2.3. Common Causes 41
2.3. Implementation of the backbone model into the Risk Observatory 43
2.3.1. Software architecture 43
2.3.2. Guidance for the Implementation of the backbone model 45

3 Processes and practices for framework update 49
3.1. Risk scenario creation 49
3.2. Risk scenario refinement 49
3.3. Risk scenario update 50

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

3.4. Technical approach 50

4 Verification of the Risk Assessment Framework 51

4.1. Uncertainty of results 51
4.2. Framework Verification 54
4.2.1. Scoping of the Verification 54
4.2.2. Quantitative verification of risk assessment framework 55
4.2.3. Verification of the usability of the framework 62

5 Conclusions 68

6 References 69

Appendix A INTEGRATED RISK ASSESSMENT FRAMEWORK DETAILS 71

Appendix A.1 Backbone Models 71
Appendix A.1.1 MAC-ER Backbone fault-trees 71
Appendix A.1.2 Runway Excursion Backbone fault-trees 75
Appendix A.2 Table of Influencing Factors, rectified weights and mapped Generic Contributing Factors 79
Appendix A.3 Conversion Rules 101
Appendix A.4 Coverage of WP4.2 Recommendations by WP4.3 Activities 102

Appendix B PROCESSES AND PRACTICES FOR FRAMEWORK UPDATE 104

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

This page is intentionally left blank

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

LIST OF FIGURES

FIGURE 2-1: CATS EVENT SEQUENCE DIAGRAM 17
FIGURE 2-2: DESCRIPTION OF A ESD AS A FAULT TREE 18
FIGURE 2-3: A FAULT TREE DESCRIPTION OF MID-AIR COLLISION (TOP LEVEL VIEW) 19
FIGURE 2-4: FAULT TREE DESCRIPTION OF NEAR-MID AIR COLLISION (TOP LEVEL VIEW) 19
FIGURE 2-5: FAULT TREE DESCRIPTION OF SCENARIOS LEADING TO THE FAILURE OF A BARRIER 19
FIGURE 2-6: INFLUENCING FACTORS INVOLVED IN MORE THAN ONE RISK 21
FIGURE 2-7: MODULAR DESCRIPTION OF THE BACKBONE MODEL 27
FIGURE 2-8: INTEGRATION OF DOMAIN1 AND DOMAIN2 SPECIFIC MODELS INTO THE BACKBONE MODEL 27
FIGURE 2-9: FRAGMENT OF THE MAC BACKBONE MODEL FAULT TREE 28
FIGURE 2-10: OPEN PSA DESCRIPTION OF LOGICAL STRUCTURE OF THE MAC BACKBONE MODEL (FRAGMENT) 29
FIGURE 2-11: OPEN PSA DESCRIPTION OF BASIC EVENTS OF THE MAC BACKBONE MODEL (FRAGMENT) 30
FIGURE 2-12: DOMAIN SPECIFIC FAULT-TREE FOR GENERIC CONTRIBUTOR 31.1 30
FIGURE 2-13: OPEN PSA DESCRIPTION OF DOMAIN SPECIFIC MODEL (LOGICAL PART) 31
FIGURE 2-14: OPEN PSA DESCRIPTION OF DOMAIN SPECIFIC MODEL (QUANTITATIVE PART) 32
FIGURE 2-15: EXAMPLES OF INTEGRATION ISSUE AT BB LEVEL DUE TO UNIT HETEROGENEITY 34
FIGURE 2-16: ILLUSTRATION OF THE INTEGRATED RISK ASSESSMENT FRAMEWORK 35
FIGURE 2-17: ILLUSTRATION OF BB TARGET REFERENCE UNITS 36
FIGURE 2-18: ILLUSTRATION OF CONVERSION FUNCTIONS 39
FIGURE 2-19: CONVERSION FUNCTIONS 40
FIGURE 2-20: OPEN PSA SYNTAX FOR THE DEFINITION OF A COMMON CAUSE GROUP 42
FIGURE 2-21: IMPLEMENTATION OF THE INTEGRATED RISK ASSESSMENT FRAMEWORK 43
FIGURE 2-22: A XFTA SCRIPT 45
FIGURE 2-23: BB FAULT TREE DISPLAY BY ARBRE ANALYSTE TOOL (EXTRACT) 48
FIGURE 4-1: HISTOGRAM OF THE MAC PROBABILITY (200 SAMPLES) 53
FIGURE 4-2: PROBABILITY OF A MAC CALCULATED WITH ARBRE ANALYSTE 55
FIGURE 4-3: CAT AEROPLANE AIRLINE FATAL ACCIDENT RATE [EASA, 2018] 56
FIGURE 4-4: CAT AEROPLANE AIRLINE NON-FATAL ACCIDENT RATE [EASA, 2018] 56
FIGURE 4-5: RUNWAY EXCURSION PROBABILITY CALCULATED WITH ARBRE ANALYSTE USING [RE MODEL] 58
FIGURE 4-6: MINIMAL CUT SETS FOR THE [MAC MODEL] 62

FIGURE A-1: STRUCTURE OF THE TABLE DESCRIBING THE MAPPING BETWEEN IF AND GCF 100

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

LIST OF TABLES

TABLE 1: INFLUENCING FACTORS RELATED TO CLUSTER "WEATHER" 21
TABLE 2: VALUE ASSOCIATED TO IF "RUNWAY SURFACE" AS PER ICAO ANNEX 14 22
TABLE 3: WEIGHTS AND RATES OF OCCURRENCES OF IF 500.6 'RWY VPG' 23
TABLE 4: TABLES RATES AND WEIGHTS FOR IF_1 AND IF_2 24
TABLE 5: MAPPING TABLE BETWEEN GCF'S AND OF IF'S 25
TABLE 6: MODIFIED MAPPING TABLE BETWEEN GCF'S AND OF IF'S 26
TABLE 7: DEFAULT AND MODIFIED TABLE OF RATES AND WEIGHTS FOR IF1 26
TABLE 8: DEFINE-GATE TABLE 32
TABLE 9: DEFINE-BASIC-EVENT 33
TABLE 10: DATA STRUCTURE OF THE MAIN CLASSES OF DATA UNITS 35
TABLE 11: ICAO SAFETY RISK SEVERITY TABLE FROM SMM 37
TABLE 12: EU SAFETY RISK SEVERITY TABLE FROM CIR (EU) 1035/2011 37
TABLE 13: EASA SAFETY RISK SEVERITY TABLE FROM CS-25 38
TABLE 14: THE TEN MOST INFLUENT CONTRIBUTING FACTOR PROBABILITIES FOR MAC BACKBONE 53
TABLE 15 DIFFERENT SOURCES AND RESULTS ON MAC ACCIDENT FREQUENCY PER FLIGHT 57
TABLE 16: DIFFERENT SOURCES AND RESULTS ON RE ACCIDENT FREQUENCY PER FLIGHT. 60
TABLE 17: CONTRIBUTING FACTORS IN TOP 10 MINIMAL CUT SETS OF MAC MODEL 63
TABLE 18: RESULTING RE ACCIDENT PROBABILITY AFTER SETTING CONTRIBUTING FACTORS PROBABILITY TO 0. 64
TABLE 19: CONTRIBUTING FACTORS IN TOP 10 MINIMAL CUT SETS OF MAC MODEL 66
TABLE 20: RESULTING RE ACCIDENT PROBABILITY AFTER SETTING CONTRIBUTING FACTORS PROBABILITY TO 0. 66
TABLE 21: INFLUENCING FACTORS FOR MAC WITH THEIR ASSOCIATED RECTIFIED WEIGHTS 80
TABLE 22: INFLUENCING FACTORS FOR RWY EXC WITH THEIR ASSOCIATED RECTIFIED WEIGHTS 87
TABLE 23: MAPPING BETWEEN THE GCF'S RELATED TO RISK OF RE EXC. AND THEIR LINKED IF'S 99
TABLE 24: CONVERSION RULES ON UNITS FOR DIFFERENT STAKEHOLDERS 101

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

1 INTRODUCTION

1.1. The Programme

The European Commission's (EC) Flight Path 2050 vision aims to achieve the highest level of safety to ensure that passengers and freight as well as the air transport system and its infrastructure are protected. However, trends in safety performance over the last decade indicate that the ACARE Vision 2020 safety goal of an 80 % reduction of the accident rate is not being achieved. A stronger focus on safety is required. Therefore, a Joint Research Programme (JRP) on Aviation Safety - Future Sky Safety (FSS) - is started at the beginning of 2015, aiming for Coordinated Safety Research as well as Safety Research Coordination. Future Sky Safety has goals to coordinate safety research of the involved EREA research establishments and perform safety research and innovation actions targeting the highest levels of safety for European aviation [1],[4].

1.2. Project context

In the FSS project P4 "Total System Risk Assessment", a prototype Risk Observatory (RO) is developed as an enabling tool for safety management, see [1]. The risk observatory will acquire, fuse and structure safety data and translate it into actionable safety information: output that helps the user to distil safety intelligence to allow the implementation of appropriate measures to positively influence safety - i.e. reducing the serious incident and accident probability. The core of the risk observatory is formed by a risk assessment framework that integrates risk assessment models specifically developed to represent a certain domain. The framework is fed by different safety data inputs: e.g. normal operation data from the aircraft operator domain (e.g. originating from Flight Data Monitoring (FDM)) and ANSP domain, but also occurrence and incident data. The risk observatory will offer important insights in safety performance to safety analysts, which can be used in the risk assessment of new aircraft and systems and in safety assurance by identifying safety trends, key risk areas, and efficient mitigation measures. The risk observatory's scope is currently limited to the EASA Member States and the operations performed by service providers within the EASA Member States. Project P4 has as main objective to develop a working and practical Risk Observatory prototype to assess and monitor safety risks throughout the Total Aviation System and allow frequent update of the assessment of risks [5].

1.3. Research objectives

The main purpose of this document is to report how several existing aviation risk models are able to provide the safety information required in the Risk Observatory (RO).

1.4. Approach

This document is part of the WP4.3 of the FSS project P4 (see [5] for more information on it).

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

This work package develops a framework able to integrate various domain specific models into the RO. This is based on the backbone model approach developed within WP4.2. The work performed in T4.3.1 consolidates the backbone model approach previously developed and it investigates the means to implement this approach in RO.

1.5. Structure of the document

The document is structured as follows:

- Section 1 introduces the background and main purposes of this document;
- Section 2 describes the development of an integrated framework for risk assessment;
- Section 3 describes processes and practises for updating the integrated risk assessment framework;
- Section 4 describes the verification of the integrated risk assessment framework;
- Section 5 contains the conclusions and recommendations of this task;

Appendices A and B include technical details supporting the texts in sections 2, 3 and 4.

- Appendix A provides the Backbone models in the Mid Air Collision-(en route) en Runway Excursion fault trees
- Appendix B provides info on the processes and practices for framework updates

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

2 RISK ASSESSMENT FRAMEWORK DEVELOPMENT

The work performed in T4.3.1 is made of three main activities:

- **Backbone Model Consolidation**: Two Backbone (BB) models were developed in WP4.2 for Runway Excursion at landing and for Mid-Air collision en-route. They follow the same general principles: they are based on generic contributors and they identify safety barriers and their failures. Additionally they provide a means to compute the probability of several safety indicators. Yet, both backbones were developed separately and there are differences in their description and the way they compute safety indicators. The consolidation activity includes works that :
    - **Backbone Model alignment**: align the two BB models so that they are described using the same kind of format and they use the same approach to compute safety- indicators and show that this approach is applicable to other risks categories (CFIT, runway incursion, etc.).
    - **Influencing Factors**: include the influencing factors in the BB models and in the computation of safety indicators;

- **Integration of domain specific risk models into the backbone model**: during WP4.2 it was demonstrated how to integrate the results from the specific models into the Backbone models. This was done in slightly different ways for the ANSP domain specific model and for the Aircraft domain specific model. The qualitative and quantitative integration of domain specific risk models needs to be harmonized. This activity covers the following work:
    - **Harmonized Formats**: propose harmonized formats for integrating results from domain specific models into the BB models,
    - **Conversion Rules**: establish conversion rules between the various units used in computations in the different domains,
    - **Common Causes**: define ways to deal with potential common causes between different domains.

- **Software aspects of the Integration of the backbone model into the Risk Observatory**: Currently the Backbone models are manually developed as standalone excel files that cannot easily be integrated in a web-based architecture for the Risk Observatory.
    - **Software architecture :** propose a software architecture that enables the integration of the backbone models in a web-based implementation of the Risk Observatory;
    - **Guidance for the inclusion of Backbone models into the Risk Observatory:** explain how to use existing tools to implement the integration of the Backbone models into the Risk Observatory implementation.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

2.1. Backbone Model Consolidation

2.1.1. Alignment of Backbone Models

The Backbone models developed during WP4.2 for Runway Excursion at landing and for Mid-Air collision en-route were based on existing AIM- [6],[31] and CATS models [7]. At the top level of description, both models use an Event Sequence Diagram (ESD) to describe how the occurrence of generic contributors and safety barrier failures can lead to an accident or serious incident situation. At other levels of description both models use the fault tree notation to describe the relations between root causes and barrier failures.

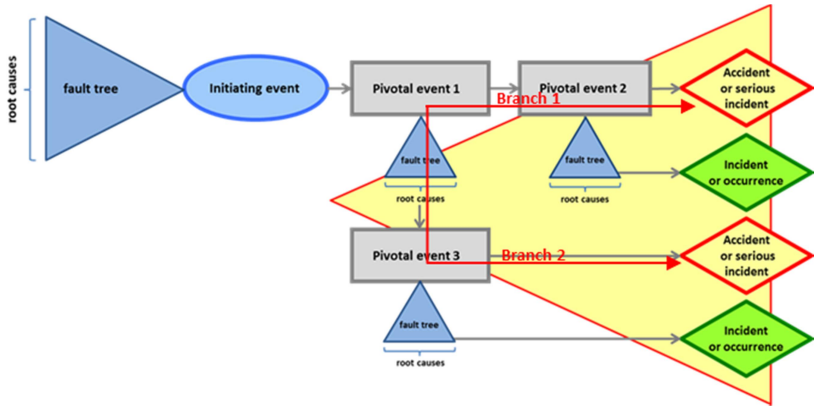


Figure 2-1: CATS Event Sequence Diagram

A positive aspect of the Event Tree notation is that it is easy for a non-specialist to read and understand the scenarios described by an event sequence diagram and to validate the models. One limitation of the Event Tree notation is related with the management of the combinations of events, a large number of initiating events or external conditions and therefore a large number of branches in the ESD make it difficult to read and validate the ESD. For instance, the AIM model for runway excursion is more difficult to understand than the MAC ER model. This is due to the fact that the runway excursion takes into account combinations of weather condition, runway suitability and quality of the approach. One way to overcome this limitation is to split the model into several related ESDs, this is the approach followed by the CATS model. For instance, in CATS several ESDs relate with runway excursion: ESD-19 “Unstable approach”, ESD-23 “Windshear encounter”, ESD-25 “A/C handling during flare inappropriate”, ESD-26 “A/C handling during landing roll inappropriate”, ESD-28 “Single engine during Landing”, ESD-29 “Thrust-Reverser Failure” and ESD-30 “A/C encounter unexpected wind”.

In the Risk Observatory it is the intention to combine risk models in order to compute safety indicators. It was shown during WP4.2 that domain specific models for the ground segment of the ANSP domain and for the Aircraft manufacturer domain could be described as fault-trees. It is considered that in the RO it would be simpler to describe all the models at all levels of description using the fault-tree notation. Modern fault-tree tools are able to deal with fault-trees including negations and multiple top-level events.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU’s Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

This makes it possible to easily translate the ESD into a fault-tree. The following figure gives a fault-tree describing the previous ESD. It should also be possible to build a fault tree that collects information from various ESD leading to the same type of accident or incident. Consequently, it should be possible to describe AIM and CATS models as fault-trees.

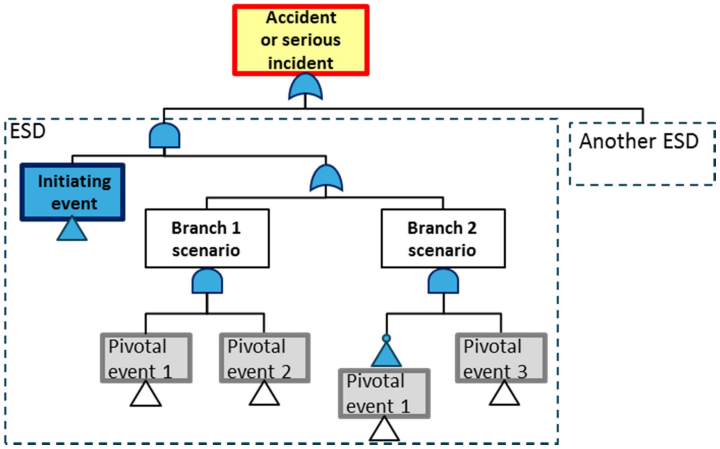


Figure 2-2: Description of a ESD as a Fault Tree

The MAC-ER and the Runway Excursion Backbone models were described as fault-trees. The following figures provide several views of the MAC-ER fault-tree:

- A top-level view describing scenarios leading to Mid-Air Collision. This fault tree does not detail the situations leading to the failure of barriers such as “31 – Airborne Collision Avoidance”, “32 – ATC collision prevention”, etc.;
- Another top-level view describing scenarios leading to near mid-air collision;
- A Lower level view describing the scenarios leading to leading to the failure of the barrier “31 – Airborne Collision Avoidance”. This fault-tree does not detail the situations leading to the Generic Contributors such as “31.1 - No ACAS RA or provided late”, “31.2 – Inappropriate Crew response to RA”, etc.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU’s Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

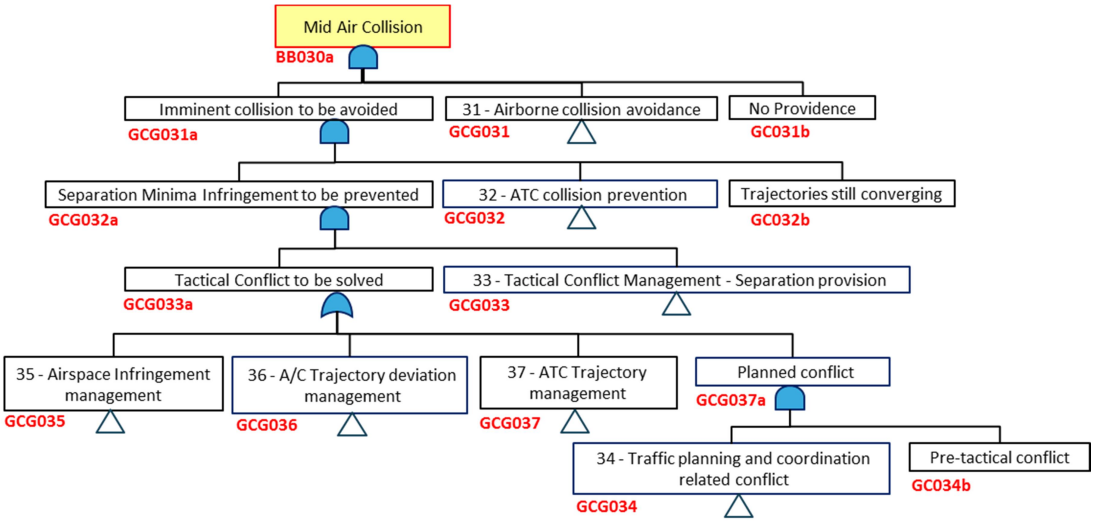


Figure 2-3: A Fault Tree description of Mid-Air Collision (Top Level View)

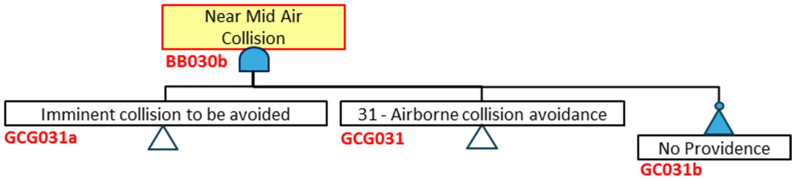


Figure 2-4: Fault Tree description of Near-Mid Air Collision (Top Level View)

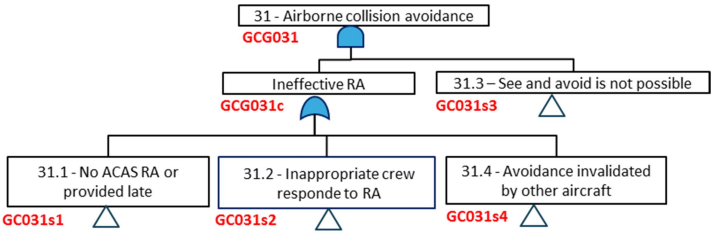


Figure 2-5: Fault Tree description of scenarios leading to the failure of a Barrier

In appendix A-1, the full description of the MAC-ER and RWY-Excursion are provided as fault-trees.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Review of the suitability of the Backbone model approach to deal with other risk categories

In order to show that the proposed Backbone model approach is applicable to other risks categories (CFIT, runway incursion, etc.), CATS and AIM models were reviewed.

Review of CATS models:

CATS models, see [7], contain 33 different generic accident scenarios covering all accident types. As has been described previously, it should be possible to collect the branches in all the ESDs leading to a given category of accident and build a fault-tree using the information found in each branch.

Describing the ESDs as fault-trees is interesting if there are domain specific models that can also be described as fault-trees. Three ESDs have been identified for which the relevant domain specific models would not be described as fault-trees:

- ESD-11 “Fire on Board aircraft”, this ESD contains pivotal event “Fire propagates”. Physical fine grain models are used to analyze the propagation of fire on board the aircraft instead of a fault-tree model;
- EDS-15 “Anti-ice/de-ice system not operating”, the initiating event is “Ice accretion on aircraft in flight”, a physical model for ice-accretion would be used to study this scenario;
- ESD-33 “Cracks in aircraft pressure cabin”, this ESD contains pivotal event ““Explosive decompression”, again a physical model would be used to analyse this scenario.

Review of AIM models:

AIM [6], [31] currently has models for MAC (with en-route, TMA and oceanic versions), runway Incursion model, CFIT model, wake turbulence and taxiway accident. As in the case of CATS models, AIM models can be transformed into backbone models.

The conclusion is that most of the AIM and CATS models are compatible with the Backbone model approach proposed in WP4.2. In particular it should be feasible to capture as fault trees other AIM and CATS models than the MAC en-route and Runway Excursion at Landing and include the captured fault-trees in the RO.

2.1.2. Influencing Factors

Definition of the Influencing Factor (IF).

The Influencing Factor (IF) is an element that may affect the frequency of occurrence of one or several contributor factors to precursors[1] involved in a given risk. An influencing factor does not increase the safety severity. Refer to EASA CS25.1309, see [8], for the definition of the severity levels for large aeroplanes). It will only increase its rate of occurrence.

[1] Precursors are hazardous situations as a result of the exposure to a barrier or as a result of a lack of barrier efficiency

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU’s Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Examples:

- The loss of aircraft deceleration at landing resulting in an overrun speed > 60 kt is classified CATASTROPHIC independently from the influence of the runway state, the weather conditions and flight crew fatigue or lack of flying experience.
- A strong tail wind combined with a contaminated runway (RWY) will increase the probability of experiencing a runway excursion, not the severity of the RWY excursion

An influencing factor never directly leads to a risk otherwise it would be a contributing factor[2].

IF's can influence several Contributing Factors or Precursors involved in a risk. Moreover, the same IF can be considered in several risks as depicted in the following figure (risk of RWY excursion and risk of MAC).

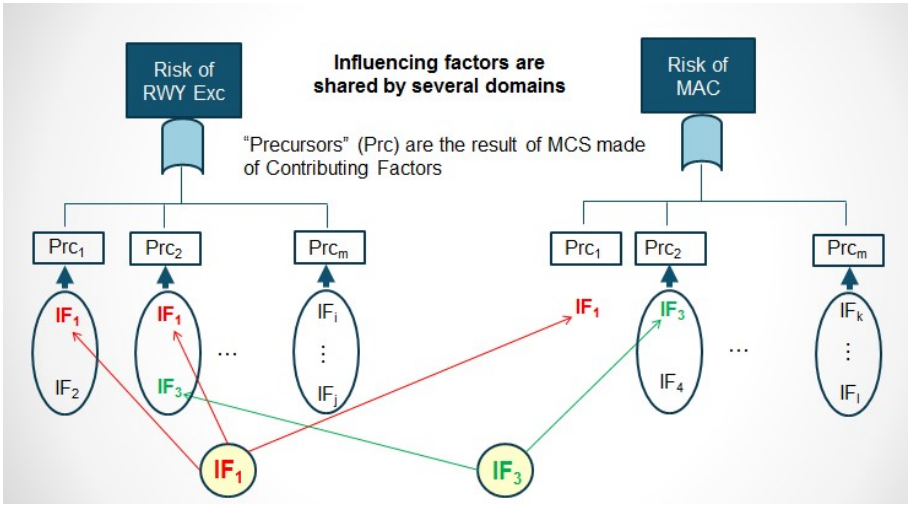


Figure 2-6: Influencing Factors involved in more than one risk

Cluster of Influencing Factors

Influencing Factors are grouped in clusters, for example the IF related to "weather conditions" as depicted in the following table. This cluster gathers several IF's that reflect the influence of various possible bad weather conditions.

501	Weather
501.1	Storms, rain, rainfall
501.2	Tailwind, headwind
501.3	Crosswind
501.4	Windshear / Turbulence
501.5	Ceiling - Visibility
501.6	Wake turbulence (note manageable in the models)

Table 1: Influencing Factors related to cluster "Weather"

[2] The definition of Contributing Factor can be found in Appendix B "System Requirements Vocabulary" of deliverable D4.4.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

In the frame of the P4 project, a table of IF's has been structured in clusters. See Appendix A of D4.4 for details.

Most IF's are linked to Contributing Factors related to human errors (flight crew errors, ATCO errors) since they can increase their workload[3] or stress and consequently increase the frequency of a risk. Influencing Factors like IF_503.2 'Flight Crew Fatigue' or IF_503.4 'Crew response to failures' are typically associated with crew errors; however IF's can also be allocated to technical contributing factors.

Characteristics of the Influencing Factors

Each influencing factor is defined by:

- A reference number (e.g. 500.1 related to IF 'Runway surface quality' that belongs to cluster "Runway characteristics")
- A title (e.g. 'Runway surface quality')
- Attributes:
    - Set of values (e.g. 'dry', 'wet', 'flooded')
    - Estimated weight and rate of occurrence for each IF value.

As an example, the **set of values** associated to the IF "Runway surface quality" has been defined according to ICAO Annex 14 requirements [29]:

RWY-SURF	Surface property
Poor	Does not respect ICAO Annex 14 requirements Deteriorated pavement Deteriorated braking action, poor draining when wet
Good	Fully in line with ICAO Annex 14 requirements Good draining and braking efficiency when wet

Table 2: Value associated to IF "Runway surface" as per ICAO Annex 14

The **weight** allocated to each value of an Influencing Factor can take the following numerical values:

- Weight equal to 1 (neutral impact). This value can be attributed to some Influencing Factor if an actual value cannot easily be determined from in-service reportable occurrences or if the RO user doesn't want to consider the influence of such an IF in the risk modelling processing.
- Weight value > 1 represents an adverse impact, which the most common case of a large majority of IF's.

Note: A positive weigh value < 1 represents a beneficial effect. This is typically the case of a positive taxiway slope that can contribute in slightly decelerating a taxiing aircraft given the slow speed during

[3] This increase of flight crew workload is not yet considered in the risk classification (e.g. slight increase in flight crew workload is one criteria associated to MINOR safety consequences while excessive flight crew workload is one criteria for HAZARDOUS severity) because here the workload must be taken as a potential cause (i.e. contributor) of the considered risk and not as a consequence of the risk itself like for example "RWY excursion at speed > 60 kt", which is CATASTROPHIC.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

taxi. This is not valid for higher ground speeds on the runway at landing. Therefor concerning the safety scenario related to the risk of "longitudinal runway excursion", such a positive influence is insignificant given the A/C ground speed of the aircraft at landing and the kinetic energy.

Concerning IF 503.1 related to the Flight Crew Experience, it has been considered that a Good F/O crew experience has been assigned a weight of 1 while a Good Captain experience IF weigh has been set by default to 0.9, which represents a positive influence on the linked contributing factors. Here again good captain flying experience can be considered by some airlines as the 'nominal' profile and thus having a weight of 1. The US Airways Flight 1549 where an Airbus A320 successfully made an emergency landing on the Hudson River in January 2009 is an isolated case where the profound experience of the captain has probably played a positive role.

For simplicity such a category of weigh in the model will not be used although positive weights < 1 could be used in the models; this is not seen as a limitation of the methodology.

Weights can be deduced from national or international databases related to major safety risks in aeronautics (e.g. ICAO – ADREP).

The **rates of occurrence** can be estimated from local databases of flight data (e.g. AirFase tool). These rates of occurrence are average values.

Example – IF ref. 500.6 RWY Visual Path Guidance

IF 500.6 - RWY Visual Path Guidance	Definition	IF 500.6 Weight	IF 500.6 Rate (Airline data)
Good	Well-calibrated PAPI, in accordance with available instrument approaches	1	85%
Medium	Visual aid other than PAPI Poorly calibrated PAPI PAPI position/angle discrepancy with available instrument approaches	1.1	10%
Poor	No visual aid	1.2	5%

Table 3: Weights and rates of occurrences of IF 500.6 'RWY VPG'

Good RWY VPG is the nominal Visual Path Guidance; therefore the associated weight has been set to 1.

The associated (estimated) rate of occurrence depends on the airport location. On the majority of airports the VPG is a calibrated PAPI (Precision Approach Path Indicator) while for some of them the VPG does not rely on PAPI (10% of the airports on average). Lastly, it has been assumed that only 5% of the airports don't have any visual aids. All these rates must be refined based on actual figures that is dependent on each an airport.

Note: The rate of occurrence could be replaced by an estimated probability or a range of estimated probabilities. However, this possibility has not been implemented in the current version of the RO prototype.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

'Rectified' weight of Influencing Factors

The 'rectified' weight of an Influencing Factor, noted as IF_{RW} , is the weight of the IF which considers the weight of each value that the IF can take, weighted by the associated rate of occurrence. The rectified weights can be considered as 'coefficients'; the failure rate of the GCF's affected by such IF's will then be multiplied by these coefficients. See paragraph on "Computing a risk in the Backbone model by taking into account considering the Influencing Factors".

The way the calculation of the numerical value of a rectified weight is made is illustrated by the following example involving two IF's: IF_1 related to 'Runway state' and IF_2 related to 'Tail wind'. The two tables below provide the associated rates of occurrence and weights for IF_1 and IF_2. Such values are provided only as an example and do not reflect actual values.

IF1 - RWY State	IF1 Weight	IF1 Rate
Dry RWY	1	65%
Wet RWY	1.1	20%
Ice/ flooded RWY	1.2	15%

IF2 - Tail wind	IF1 Weight	IF1 Rate
No wind	1	70%
Low wind (≤ 5 kt)	1.1	10%
Strong wind (> 5 Kt)	1.5	20%

Table 4: Tables rates and weights for IF_1 and IF_2

Notation:

$IF_{1\,RW}$ refers to the rectified weight of Influencing Factor IF_1. Similarly, $IF_{2\,RW}$ refers to the rectified weight of Influencing Factor IF_2.

Considering the example of IF_1, "Runway state", it is found that:

- $IF_{1\,RW}$ = (65% dry RWY) + (20% wet RWY) + (15% flooded RWY).

Considering the weight of each possible RWY state:

- $IF_{1\,RW}$ = (65% x 1) + (20% x 1.1) + (15% x 1.2) = 0.65 + 0.22 + 0.18 = **1.05**

Similarly, from the previous table dealing with IF_2 related to "Tail wind":

- $IF_{2\,RW}$ = (70% x 1) + (10% x 1.1) + (20% x 1.5) = 0.7 + 0.11 + 0.3 = **1.11**

Computing a risk in the Backbone model by considering the IF's

The computation of a risk *R* in the backbone model will consider the effect of the Influencing Factors linked to each Contributing Factor involved in the minimal cut sets (shortest combinations of contributing factors leading the risk). The first step consists of calculating the rectified weight as previously explained by using the IF characteristics (rates of occurrence and weights) stored in the RO database.

The computation of a risk *R* considering the effect of the involved IF's can only be made at the level of the backbone model for the following reason: For lack of write-access grants, the RO users might not be allowed to modify the domain specific safety models. This is the case when the owner of such domain

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

specific safety models does not want to make them "open source". Therefore, if the RO users want to replace the default values of the IF characteristics with their own set of parameters, this cannot be done at the level of the domain specific safety model.

The methodology used to compute a risk *R* (or a precursor) in the backbone model by considering the effect of the Influencing Factors is illustrated below.

The link between each GCF and one or several IF's must be defined. Such a link is defined in a mapping table (see Appendix A.2 for details).

In the calculation of the Minima Cut Set (MCS) involving the IF's linked to each GCF, it has been assumed that all IF's are independent of each other. However, some dependence can refute this assumption as for example:

- Runway surface condition and weather
- Ceiling/ visibility and weather
- Ceiling/ visibility and lighting
- Flight crew fatigue and flight crew response to failure

Since it is very difficult to estimate the level of dependence between two IF's it has been considered that they are all independent. This assumption is acceptable because it leads to a conservative calculation of the probability of the risks. To avoid such dependence issue, dependent IF's linked to a GCF in the mapping table of GCF's have been excluded. In the example in the following table, IF_1 and IF_2 cannot be dependent. Therefore, the combination of IF 502 'Runway surface condition' and IF 501 'weather' linked to GCF_1 is not allowed. If these two IF's are assumed to be potentially linked to GCF_1 then it is up to the RO user to select the most significant one. This choice may depend on the numerical values of the rectified weights of the two IF's which themselves depend on the weights and the rates of occurrences.

The assumption made on the independence of the linked IF's enables the multiplication of a GCF affected by several IF's by their rectified weights.

As an example, If CGF_1 is mapped with IF_1 and IF_2 then CGF_1 will be weighted by $IF_{1\ RW}$ x $IF_{2\ RW}$

If CGF_2 is mapped only with IF_2 then CGF_1 will be weighted $IF_{2\ RW}$

GCF's	Linked IF's	
GCF_1	IF_1	IF_2
GCF_2	IF_2	-

Table 5: Mapping table between GCF's and of IF's

Let's consider MCS_1 the MCS of order 2 that is made of GCF_1 ^ GCF_2

- Without considering the influence of the two IF's, $P(MCS_1)$ would be equal to $P(GCF_1)$ x $P(GCF_2)$
- When considering the influence of the two IF's,

  $P(MCS_1) = IF_{1\ RW}$ x $IF_{2\ RW}$ x $P(GCF_1)$ x $IF_{2\ RW}$ x $P(GCF_2)$.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

The RO user can disregard the influence of the IF's in the calculation of the MCSs by modifying the default mapping and removing all the 'non-modelled, or non-existing' links between each GCF and their 'IF's as illustrated in the following table.

GCF's	Linked IF's	
GCF_1	-	-
GCF_2	IF_2	-

Table 6: Modified mapping table between GCF's and of IF's

If the RO user is unable to set relevant (actual) rate of occurrences associated to each parameter of an IF, then they can modify the table of weights and rates of occurrences associated to this IF as illustrated in the following table. Because of this operation $IF_{1\ RW}$ = 1 (neutral effect). Consequently, $IF_{1\ RW}$ x $P(GCF_1)$ = $P(GCF_1)$

IF1 - RWY State	IF1 Weight	IF1 Rate
Dry RWY	1	65%
Wet RWY	1.1	20%
Ice/ flooded RWY	1.2	15%

⇨

IF1 - RWY State	IF1 Weight	IF1 Rate
Dry RWY	1	100%
Wet RWY	1.1	0%
Ice/ flooded RWY	1.2	0%

Table 7: Default and Modified Table of rates and weights for IF1

If the numerical values of $IF_{1\ RW}$ and $IF_{2\ RW}$ as previously calculated are used ($IF_{1\ RW}$ = **1.05** and $IF_{2\ RW}$ = **1.11**) then:

$P(MCS_1) = IF_{1\ RW}$ x $IF_{2\ RW}$ x $P(GCF_1)$ x $IF_{2\ RW}$ x $P(GCF_2)$ = 1.05 x 1.11 x $P(GCF_1)$ x 1.11 x $P(GCF_2)$ = 1.16 x $P(GCF_1)$ x 1.11 x $P(GCF_2)$

IF parameters to be provided to the Backbone model.

For each IF, the following parameters must be provided to the backbone model in addition to the MCSs or any other safety outcome from the domain specific models:

IF_i {Ref IF_i, Title IF_i, $IF_{i\ RW}$}, where $IF_{1\ RW}$ is the rectified weight deduced from the various values of weight and linked probability of occurrences as previously detailed.

These values are stored in the RO database and can be modified by the RO users. Default values will be provided for each IF. A Graphic User Interface might be developed in the 'end product' version of the RO to give the user the possibility to change the values of weights and rate of occurrence of each IF.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

2.2. Integration of domain specific risk models into the backbone model

2.2.1. Harmonized Formats

The integration of domain specific risk models into the backbone model requires the use of a common model description format. During WP4.2, it has been shown that domain specific models could be integrated in the Backbone models as fault-trees describing the occurrence of Generic Contributors. In order to facilitate this integration, it is important to structure the fault-tree representing the Backbone model in a certain way.

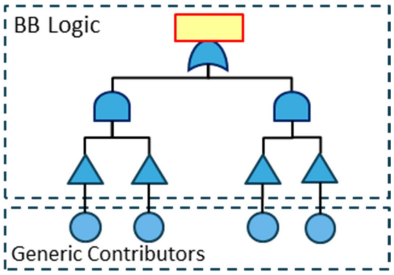


Figure 2-7: Modular description of the Backbone model

The previous figure shows a modular description of the Backbone model where one module (named BB Logic in the figure) describes the logical structure of the Backbone model and the second module (named Generic Contributors in the figure) describes the probabilities of the basic events of the Backbone fault-tree. This modular description that separates the logical description of the Backbone from its quantitative description enables the ability to easily change the probabilities of the generic contributors. This is useful when the computation of the probabilities of the accident/incidents described by the Backbone for several possible probabilities of the generic contributors is desired.

Moreover, the modular description makes it possible to integrate the domain specific models into the Backbone model. The following figure shows the integration of two domain specific models (named Domain1 and Domain2) into the Backbone model.

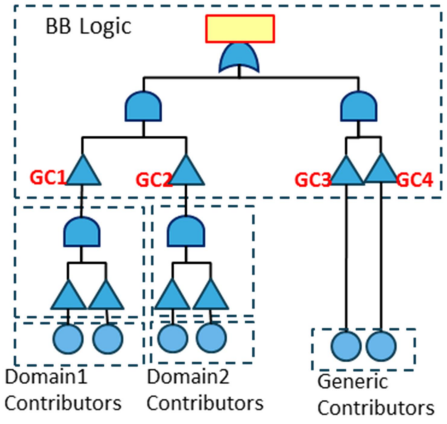


Figure 2-8: Integration of Domain1 and Domain2 specific models into the Backbone model

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

In the previous figure, the Backbone model has four generic contributors GC1, GC2, GC3 and GC4. In the integrated model, generic contributor GC1 (resp. GC2) is connected to a fault-tree that relates this contributor with domain specific contributors in Domain1 (resp. in Domain2). The two other Generic contributors (e.g. GC3 and GC4) are not connected to a domain specific fault-tree. Again, it is proposed to split the domain specific fault-trees into two modules: one module that describes the logic of the domain specific model and the other module that describes the probabilities of the domain specific contributors.

The following section explains how the modular description of fault trees can be implemented using the open PSA format.

The Open PSA Format

The Open PSA format, see [9], is an XML format that describes Fault Trees. It is used by several tools as a model interchange format. Translators between Open PSA and the internal formats of industrial tools such as RiskSpectrum® and CAFTA® exist. Open PSA format is also the native format of open source tools such as XFTA or SCRAM, see [12] respectively [30].

Considering again the fault-tree that describes the MAC-ER backbone model. In the following figure a fragment of the fault-tree is shown where intermediary node "Imminent collision to be avoided" is not expanded whereas the intermediary node "31 – Airborne collision avoidance" is expanded.

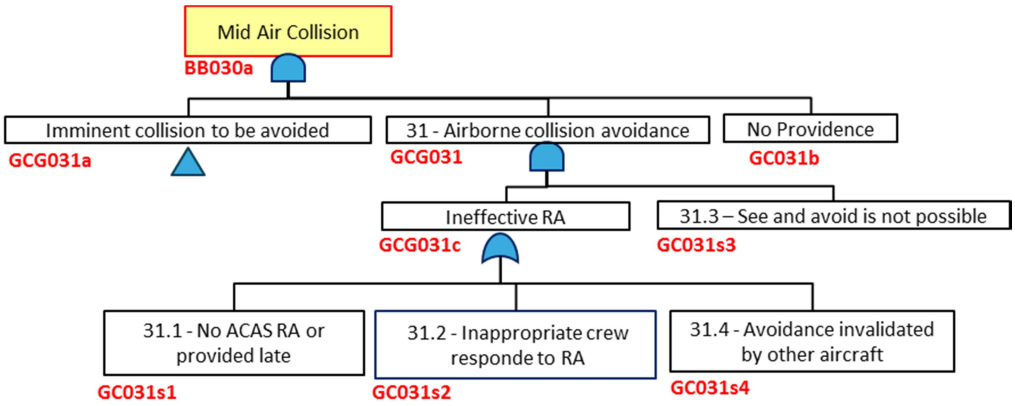


Figure 2-9: Fragment of the MAC Backbone model Fault Tree

This fault-tree is represented by two open-PSA files. The first file describes the logical structure of the fault-tree. The following figure gives a fragment of this file. Each gate of the fault-tree is defined using a <define-gate> tag. The gate is uniquely identified by its name. The naming convention that has been used for the gates is as follows:

- BB*NNN*nn for top level nodes where *NNN* is the identifier of the risk (030 for MAC-ER and 000 for Runway Excursion) and nn is identifier of the top-level node (in the MAC-ER model, where use is made of "a" for "Mid Air Collision", and of "b" for "Near Mid Air Collision")

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

- GCG*MMM*nn for intermediary nodes where *MMM* is the identifier of the Generic Contributor Group (for instance, 031 for Airborne collision avoidance) and nn is an identifier in the Group (for instance a for “Imminent collision to be avoided”, c for “Ineffective RA”)
- GCMMMsK for basic events of the fault-trees representing Generic Contributors where K is the identifier of the contributor in its group (for instance 1 for “No ACAS RA or provided late, 2 fr “Inappropriate cress response to RA”, etc)

A label is associated with the gate using the <label> tag. The logical equation linking the gate with its lower level nodes is defined using a logical connector tag <and>, <or>, <not>, etc, the identifiers of the connected nodes use the <event> tag.

```
<?xml version='1.0' encoding='utf-8'?>
<open-psa>
  <define-gate name="BB030a">
    <label>Mid Air Collision</label>
    <and>
     <event name="GCG031a" />
     <event name="GCG031" />
     <event name="GC031b" />
    </and>
  </define-gate>
  <define-gate name="GCG031">
    <label>Airborne collision avoidance</label>
    <and>
      <event name="GC031c" />
      <event name="GCG031s3" />
    </and>
  </define-gate>
  <define-gate name="GCG031c">
   <label>Ineffective RA</label>
   <or>
     <event name="GC031s1" />
     <event name="GCG031s2" />
     <event name="GCG031s4" />
    </or>
  </define-gate>…
 </open-psa>
```

Figure 2-10: Open PSA description of Logical Structure of the MAC Backbone Model (Fragment)

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU’s Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

The second file defines the Generic Contributors of the fault-tree using the tag <define-basic-event>. Again, a unique identifier has to be used, a textual label can be associated to the Generic Contributor, and a probability value can associated to the contributor using the <float> tag.

```
<?xml version='1.0' encoding='utf-8'?>
<open-psa>
  <define-basic-event name="GC031b">
    <label>31.b - No Providence</label>
    <float value="0.001" />
  </define-basic-event>
  <define-basic-event name="GC031s3">
    <label>31.3 - See and avoid is not possible</label>
    <float value="0.7141" />
  </define-basic-event>
  <define-basic-event name="GC031s1">
    <label>31.1 - No ACAS RA or provided late</label>
    <float value="0.0755" />
  </define-basic-event>
 …
 </open-psa>
```

Figure 2-11: Open PSA description of basic events of the MAC Backbone Model (Fragment)

A fault-tree extracted from the Aircraft Manufacturer Domain Specific model that provides the Domain specific contributors for Generic Contributor 31.1, is considered below.

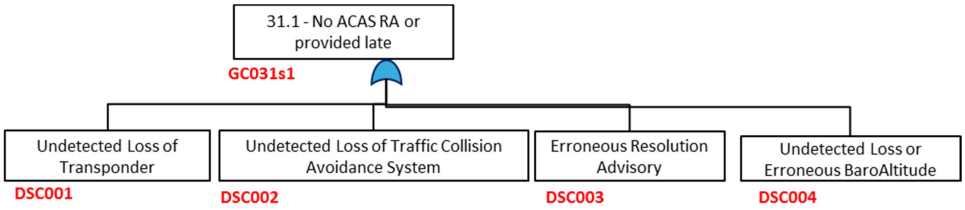


Figure 2-12: Domain Specific Fault-tree for Generic Contributor 31.1

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

The two files describing the fault-tree are given below.

```
 <?xml version='1.0' encoding='utf-8'?>
<open-psa>
  <define-gate name="GC031s1">
    <label>31.1 - No ACAS RA or provided late</label>
    <or>
     <event name="DSC001" />
     <event name="DSC002" />
     <event name="DSC003" />
     <event name="DSC004" />
    </or>
  </define-gate>
</open-psa>
```

Figure 2-13: Open PSA description of Domain Specific Model (Logical part)

```
<?xml version='1.0' encoding='utf-8'?>
<open-psa>
  <define-basic-event name="DSC0001">
   <label>Undetected Loss of Transponder</label>
   <float value="1.0e-05" />
  </define-basic-event>
  <define-basic-event name="DSC0002">
    <label>Undetected Loss of Traffic Collision Avoidance System</label>
    <float value="1.0e-05" />
  </define-basic-event>
  <define-basic-event name="DSC0003">
    <label>Erroneous Resolution Advisory</label>
    <float value="1.0e-05" />
  </define-basic-event>
```


This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

```
  <define-basic-event name="DSC0004">

    <label>Undetected Loss or Erroneous BaroAltitude</label>

    <float value="1.0e-07" />

</define-basic-event>

 </open-psa>
```

Figure 2-14: Open PSA description of Domain Specific Model (Quantitative part)

To integrate the Backbone model with this domain specific model the definition of basic event "**GC031s1**" from the Backbone fault-tree needs to be discarded and the definition of the gate "**GC031s1**" provided in the Domain specific fault-tree needs to be used instead. A similar operation can be performed for all generic contributors defined in a domain specific model.

In the special case where a generic contributor would be defined in several domains an adaptation layer has to be defined. The adaptation layer contains logical equations that relate the generic contributor with its contributors in the various domains.

Equivalent Tabular Format

As the Open PSA format is not easily readable by a human being, the information provided can also be described in an equivalent tabular format that could be opened by the excel tool. The fault-tree would be described by two tables: the define-gate table that describes the logic structure of the fault-tree and the define-basic-event table that describes the quantitative information. In the following the two tables that are equivalent to the Open PSA files for the MAC BB model are provided.

Name	Label	Gate	Event	Event	Event
BB030a	Mid Air Collision	and	GCG031a	GCG031	GC031b
GCG031	Airborne collision avoidance	and	GC031c	GCG031s3	
GCG031c	Ineffective RA	or	GC031s1	GCG031s2	GCG031s4
…					

Table 8: define-gate Table

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Name	Label	Probability
GC031b	31.b - No Providence	0.001
GC031s3	31.3 - See and avoid is not possible	0.7141
GC031s1	31.1 - No ACAS RA or provided late	0.0755
…		

Table 9: define-basic-event

2.2.2. Conversion Rules

This section starts by explaining the integration issue in BackBone (BB) models due to data units, then the methodology to solve this issue is presented, and lastly the conversion rules collected from partners' inputs are summarized.

2.2.2.1. Integration issue due to heterogeneity of data units

The contributor factors coming from different domains may have different units (e.g. Flight Hours on airborne side vs Controlled Flight Hours on ground side). It should be noted that this heterogeneity of baseline impacts both:

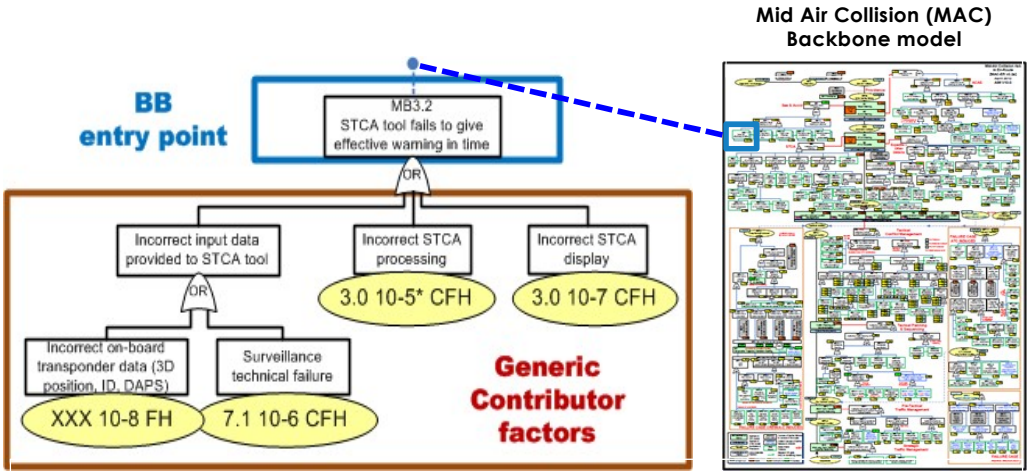
- quantitative data: e.g. failure rate of the precursors (expressed as MCSs in the domain-specific model that are then transmitted to the BB) and in the end, the feared event computed in the BB (risk index)) and,
- qualitative data (e.g. severity of a feared event).

From these observations, it is possible to identify an **integration issue** at BB model level. This integration issue is located:

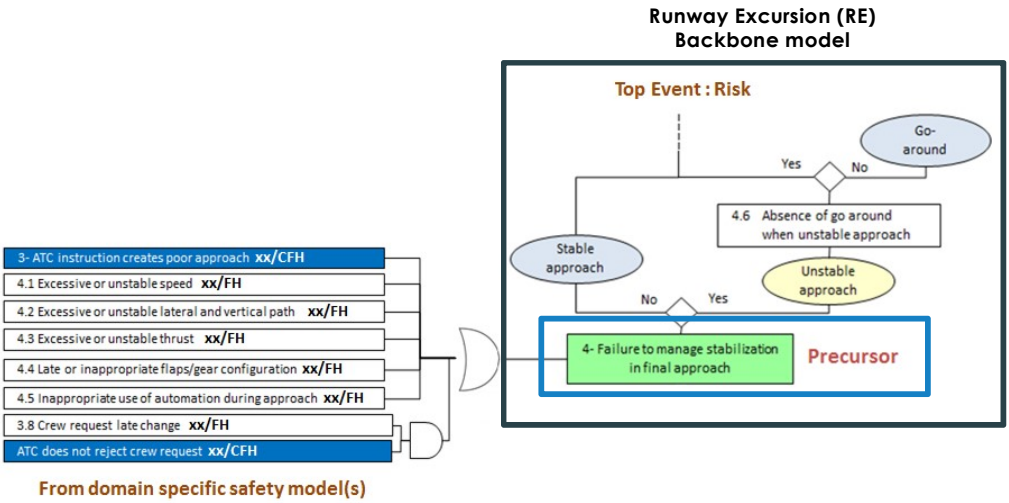
- at the generic contributing factors level for the risk index dashboard of the RO
- In the components computing KPIs directly from raw data (occurrences, FDM, etc.) for the occurrence dashboard of the RO

In Figure 2-15 below two examples of integration issue at the BB level are depicted. In Figure 2-15-(a), in the Mid Air Collision BB case, it is possible to observe in the red box that the specific contributing factors at aircraft level are expressed in Flight Hours (FH) and the specific contributors on Ground Equipment side are expressed in Controlled Flight Hours. These different units should be integrated into a common one at the generic contributing factors of the BB (blue box). In Figure 2-15-(b), in the Runway Excursion (RE) BB case, it is possible to observe generic contributors form ATC domain have estimated failure rates expressed in CFH while the other contributors coming from the Aircraft are expressed in FH.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.



(a) Integration issue at Mid Air Collision (MAC) BB level due to unit heterogeneity



(b) Integration issue at Runway Excursion (RE) BB level due to unit heterogeneity

Figure 2-15: Examples of integration issue at BB level due to unit heterogeneity

In the next section, the methodology to solve this kind of integration issues is presented.

2.2.2.2. Methodology to solve this integration issue

In the previous section, the integration issue due to the heterogeneity of data units (coming from different domains) has been presented and illustrated through examples. At the BB level, all the quantitative and qualitative values coming from various domain specific models must be expressed with the same reference unit, called 'target reference unit' in order to make the BB homogenous. The

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

conversion of specific units into the target one will be made by the BB. Therefore, the methodology proposed to solve this integration issue consists in 5 steps:

- 1st: Identify the main classes of data units to be used
- 2nd: Select the target reference units of BB models
- 3rd: Specify the integration & conversion functions
- 4th: Implement & validate a common library of conversion functions
- 5th: Provide to RO users a capability to add new conversion functions if needed

The three first steps are part of WP 4.3.1 and are detailed below. The two last steps (4th and 5th) will be handled within WP4.4. As depicted in the diagram below, the implementation of the integration and conversion functions will be done, either:

- in a specific Data Integration Engine (DIE) for the computation of the Risk Index, or
- directly in the Occurrence Dashboard components

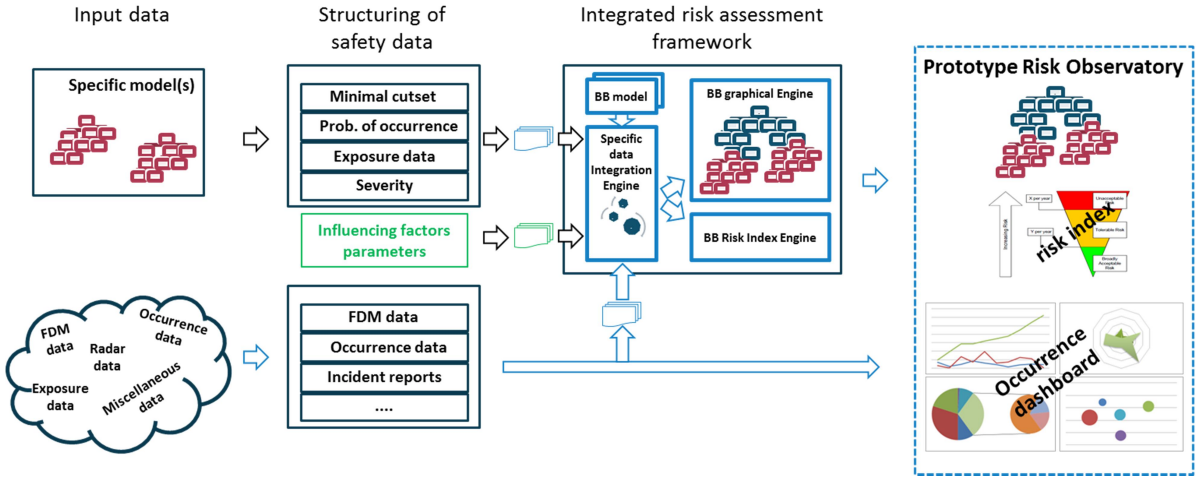


Figure 2-16: Illustration of the integrated risk assessment framework

2.2.2.3. Identification of the main classes of data units used in the RO

The identification of the main classes of data units to be used within the RO are collected from all partners of the FSS P4 project. A database is built with all data gathered during this data collection process. The structure of this data is described in the table below.

Domain	Input data	Type	Initial unit
Aircraft Manufacturer	Probability of occurrence	Likelihood	Flight
ANSPs	Probability of occurrence	Likelihood	Controlled flight hours per sector
XXXX	XXXX	XXXX	XXXX

Table 10: Data structure of the main classes of data units

The final table is provided in Appendix A.3.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

2.2.2.4. Target reference units of BB models

Target reference units are the means used to ensure data unit homogeneity in BB models provided that a library of appropriate conversion functions is available to convert native data units into target reference units. Indeed, the homogeneity in BB models relies on this set of conversion rules to ensure that the computations made in the BB are done with a single unit reference (target reference unit).

The figure below illustrates this concept of target reference units for the MAC BB.

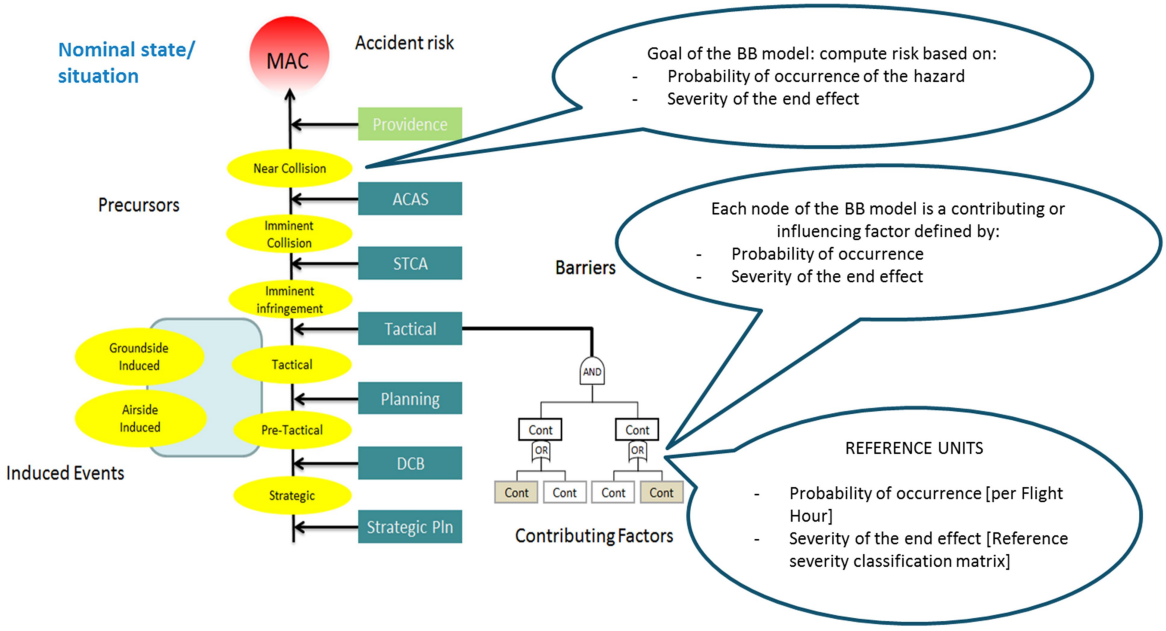


Figure 2-17: Illustration of BB target reference units

Following a brainstorming of the FSS P4 partners, the following target reference units have been selected for the different nodes of BB models:

- Probability of occurrence in [Flight hour] as the aircraft-centric approach is the most appropriate to federate the different domains represented in FSS P4
- Generic severity classification scheme with 5 levels: from level 1 (most severe) to level 5 (less severe)

This generic severity classification scheme should be mapped in the risk observatory according to the user profile (or on user request) to:

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

a) ICAO safety risk severity table in Safety Management Manual – Doc 9859 3rd edition (2013), see [2].

Severity	*Meaning*	*Value*
Catastrophic	— Equipment destroyed — Multiple deaths	A
Hazardous	— A large reduction in safety margins, physical distress or a workload such that the operators cannot be relied upon to perform their tasks accurately or completely — Serious injury — Major equipment damage	B
Major	— A significant reduction in safety margins, a reduction in the ability of the operators to cope with adverse operating conditions as a result of an increase in workload or as a result of conditions impairing their efficiency — Serious incident — Injury to persons	C
Minor	— Nuisance — Operating limitations — Use of emergency procedures — Minor incident	D
Negligible	— Few consequences	E

Table 11: ICAO safety risk severity table from SMM

b) ATM/CNS ground severity matrix coming from the Commission Implementing Rule (EU) N° 1035/2011.

Severity class	Effect on operations
1 (Most severe)	Accident as defined in Article 2 of Regulation (EU) No 996/2010 of the European Parliament and of the Council (1).
2	Serious incident as defined in Article 2 of Regulation (EU) No 996/2010.
3	Major incident associated with the operation of an aircraft, in which the safety of the aircraft may have been compromised, having led to a near collision between aircrafts, with ground or obstacles.
4	Significant incident involving circumstances indicating that an accident, a serious or major incident could have occurred, if the risk had not been managed within safety margins, or if another aircraft had been in the vicinity.
5 (Least severe)	No immediate effect on safety.

Table 12: EU safety risk severity table from CIR (EU) 1035/2011

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

c) Airborne Certification Specification and AMC for Large Aeroplanes Amendment 20

Severity of the Effects	Effect on Aeroplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
	Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
	Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Classification of Failure Conditions		No Safety Effect	Minor	Major	Hazardous	Catastrophic

Table 13: EASA safety risk severity table from CS-25

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

2.2.2.5. Specification of the conversion functions

The structure of the specification of the conversion functions is described in the table below.

Parameters	Conversion function	Reverse conversion function	Comment
param1 = … param = …	P [per flight hour] = f(P[per Initial Unit], param1, param2,…)	P[per Initial Unit] = f^{-1}(P[per flight hour], param1, param2,…)	Free text

Below an example of functions to convert probability of occurrence [per flight] and [per controlled flight hours per sector] in the target reference unit [per flight hour] and vice-versa.

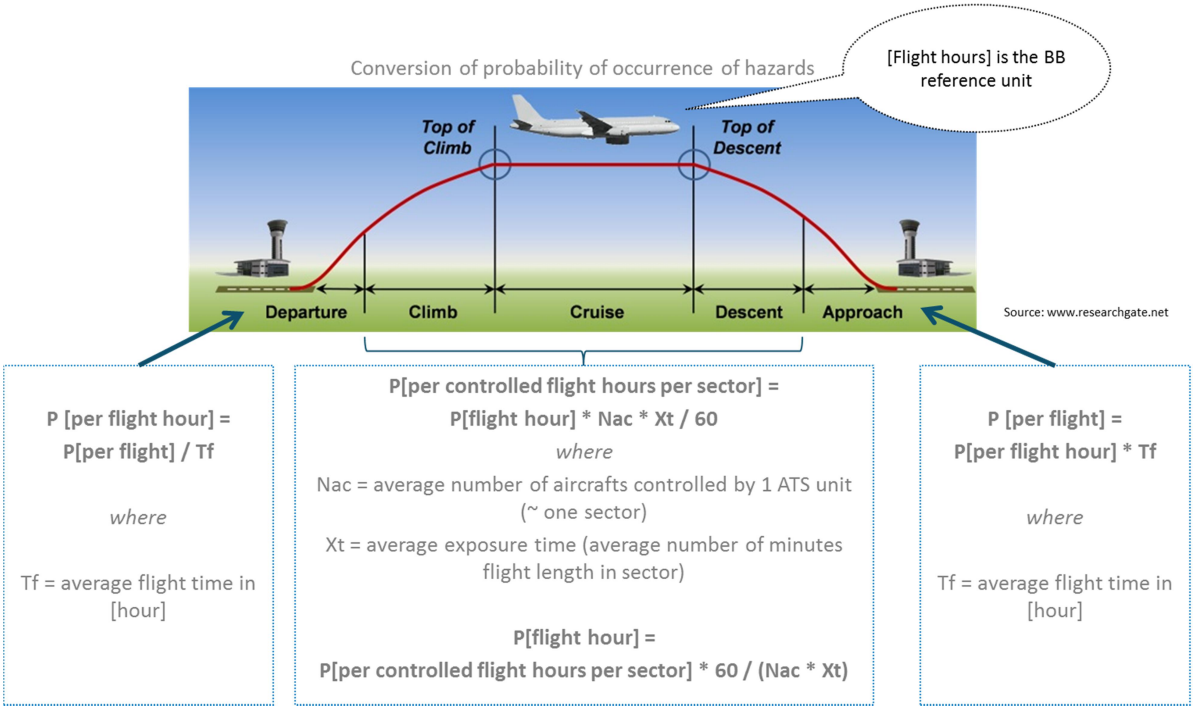


Figure 2-18: Illustration of conversion functions

Note: "Nac" is a number of A/C but it should be interpreted as the capacity of the sector during one hour of control (i.e. a number of flights per hour sector capacity).

Let's take an example by considering the use case of ED-161 (edition 2009, §. A.4.2.2 Traffic Characteristics, page 77, see [11]) related to En route airspace for High density traffic.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Consider that longitudinal separation between 2 successive a/c on the same track is in average equal to 5 min. So during 1 hour [T0, T0 +60 min], this will provide:

- T0 1st group of 5 a/c entering at the same time in the sector
- T0 + 5 min 2nd group of 5 a/c entering at the same time the sector
- T0 + 10 min 3rd group of 5 a/c entering at the same time the sector
- …
- T0 + 55 min 12th group of 5 a/c entering at the same time the sector

In the figure below is represented this traffic.

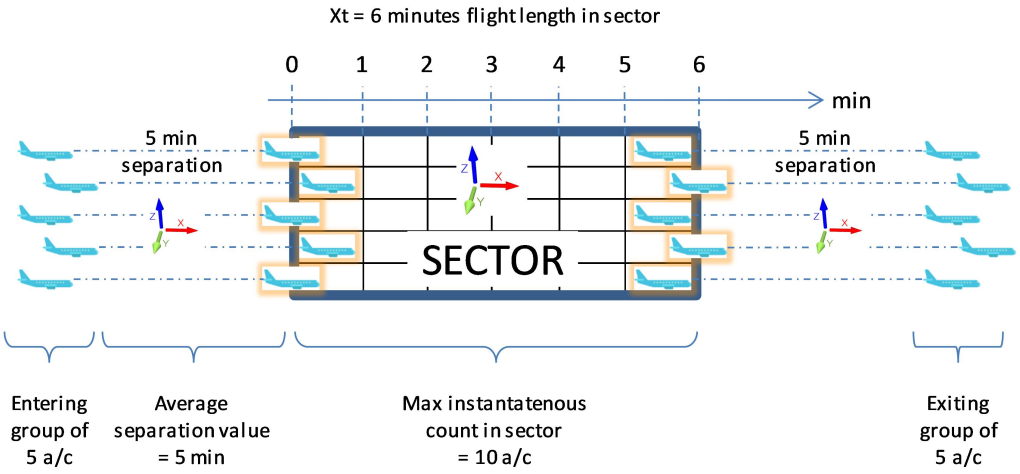


Figure 2-19: Conversion functions

In our FSS case: P_per_FH = P_per_CFH * 60 / (60 *6) = P_per_CFH / 6 (for En Route High Density)

The next steps in the implementation of the FSS Risk Observatory will be to implement & validate a common library of conversion functions, and to provide to Risk Observatory users a capability to add new conversion functions if needed.

The final table is provided in Appendix A.3.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

2.2.3. Common Causes

In this section, the issues related with Common Causes are explained. In fault-trees, the basic events are supposed to occur independently one from the other. But this assumption is not always true because, for instance, two basic events representing the same contributor could be labelled differently. These two basic events should not be considered as independent. There is a common cause failure that could lead to the simultaneous occurrence of these basic events. Common causes have an impact on the computation of safety index as they decrease the size of the minimal cut sets and they increase the probability of the top level event of the fault-tree. This could be an important issue for the Backbone models. In a paper [10], published at the ICRAT 2016 conference, authors S. Noh and J. Shortle studied the impact of common causes on ISAM models that are very similar to the CATS and AIM models. They showed that, in the worst-case, taking into account common causes could lead to an increase of the computed Risk Index by a factor 1000.

In our models common causes can be found either between generic contributors or between domain specific contributors. In the MAC-ER Backbone model, there are several generic contributors labelled "Communication issues". It is likely that generic contributors "32.5 - Communication issues - technical Airborne", "33.5 - Communication issues - technical Airborne" and "37.3 - Communication issues - technical Airborne" do not occur independently because the same Aircraft system is used to support all the air ground communications. Consequently a failure of this system will lead to the occurrence of the three generic contributors. A review of generic contributors of the Backbone models should be performed in order to identify potential common causes.

It could also be the case that common causes lead to the simultaneous occurrence of various domain specific contributors. As domain specific models are developed by various partners, it is likely that similar contributors are labelled with different names in different domains. For instance, the failure of an aircraft transponder is labelled "Undetected Loss of Transponder" in the aircraft manufacturer model whereas it is labelled "Transponder failure" in the ATM model.

Two approaches to deal with common causes were considered. The first one is based on the definition of Common Cause Groups that group together all contributors that are supposed to occur simultaneously.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

The Open PSA syntax for Common Cause group is the following:

```
<define-CCF-group name="Communication Issues – Technical airborne" model="beta-factor" >
 <members><basic-event name="GC037s3" /> <basic-event name="GC033s5" > <basic-event name="GC032s5" > </members>
 <factors><factor><float value="0.6" /></factor></factors>
 <distribution><float value="1e-04" /></distribution>
 </define-CCF-group>
```

Figure 2-20: Open PSA syntax for the definition of a Common Cause Group

A name is given to the common cause group, used was “Communication Issues – Technical Airborne” in the previous example. Members of the group are declared using the <members> tag. This group uses the Beta Law in order to quantify the independent or simultaneous occurrence of members of the group. For each member of the group the probability to fail simultaneously is equal to its failure probability multiplied by factor beta and the probability to fail independently is equal to its failure probability multiplied by (1- beta). So if beta=0 the members never fail simultaneously, if beta=1 the members always fail simultaneously. In the previous example the value 0.6 was selected meaning that the probability of simultaneous failure is greater than the probability of independent failure. Modern fault-tree tools implement Common Cause group. The main difficulty to apply this approach would be to identify which contributors should be grouped and to select the most appropriate beta value.

Another approach to deal with common cause failures could be derived from the approach used by Airbus to orchestrate the development of fault-trees by various teams. The aim is to avoid the definition of a contributor by several teams with different labels. If the Airbus scheme to multi-domain fault-trees is adopted then a unique domain would be in charge of the definition of a contributor, this domain should publish the labels of its contributors and all other domain that we would like to use this contributor should refer to the published label. For instance, as the transponder is a part of the aircraft, the aircraft manufacturer domain would define the label for the failure of the transponder and the ATM fault-tree would use this label. To apply this approach all the domain specific fault-trees would have to be reworked.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU’s Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

2.3. Implementation of the backbone model into the Risk Observatory

2.3.1. Software architecture

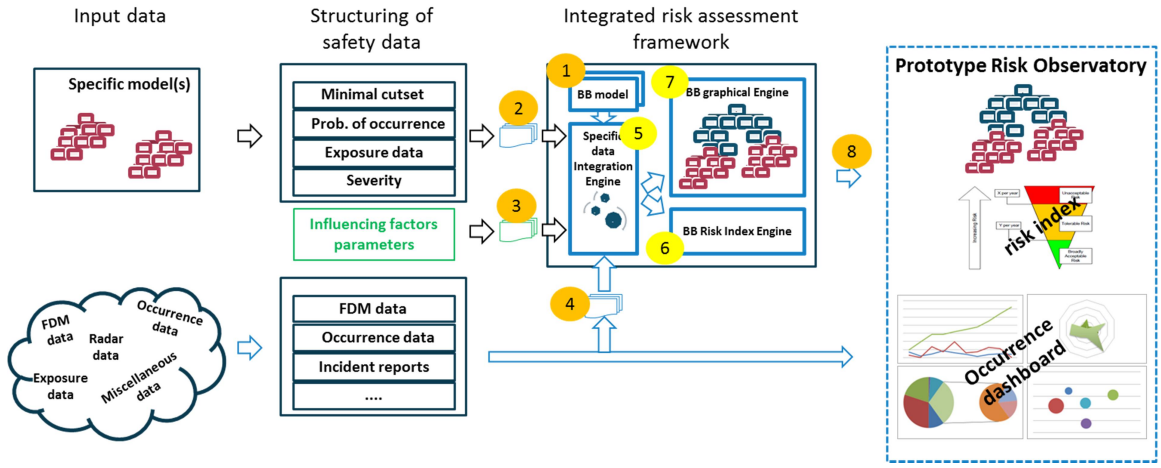


Figure 2-21: Implementation of the integrated risk assessment framework

The previous figure was used to illustrate the software architecture proposed for the implementation of the Backbone models into the Risk Observatory. The figure shows two streams of activities that relate with the two main functionalities studied in FSS P4:

- The bottom stream relates collected data (FDM data, occurrence, incident data) and the occurrence dashboard of the RO,
- The upper stream relates the results of domain specific risk models with Risk index computation and visualization in the RO.

In this document, the main interest is in the upper stream, hence explanations will be provided about the items of the figure that are labeled from 1 to 8 in orange or yellow circles. The orange circles are used to label the inputs or outputs of the integrated risk assessment framework. Yellow circle are used to label the internal functionalities of the integrated risk assessment framework.

Inputs and outputs of Integrated Risk Assessment Framework:

1- A library of predefined Backbone models: as explained previously each backbone model can be described as two open PSA files (one describing the logic and the other one the default probabilities of generic contributors)

2- Results from the domain specific models: each domain specific result can be described as two open PSA files (logic, probabilities). Each domain should also provide information needed to perform unit conversion (average flight time, average number of aircrafts controlled by one ATS unit, average exposure time).

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

3- Influencing factors parameters: the weight, probabilities and values of an IF should be stored in the Integrated Risk Assessment framework, this will enable the computation of the rectified weight of the IF and use this in the computation of the risk index

4- Alternative quantitative information computed from collected data: it could be possible to directly compute the probability of some generic contributors on the basis of collected data, in that case these probabilities could be stored in a new open PSA file.

8- Risk index: the results from the computations performed by the integrated risk assessment are sent to the RO in order to be visualized

Functionalities of the Integrated Risk Assessment Framework:

5- Data Integration Engine: this tool integrates the backbone and specific models and prepares all the inputs needed by the Risk Index Engine (integrated fault-tree, probabilities, relevant IF, etc.).

6- Risk Index Engine: this tool takes as input the fault-tree prepared by the Data Integration Engine and computes risk index in the form of probabilities of occurrence, importance factors, sensitivity analysis results, etc.

7- Graphical Engine: this tool graphically displays the integrated fault-tree representing the combination of the backbone model and the domain specific models.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

2.3.2. Guidance for the Implementation of the backbone model

During WP4.2 the Backbone models were manually developed as excel files. Introducing computation formulas in the excel cells is a tedious and error prone process. In this section, the use of a more robust computation tool such as XFTA [12] is described in order to implement the integrated risk assessment framework.

The XFTA tool takes as input a script that is described using an XML format similar to the Open PSA format used to describe fault trees.

```
<?xml version="1.0"?>
<!DOCTYPE xfta>
<xfta>
  <load>
    <model input="FaultTrees/BB_MAC_v4.xml" />
    <model input="FaultTrees/BB_MAC_v3_basic-events.xml" />
  </load>
  <build>
    <minimal-cutsets top-event="BB030a" handle="MCS" minimum-probability="1.0e-12"/>
  </build>
  <compute>
    <probability top-event="BB030a" handle="MCS" output="Results/BB_MAC_v4_Proba_BB030a.txt" />
    <importance-factors top-event="BB030a" handle="MCS" output="Results/BB_MAC_v4_Factors_BB030a.txt" />
  </compute>

</xfta>
```

Figure 2-22: A XFTA Script

The previous script is made of three main parts that relate with the three main steps of an XFTA session:

1. Fault trees in Open PSA formats are loaded. In the previous example, two fault trees are loaded. The first one describes the logic part of the Backbone mode (it is called BB_MAC_v4.xml) and the second one contains the probabilities of the generic contributors (it is called BB_MAC_v4_basic_events.xml). To take into account domain specific models, it would be sufficient to load the files describing the domain specific fault-trees instead of the second file describing the probabilities of generic contributors.

2. Minimal Cut Sets (MCS) of the Top Event are calculated. In the previous example, the identifier of the top event considered is “BB030a” (Mid Air Collision). To compute the MCS for any other gate of the BB fault tree it is sufficient to give its identifier instead of “BB030a”.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU’s Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

A given cutoff (maximum order and minimum probability of cutsets) can be used to limit the number of MCS generated. In the previous example, only MCS whose individual probability is greater than 10^{-12} will be produced.

3. Probabilistic calculations are performed from the MCS. In the previous example, the probability of the top level event is computed. The result is written is the file "BB_MAC_v4_Proba_BB030a.txt". Various Risk Factors can also be computed by XFTA. Importance Factors are calculated for each Basic Event of a Fault Tree. These indicators aim to assess the relative contributions of the different components of the system to the overall risk. Five importance factors are computed (Marginal Importance Factor, Critical Importance Factor, Fussel-Vesely Importance Factor, Risk Increase Factor and the Risk Decrease Factor .Sensitivity analysis can be performed when the description of the probabilities of the basic events also includes a range of variation for these probabilities.

The XFTA tool can directly be used to implement the "**Risk Index Engine"** function of the Integrated Risk Assessment Framework. One big advantage of the XFTA tool over Excel ad-hoc computations is that is a well-tested tool that was proved to be quite efficient and accurate. Furthermore it computes a variety of safety indicators such as probabilities, importance factors, sensibility analysis and it deals with common cause failures.

The timing performances of the XFTA should be tested on a hardware platform similar to the future the RO server. If the tool is not able to perform its computations with an acceptable speed then an alternative approach that would split the computation into two parts might have to be considered:

- An offline part using XFTA in order to compute the set of Minimal Cut Sets for the top level event (this is the most time consuming computation);
- An online part coded using a "fast" programming language that would read the file containing MCS computed off-line and use them to compute the probability of the top level event.

If XFTA is used to implement the Risk Index Engine function then the main role of the "**Data Integration Engine"** function would be to generate the appropriate script for XFTA based on a configuration defined by the RO user. In order to be able to generate an XFTA script, the tools should manage an analysis configuration by using the answers given by the user to the following questions:

1. Which predefined Backbone model should be used?

   The answer to this question is used to select the Open PSA file of the Backbone model to be loaded.

2. Which predefined Domain Specific models should be used?

   The answer to this question is used to select the Open PSA files of the Domain Specific models to be loaded.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

3. Should already existing probabilities for Generic and Domain Specific Contributors be used? if the answer is No, What are the probabilities to be used for Generic and Domain Specific Contributors? Should the values provided by the user be stored for later use?
   A PROBA data dictionary associating contributors with their probability should be managed by the tool. If the answer to this question is Yes then the PROBA dictionary should contain the probability values stored in the Open PSA files describing the basic events of the Backbone and domain specific models. If the answer is No then the tool should store in the PROBA dictionary the values provided by the user. If the user wants to store these probabilities for later use then a new version of the Open PSA file that includes the probabilities should be generated, its name should be provided by the user.

4. Should Influencing Factors be used to perform the computations? If the answer is Yes, should predefined weight and probabilities be used? if the answer is No, What are the weight, and probabilities to be used for the Influencing Factor? Should the weights and probabilities provided by the user be stored for later use ?

   If Influencing Factors are used then two data structures IFdef and IFmap should be managed by the tool. The IFmap structure should contain the mapping of applicable Influencing Factors on Generic Contributors of the selected Backbone Model (the second table of Appendix A.2 provides the mapping for the Runway Excursion Backbone). If predefined weight and probabilities should be used then the IFdef structure should contain the definition of Influencing Factors parameters as defined by the first table in appendix A.2. Otherwise the tool should store in the IFdef structure the values provided by the user and the tool should compute and store the rectified weight of the IF. Finally, the tool should update the PROBA data dictionary by multiplying the current probability of Generic Contributors with the rectified weight of the Influencing actors mapped on these Generic Contributors. If the user wants to store the weight and probabilities for later use then a new version of the IF parameter file that includes these values should be generated, its name should be provided by the user.

5. What reference unit should be used to perform the computations? Should predefined conversion parameters values be used? if the answer is no, What are the values of Tf, Xt and Nac to be used? Should the values provided by the user be stored for later use?
   A CONV data structure should be managed by the tool, it should contain the information found in the conversion rule table provided in appendix A.3. If the user does not want to use the predefined conversion parameters values for Tf, Xt and Nac then the tool should update CONV with the parameter values provided by the user. Once the conversion rules are defined, the tools should update the PROBA data dictionary by applying the conversion rules to the stored probability of Generic and Domain Specific Contributors. If the user wants to store these new values for later use

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

then a new version of the conversion table that includes these values should be generated, its name should be provided by the user.

Then the tool should generate Open PSA files describing the probabilities of all Generic and Domain Specific contributors as stored in the PROBA data dictionary. The tool should generate a XFTA script that:

- loads the various Open PSA files that were selected or generated;
- computes the Minimal Cut Sets for all top level nodes of the fault-tree,
- computes the probability and the importance factors for all the top level nodes

To implement the **"Graphical Engine"** function that graphically displays the integrated fault-tree it should be possible either to use an external tool that allows to display and edit fault-trees written in open PSA format such as the Arbre Analyste [13], [14] tool or to develop an ad-hoc fault-tree viewer function.

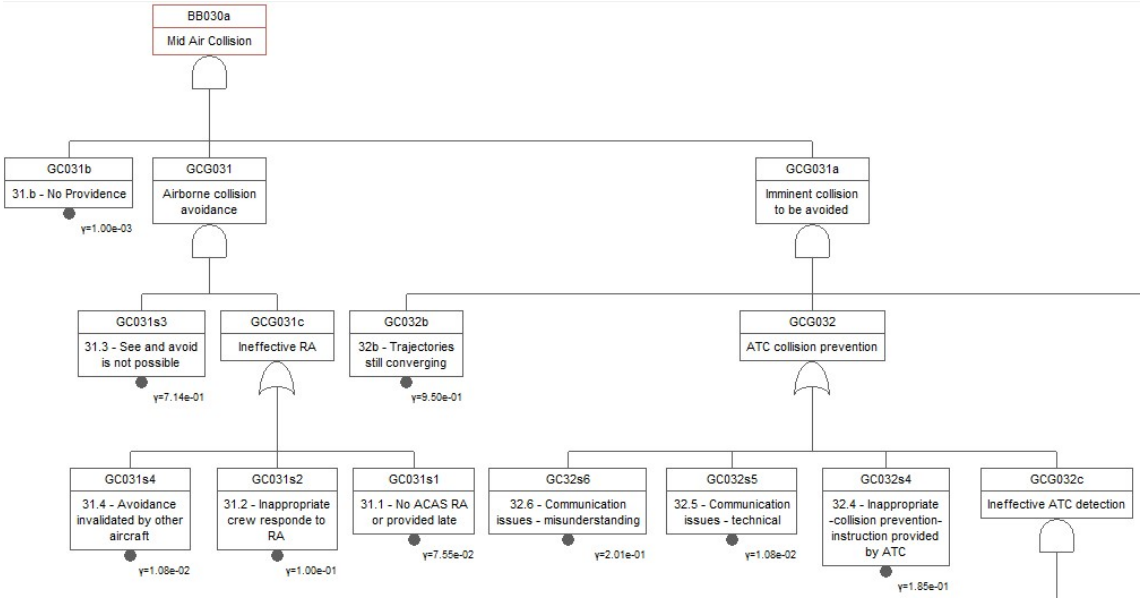


Figure 2-23: BB Fault Tree display by Arbre Analyste tool (extract)

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

3 PROCESSES AND PRACTICES FOR FRAMEWORK UPDATE

The RO, as a tool for safety management in which the integrated risk framework is a core building block, shall provide the most accurate and up-to-date information possible. Besides, each organization can manage different scenarios, evolving in different directions. In order to assure the reliability of the tool and the framework, processes able to capture and incorporate the dynamic nature of safety in the aviation industry and also of all the elements influencing the scenarios in analysis have to be put in place.

This chapter describes three update processes considered in the integrated risk framework, namely: risk scenario creation, model refinement and model update. In addition, a technical approach about how to implement these processes is described.

3.1. Risk scenario creation

Safety and risk management, as described in this document, are dependent on an uncountable number of elements, both internal and external to the organization, for instance, related to geography, weather or technical systems. Most organizations in the aviation industries have large sets of risk scenarios they want to analyse, to be able to identify and mitigate relevant risks. Nevertheless, risk management is not only related to direct mitigation and identification of imminent risks, but much more about comparing and complying to standards and to competing scenarios.

Therefore, the implementation of the integrated risk framework in a software platform such as the RO, must accommodate multi scenario management and analysis. The capacity to create new scenarios will provide the safety management with the ability to analyse the same risk, for instance, for different airports, having in consideration different aircraft type, or even entire different operations. These scenarios may be later refined and updated independently, providing trends analysis and further comparisons between them.

When creating a new risk scenario, the relevant inputs for the new scenario, specifically the results from the domain specific models and the Influencing factors parameters, must be set.

3.2. Risk scenario refinement

Three major elements are part of the framework for the calculation of a risk index for a given scenario: the backbone model, the results from the domain specific models and the influencing factors parameters.

The results from the domain specific models, describe each scenario from different perspectives, and provide the basis for the overall output of the risk model. Although not frequently, these results will evolve over time, as new tools, mitigation actions or threats come into play. The RO shall be able to provide processes, tools and/or interfaces that allow the system to reflect changes in the domain specific components. These processes will allow the risk scenario to be refined and adapted to the new conditions, while providing a perspective of the evolution of the risk over time.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

3.3. Risk scenario update

While the backbone models are static representation, and the domain specific models changes shall not be much frequent, it is easy to understand that there are conditions that may influence specific risks that are constantly changing, depending for instance, on the geography, time of the day, season of the year, and so on.

In order to provide up-to-date information about a specific risk scenario, and to be able to reflect trends and seasonality of each risk scenario, the RO implementation must be able to accommodate processes, tools and interfaces that allow the system or the risk analyst to set the most accurate influencing factors parameters at any time. These processes are fundamental to ensure the information provided to the users are up-to-date and reflect the latest observed or predicted conditions.

3.4. Technical approach

The risk framework is, by definition, an integrator and orchestrator of data arriving from different stakeholders, sources and perspectives, which in the end will enrich a global vision of a specific risk scenario.

Ideally, the RO should be able to automatically fetch and process updated inputs for each risk scenario. From the communication with external systems and services that could provide up-to-date information about Ifs conditions, such as weather services, or the results from domain specific models to the incorporation of alternative quantitative information computed from collected data, as described in Figure 2-21 (point 4).

In order to provide means for that to happen, the RO shall provide tools and processes to consume external services and also an API that can be called for these update processes to take place as automatically as possible.

Nevertheless, the heterogeneity and sensitiveness of the data needed to compute the above described processes will certainly raise barriers that can impede the complete automation. Therefore, as a basis for assuring the risk scenarios can be updated, the RO shall implement manual interfaces that allow the risk analyst to update the scenarios with the data he considers the most up-to-date. Besides, to override potential system errors, the manual updates shall have higher priority over potential automatic updates in case both alternatives are set in place.

Due to the low volume of data, difficult to connect to providers of results for the domain specific contributors and to make the implementation simple, the RO prototype will allow the creation, refinement and update of risk scenarios from dedicated interfaces included in the tool.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

4 VERIFICATION OF THE RISK ASSESSMENT FRAMEWORK

4.1. Uncertainty of results

The backbone model may be considered as a scalar input output black box function. Its inputs are the terminal leaf probabilities of the backbone model and its output is the general failure probability. Determining the most important inputs of the backbone model on its failure probability is an interesting question of safety. It is exactly the purpose of sensitivity analysis. Indeed, sensitivity analysis of model output aim is to study how the model output of a computer code varies regarding the inputs. It enables for instance to identify model inputs that cause significant uncertainty in the output and should therefore be the focus of attention or to fix model inputs that have no effect on the output. Two main classes of sensitivity analysis are often considered in practice, see [15]:

- Local sensitivity analysis. This deterministic approach consists in calculating or estimating the partial derivatives of the model at a specific point.
- Global sensitivity analysis. In contrast to local sensitivity analysis, it considers the whole variation range of the inputs.

In this project, it has been focused on a global sensitivity analysis method based on the estimation of Sobol indices [17]. They are a central tool in sensitivity analysis since they give a quantitative and a rigorous overview of how the different inputs influence the output. Sobol indices enable to determine which part of the output variance is due to the different inputs. In the following, the estimation of these indices is reviewed and applied to mid-air collision (MAC) backbone model developed in WP4.2.

Let us consider a d-dimensional random vector $X=(X^{(1)}, X^{(2)},\ldots, X^{(d)})$ of terminal leaf probabilities with a probability density function (PDF) h. The support of h is $[0, 1]^d$ as X is a vector of probability. d is equal to 42 for the MAC backbone model.

Let us denote φ a continuous deterministic positive scalar function $\varphi: [0, 1]^d \rightarrow [0, 1]$; φ represents mathematically the backbone model. φ(X) is the random value that gives the MAC probability in the backbone model.

It is possible to represent this function φ as a sum of elementary functions, see [16]:

$$Y = \varphi(X) = \varphi_0 + \sum_{i=1}^{p} \varphi_i(X^{(i)}) + \sum_{1 \le i < j \le p} \varphi_{ij}(X^{(i)}, X^{(j)}) + \ldots + \varphi_{1\ldots p}(X^{(1)}, \ldots, X^{(p)})$$

This decomposition is unique under some integrability conditions over the different elementary functions.

When the inputs $X^{(i)}$ are statistically independent, one can obtain the well-known ANOVA (Analysis Of Variance) decomposition by applying the variance operator to the previous equation :

$$Var(Y) = V = \sum_{i=1}^{p} V_i + \sum_{1 \le i < j \le p} V_{ij} + \ldots + V_{1\ldots p}$$

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

with *Var* the variance operator and with

$$\begin{aligned} V_i &= Var(E(Y|X^{(i)})) \\ V_{ij} &= Var(E(Y|X^{(i)}, X^{(j)})) - V_i - V_j \\ V_{ijk} &= Var(E(Y|X^{(i)}, X^{(j)}, X^{(k)})) - V_i - V_j - V_k - V_{ij} - V_{ik} - V_{jk} \\ &\dots \end{aligned}$$

where *E* describes the mathematical expectation.

Sobol's sensitivity index at first order S_i for the variable $X^{(i)}$ is then defined by, see [17]:

$$S_i = \frac{V_i}{V} = \frac{Var(E(Y|X^{(i)}))}{Var(Y)}$$

Sensitivity indices at second order S_{ij} can also be derived relatively to the variables $X^{(i)}$ and $X^{(j)}$

$$S_{ij} = \frac{V_{ij}}{V}$$

Sensitivity indices at higher order can be defined in the same way. For computational time and interpretation reasons, practitioners rarely evaluate indices of order higher than two. All the Sobol indices are estimated in practice with Monte Carlo sampling, see [18].

The interpretation of the sensitivity indices is easy since they vary between 0 and 1 and their sum is equal to 1. If S_i is close to 1, then the variable $X^{(i)}$ has a great influence on φ(X).

Let us apply this approach to the MAC backbone model. It is first necessary to define a pdf h over the leaf probabilities that model their uncertainty. It is assumed here that the leaf probabilities follow independent uniform distribution whose support depends on the initial leaf probability value. If p_i is the i^{th} leaf probability of the backbone model without uncertainty, then the corresponding input $X^{(i)}$ follows a uniform distribution on the support $[p_i/5, p_i*5]$ if $p_i<10^{-3}$, on the support $[p_i/2, p_i*2]$ if $10^{-3}<p_i<0,5$, on the support $[p_i*0.9, \max(1,p_i*1.1)]$ if $p_i>0.5$. Here it is assumed that that the error order of magnitude is greater for low probabilities. These assumptions are only based on subjective expert opinions and can be easily modified.

The distribution of the output probability φ(X) **for** the MAC backbone model is given in the following Figure 4-1. As a comparison, the MAC probability without uncertainties is $5.1\ 10^{-9}$. Uncertainties tend to increase this probability.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

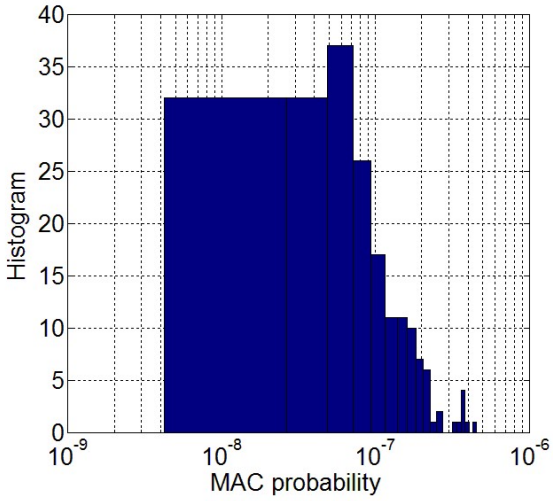


Figure 4-1: Histogram of the MAC probability (200 samples)

Then, first order Sobol indices have been estimated on the MAC backbone model. The ten most influent leaf probabilities are given in the following table with their corresponding Sobol indices estimated with 1000 Monte Carlo simulations.

Contributing Factor	Sobol Indices
Providence	22.4%
Pre-tactical conflict	19.5%
Inadequate Planning task fails to remove conflict	13%
No detection by ATCo	8.7%
Inappropriate crew responde to RA	7.8%
No time to provide separation	7%
No ACAS RA or provided late	3.8%
No or late detection of conflict	3.3%
Inappropriate traffic data information	2.5%
Inappropriate crew response to ATC instruction	2%

Table 14: The ten most influent Contributing Factor probabilities for MAC Backbone

Input probabilities whose Sobol indices is greater than 5% have to be estimated with caution. An error on their estimation could lead to a very inaccurate MAC probability.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

4.2. Framework Verification

In the FSS P4 project plan of 2015, see [5], the Frame work verification Task 4.3.3 is described as follows: ”This task will verify the framework’s usability and its results. The framework’s usability will be verified against requirements set. The results obtained using the framework will be verified by comparing framework outcomes (e.g. accident rates) with data representing actually achieved safety performance in the operation. The verification process safeguards the transparency of the techniques developed in this research project. The focus in this task is on verification of the framework as a whole to verify the correct functioning of the framework and the interfaces between the individual risk models.” Verification of the risk framework against the defined high-level RO-requirements, see [3], will be part of P4-deliverable D4.10.

4.2.1. Scoping of the Verification

At the start of the execution of Task 4.3.3, the objective of the task was further detailed, taking into account the status of the project. This led to the following main topics and scope [27]:

1. Quantitative verification of the backbone models
2. Verification of the usability of the framework

Ad.1 Quantitative verification of the backbone models

The scope for the verification of the MAC and RE models was reduced to the verification of the top level only, i.e. related to the probabilities of the MAC and the RE model. A verification of the quantification of lower-level elements of these models was considered outside the scope of this task.

For a quantitative verification of the backbone models with actual data it is important to know which actual data sources have been used to quantify the elements of these models. This information should be available for Contributing Factors as well as Influencing Factors, taking into account that certain information in the data sources is confidential.

Ad.2 Verification of the usability of the framework

The usability and correct functioning of the framework has been verified by performing simple What-If scenarios with the risk models, e.g. by inhibiting certain failures (probability is zero) and checking whether the top level risks moved in the expected direction (i.e. relative assessment was performed). Most interesting failures inhibited are those that are the strongest contributors to risk.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU’s Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

4.2.2. Quantitative verification of risk assessment framework

A quantitative verification of the Backbone models has been performed on the top-level of the models. The accident probabilities at the top of the models are compared with actual data from the operation. In Section 4.2.2.1, this has been done for mid-air collisions and in Section 4.2.2.2 for runway excursions. For this verification, it was essential to make explicit which versions of the models, which data sources were used for the quantification of these models and the scope of the actual data. To be able to draw any conclusion on the top level probabilities of the model, the data sources and the scope of the actual data should correspond as much as possible.

For the actual data for mid-air collisions and runway excursions, the following sources have been used:

- EASA Annual Safety Review 2017 [20];
- FSS-P4 Risk Pictures 2016 and 2017, see [22] respectively [23];
- FSS FDM workshop, see [21].

4.2.2.1. Mid-Air Collisions En Route

4.2.2.1.1. Mid-Air Collision probability

The top level probability for a mid-air collision en route has been derived from the MAC model [25], making use of the Arbre Analyste tool, see [13] and [14]. The resulting probability of a mid-air collision is 4.06E-09 per flight (SumOfProduct) as shown in Figure 4-2.

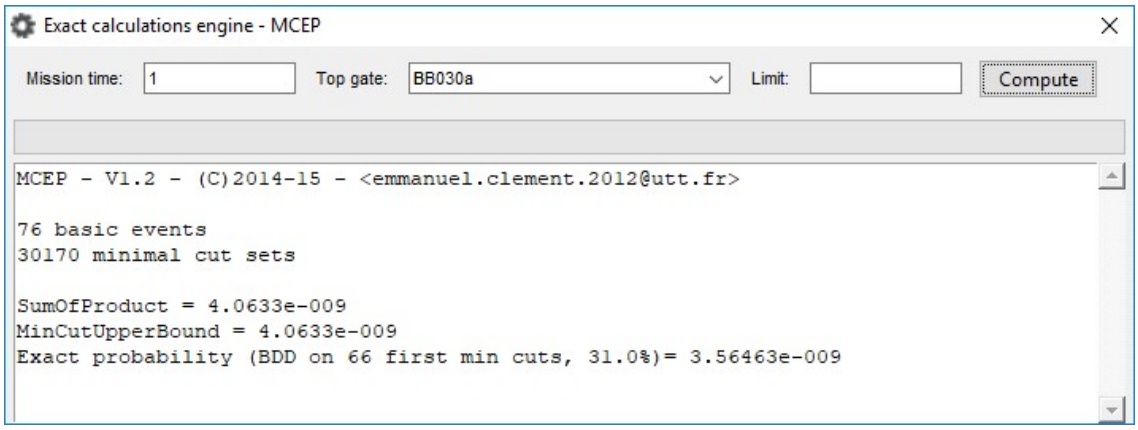


Figure 4-2: Probability of a MAC calculated with Arbre Analyste

The scope for this probability needs to be clarified: which types of flights are considered, for which Region, for which years? This was done by looking at the data sources for the quantification of the Contributing Factors of the model.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

In the spreadsheet of [25] related to the MAC-model sources like “incident reports” and “expert judgement” are mentioned without specific details on e.g. timeframe, region, and types of operation considered.

4.2.2.1.2. EASA Annual Safety Review 2017

The EASA Annual Safety Review 2017 [20] provides accident statistics, for different scopes of flight such as commercial air transport, special operations, helicopter operations, non-commercial operations, etc. For the verification of the risk assessment framework it is expected that the statistics for the scope “CAT – Aeroplane Airline” is most relevant. This scope includes the airline passenger/cargo operations with aeroplanes having a maximum take-off weight above 5700 kg. EASA provides the following results for fatal and non-fatal accidents:

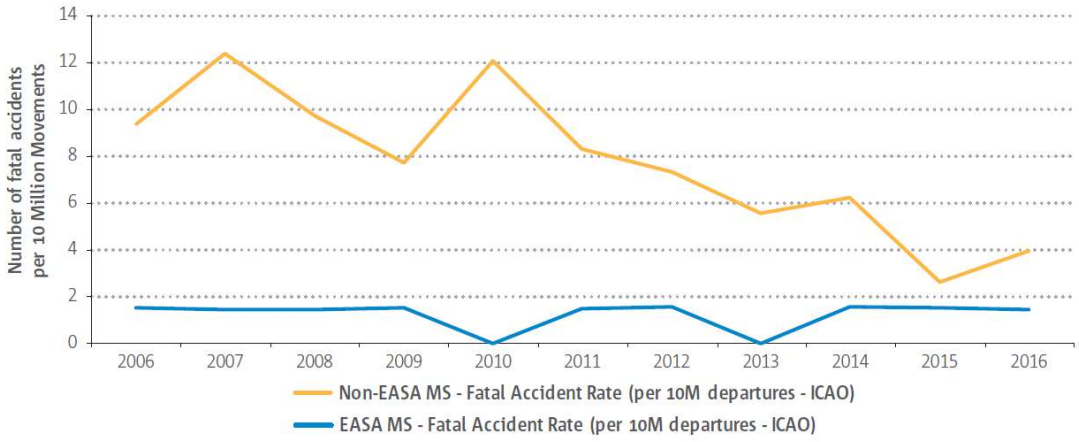


Figure 4-3: CAT Aeroplane Airline fatal accident rate [EASA, 2018]

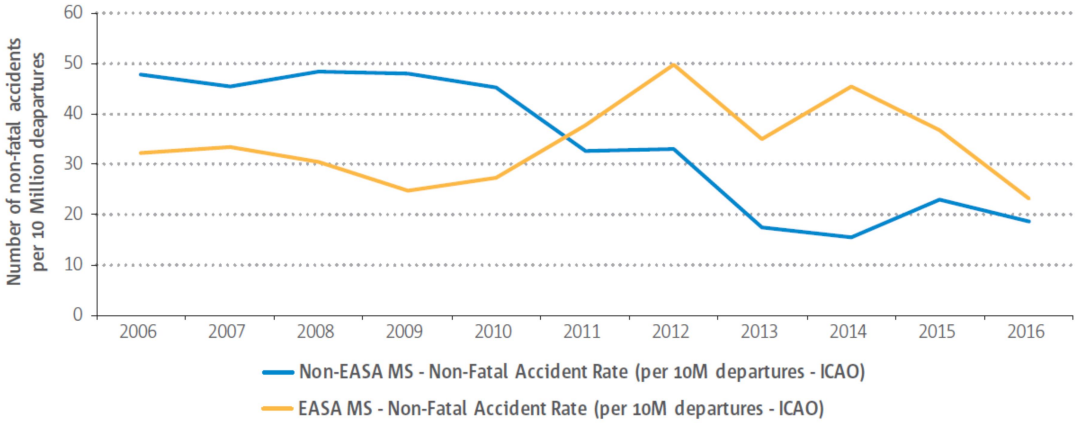


Figure 4-4: CAT Aeroplane Airline non-fatal accident rate [EASA, 2018]

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU’s Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

From these figures it can be deduced that the overall fatal accident frequency over the period 2006-2016 for EASA member states is approximately 1.8E-07 per departure (Figure 4-3) and the non-fatal accident frequency between 1.8E-06 and 5.0E-06 per departure (Figure 4-4). This leads to an accident (fatal plus non-fatal) frequency of between 2.0E-06 and 5.2E-06 per departure

Note that these figures provide information on the sum of all accidents types, not on mid-air collisions only. To deduce the latter accident rate, more information is needed. In the EASA annual safety review 2017 EASA furthermore states that for 2007-2016 Airborne Collisions are 0% of Fatal Accidents and 1% of Non-Fatal Accidents (Note: an Airborne Collision could include more flight phases than en route only). Combining this with the above, this leads to an accident rate of mid-air collisions between 1.8E-08 and 5.0 E-08 per departure in EASA Member States.

4.2.2.1.3. FSS Risk Pictures 2016 and 2017

The FSS Risk Pictures of 2016 and 2017, see [22]-[23], do also provide statistics for Mid-Air Collisions. The scope for these statistics is:

- Occurrence class: Accidents and Serious incidents
- Operation type: Scheduled revenue ops, Non-scheduled revenue ops
- Aircraft category: Fixed wing
- Aircraft mass group: > 5,701 kg maximum take-off weight
- Aircraft propulsion type: Turboprop, Turbofan, Turbojet
- State or area of occurrence: EASA Member States: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom, Iceland, Liechtenstein, Norway, Switzerland.
- Time interval:
    - Between 1-1-1995 to 31-12-2015, see [22]
    - Between 1-1-1995 to 31-12-2016, see [23]

FSS-Risk Picture 2016 Table 3 in [22] shows the accident frequencies of Mid-Air Collisions to be 2.88E-08 per flight (1.92E-08 per flight hour). In FSS –Risk Picture 2017, see [23] this is 2.66E-08 per flight.

4.2.2.1.4. Comparison

The results of the previous sections are summarized in the following table:

Source	MAC accident frequency per flight
EASA	between 1.8E-08 and 5.0E-08 per departure
FSS Risk Picture 2016	2.88E-08 per flight
FSS Risk Picture 2017	2.66E-08 per flight
P4 MAC model	4.06E-09 per flight

Table 15 Different Sources and results on MAC accident frequency per flight.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

From the table above, it can be found that the MAC probabilities of EASA and the FSS pictures are consistent, as can be expected because the scopes for these probabilities are comparable.

Apparently, the MAC probability as calculated by the BB model is approximately a factor 5 lower than the EASA and FSS figures. That the figures differ could be because the BB model is quantified by means of different data sources, as described in Section 4.2.2.1.1. Possibly, not all European States are included in the data sources, data could be only of the last couple of years, and also sometimes expert judgement has been used. For a more generic discussion on quantitative verification, see Section 4.2.2.4.

4.2.2.2. Runway Excursions

4.2.2.2.1. Runway Excursion probability

The top level probability for a runway excursion (longitudinal excursions, so only runway overruns are considered) has been derived from [RE model], making use of the Arbre Analyste tool [14]. The probability of a runway excursion has been assessed as 6.53E-06 per flight (SumOfProduct) as shown in Figure 4-5:

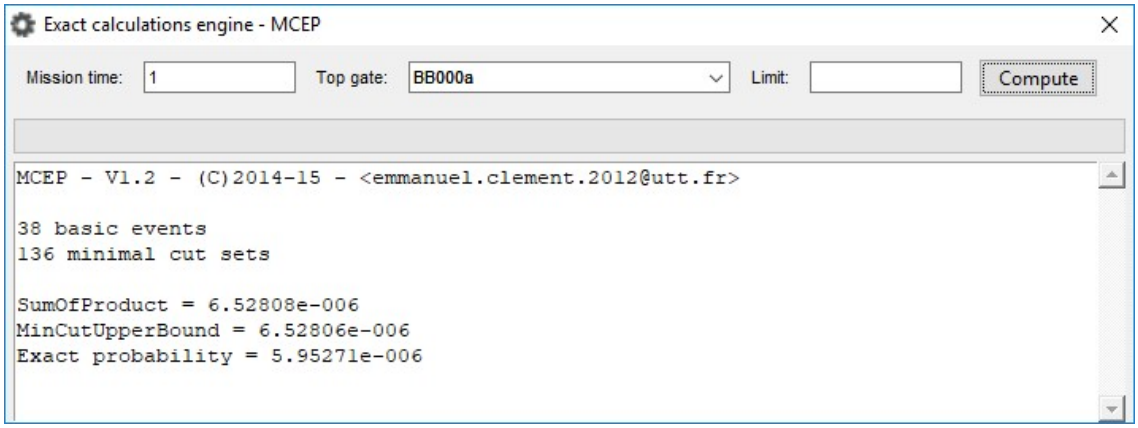


Figure 4-5: Runway excursion probability calculated with Arbre Analyste using [RE model]

The data sources used for the quantification of the RE model are, see [26]:

- EUROCONTROL statistics in the TMA area;
- Worldwide network of a large European airline;
- Data from some Airbus operators on a set of flights over 12 months (Flight Data Monitoring data);
- Aircraft & systems Functional Hazard Assessment (FHA) and System Safety Assessment (SSA);
- Expert judgement.

4.2.2.2.2. EASA Annual Safety Review 2017

As described in Section 4.2.2.1.2, the overall fatal accident frequency over the period 2007-2016 for EASA member states is approximately 1.8E-07 per departure and the non-fatal accident frequency between 1.8E-06 and 5.0E-06 per departure. Overall this means an accident frequency of between 2.0E-06 and 5.2 E-06 per departure. This is for commercial air transport, airline passenger/cargo with aeroplanes having a maximum take-off weight above 5700 kg and operations in EASA Member States.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Furthermore, EASA Safety Review 2018, see [20], states that for 2007-2016, runway excursions are 13% of Fatal Accidents and 30% of Non-Fatal Accidents. *This includes both runway overruns and runway veer-offs*. This leads to a runway excursion frequency of between 5.6E-07 and 1.5E-06 per departure. For our analysis it is assumed that EASA's unit "per departure" means that the EASA probability covers both runway excursions during take-off and runway excursions during landing.

To assess the accident probability for runway overruns only, the results from the FFS-(P3) FDM-workshop on runway veer-off, held at NLR at 26th of September 2018 have been used, see [21]. At that workshop, it was learned that the overall probability of veer-offs has been derived (i.e. via a Bayesian Network calculated) as 2.8834E-08 (1 in 35 million flights). This figure is based on 310,000 A320 series flights:

- 10 year span;
- Approximately 370 recorded parameters;
- 68 measures extracted from each landing (P3-D3.5);
- METAR info added.

When using this veer-off probability in combination with the above mentioned EASA data, the estimated *runway overrun* probability is expected to lay between:

1.5E-06 = P_1(RWYEX)+2.8834E-08 and

6.2E-07 = P_2(RWYEX)+2.8834E-08.

Thus between:

P_1(RWYEX) = 6.2E-07 -2.8834E-08 = 5.9E-07 and

P_2 (RWYEX) = 1.5E-06 -2.8834E-08=1.2E-07.

4.2.2.2.3. FSS Risk Pictures 2016 and 2017

In the FSS project, risk pictures have been made in 2016 and 2017. These risk pictures consider the following scope; see [22] and [23]:

- Occurrence class: Accidents and Serious incidents
- Operation type: Scheduled revenue ops, Non-scheduled revenue ops
- Aircraft category: Fixed wing
- Aircraft mass group: > 5,701 kg maximum take-off weight
- Aircraft propulsion type: Turboprop, Turbofan, Turbojet
- State or area of occurrence: EASA Member States: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom, Iceland, Liechtenstein, Norway, Switzerland.
- Time interval:
    - Between 1-1-1995 to 31-12-2015, see [22]
    - Between 1-1-1995 to 31-12-2016, see [23]

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

This largely corresponds with the scope for the EASA Safety Review 2017, see [20], except for the larger period of time and the serious incidents as additional severity class.

Table 3 in [23] shows the following accident and serious incident frequencies of Runway Safety (runway excursions AND runway incursions):

- Accident frequency: 5.18E-07 per flight
- Serious incident frequency: 6.33E-07 per flight

To determine the runway excursion accident frequency, the table in Appendix A of [23] was used. In that table, the runway excursion frequency, added over all event sequence diagrams is 1.16E-06 per flight, the runway incursion frequency is 5.04E-08 per flight. Note that this includes both accidents and serious incidents. This means that approximately 96% of the runway safety events are runway excursions and 4% are runway incursions. With this percentage, the accident frequency for a runway excursion is 0.96 x 5.18E-07 = 5.0E-07 per flight for all flight phases. Using the same Appendix, the percentage of runway excursions during the landing phase is assessed to be 84%. This leads to a runway excursion accident frequency during landing of 0.84 x 5.0E-07 = 4.2E-07 per landing.

Table 3 in [23] shows the following accident and serious incident frequencies of Runway Safety (runway excursions AND runway incursions):

- Accident frequency: 4.78E-07 per flight
- Serious incident frequency: 6.38E-07 per flight

Similar to the figures for [22], the runway excursion frequency is assessed as 1.13E-06 per flight and the runway incursion frequency as 4.65E-08 (accidents and serious incidents). With the 96% the accident frequency for a runway excursion is 0.96 x 4.78E-07 = 4.6E-07 per flight for all flight phases. For the landing phase only (In 2017, 82% of the runway excursions occurs during landing), this leads to 0.82 x 4.6E-07 = 3.8E-07 runway excursions per landing. Note that this number is within the FDM-results (1.2E-07 and 5.9E-07) derived from the FDM-workshop data (see Section 4.2.2.2.2).

4.2.2.3. Comparison

A summary of the results of the previous sections is given in the following table:

Source	RE accident frequency per flight
EASA	between 5.6E-07 and 1.5E-06 per departure (overruns and veer-offs)
FSS Risk Picture 2016	5.0E-07 per flight (overruns and veer-offs, all flight phases) 4.2E-07 per landing (overruns and veer-offs, landing only)
FSS Risk Picture 2017	4.6E-07 per flight (overruns and veer-offs, all flight phases) 3.8E-07 per landing (overruns and veer-offs, landing only)
FDM workshop 2018	2.8834E-08 per flight for veer-offs only Combined with EASA data gives: Between 1.2E-07 and 5.9E-07 per departure (overruns only)
RE model	6.53E-06 per flight (runway overruns only)

Table 16: Different Sources and results on RE accident frequency per flight.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Note that the RE model considers longitudinal runway excursions during the landing phase only, where other sources consider both runway overruns and veer-offs.

Even when accounting for this, the table above shows that the RE probability calculated by the BB model is at least one order of magnitude larger than probabilities from actual data. One important cause could be that Contributing Factors corresponding to aircraft system failures have been quantified with probabilities from aircraft system safety assessments, i.e. the target probabilities for certification. This means that for such Contributing Factors a pessimistic approach is used: in real-life failure probabilities are generally better than these target figures. Also, different data sources have been used for the quantification of the Contributing Factors than for the quantification of the EASA and FSS probabilities: fewer flights, different selection of aircraft types (FSS used data of Airbus aircraft only based on a new Long Range version) and operations, different geographical area, different period for data collection. Another reason could be that the model is incomplete and does not consider all possible root causes but only the most significant ones but testing this is not part of this verification activity.

For a generic discussion on verification of the (integrated) risk assessment framework, see Section 4.2.2.4.

4.2.2.4. Discussion on quantitative verification

Sections 4.2.2.1.4 and 4.2.2.3 show that risk results of the quantified MAC and RE models do not perfectly match the MAC and RE accident probabilities assessed in the actual operation. Important reason for this is that the BB models are quantified by using various data sources with different scopes in period of time, type of aircraft, type of aircraft operations, geographical region etc. A second cause is that accident probabilities are often quite accurate because of the mandatory accident reporting, while information on lower levels in the BB models is often less complete because these events address situation that appear more regular and not necessarily have a significant effect on safety. Another cause could be that some of the effects that are implicit in the top-level EASA probabilities are modelled through the Influencing Factors of the MAC and RE models, e.g. wind and runway contamination. However, these Influencing Factors were not integrated into the BB models at the time of performance of this this verification. That verification will be done in another task of this project. All in all, the quantitative verification of the BB models is difficult and not easy to achieve in the project.

Nevertheless, all Contributing Factors have been quantified with as much available data as possible and this is a good result. The quantified Contributing Factors are valuable input to the Users of the Risk Observatory if the following information is available to them: what is a clear qualitative definition of a Contributing Factor (including some examples if possible) and on which actual data the probability of the Contributing Factor is based. The user can then assess whether the probability is applicable to their operation or not.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

4.2.3. Verification of the usability of the framework

The usability and correct functioning of the framework has been verified by performing simple what-if scenarios with the risk model by inhibiting certain failures and to check whether the top level risks move in the expected direction, i.e. the top-level risk shall not increase.

To identify interesting scenarios, use is made of minimal cut sets. Minimal cut sets are those combinations of events that are sufficient to cause the top event. The minimal cut set with the largest probability is the most important one for causing the top event. Therefore, as a starting point, the top 10 of the minimal cut sets have been chosen. The events in these minimal cut sets are selected and one by one, the probabilities for these events have been set to 0, so that these "failures" do not happen. The effect of this on the top-event has assessed.

The following models and software has been used for the verification:

- Model Versions: MAC model, see [25] and RE model, see [26]
- Arbre-Analyste [14] for identification of the scenarios on the level of the Contribution Factors. This tool includes the XFTA engine that is also part of the RO prototype, so that this tool has also been used to run the what-if scenarios.

4.2.3.1. Mid-Air Collisions

4.2.3.1.1. Identification of scenarios on the level of Contributing Factors

Arbre-Analyste has identified the following Minimal Cut Sets for the MAC model [25]:

XFTA calculations engine

Mission time: 1 Top gate: BB030a Limit: Compute

Executive Summary | Importance | Minimal cuts set | Probabilities | Sensitivity

N°	Quantity	Probability	Percent	Events					
1	6	4.07444e-010	0.100274	GC031b	GC031s2	GC031s3	GC032b	GC032s6	GC037sx
2	6	4.06996e-010	0.100164	DC002t1	GC031b	GC031s3	GC032b	GC032s3	GC034b
3	6	2.2499e-010	0.0553712	DC002t1	GC031b	GC031s3	GC032b	GC032s7	GC034b
4	6	1.66671e-010	0.0410187	DC002t1	GC031b	GC031s3	GC032b	GC032s4	GC034b
5	8	1.56749e-010	0.0385769	GC031b	GC031s2	GC031s3	GC032b	GC032s7	GC033s4
GC034b	GC034s3								
6	8	1.16119e-010	0.0285776	GC031b	GC031s2	GC031s3	GC032b	GC032s4	GC033s4
GC034b	GC034s3								
7	7	9.7481e-011	0.0239906	GC031b	GC031s2	GC031s3	GC032b	GC032s6	GC034b
GC034s3									
8	8	7.83747e-011	0.0192884	GC031b	GC031s2	GC031s3	GC032b	GC032s7	GC033s8
GC034b	GC034s3								
9	8	6.85779e-011	0.0168774	GC031b	GC031s2	GC031s3	GC032b	GC032s7	GC033s9
GC034b	GC034s3								
10	8	5.8781e-011	0.0144663	GC031b	GC031s2	GC031s3	GC032b	GC032s7	GC033s3
GC034b	GC034s3								
11	8	5.80597e-011	0.0142888	GC031b	GC031s2	GC031s3	GC032b	GC032s4	GC033s8
GC034b	GC034s3								
12	8	5.7655e-011	0.0141892	GC031b	GC031s2	GC031s3	GC032b	GC032s7	GC033s4
GC034b	GC034s5								
13	9	5.41586e-011	0.0133287	GC031b	GC031s2	GC031s3	GC032b	GC032s3	GC032s8
GC033s4	GC034b	GC034s3							
14	8	5.08022e-011	0.0125027	GC031b	GC031s2	GC031s3	GC032b	GC032s4	GC033s9
GC034b	GC034s3								
15	6	4.46621e-011	0.0109916	DC002t1	GC031b	GC031s3	GC032b	GC032s9	GC034b
16	6	4.396e-011	0.0108188	GC031b	GC031s3	GC031s4	GC032b	GC032s6	GC037sx
17	8	4.35448e-011	0.0107166	GC031b	GC031s2	GC031s3	GC032b	GC032s4	GC033s3
GC034b	GC034s3								
18	8	4.27106e-011	0.0105113	GC031b	GC031s2	GC031s3	GC032b	GC032s4	GC033s4

Figure 4-6: Minimal Cut Sets for the [MAC model]

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Taking the first 10 minimal cut sets leads to the following set of events:

ID	Event title		Probability
DC002t1	Undetected loss of Transponder	Constant	1e-05
GC031b	31.b - No Providence	Constant	0.001
GC031s2	31.2 - Inappropriate crew response to RA	Constant	0.1001
GC031s3	31.3 - See and avoid is not possible	Constant	0.7141
GC032b	32b - Trajectories still converging	Constant	0.95
GC032s3	32.3 - No detection by ATCo	Constant	0.3636
GC032s4	32.4 - Inappropriate -collision prevention- instruction provided by ATC	Constant	0.1489
GC032s6	32.6/33.6/37.4 - Communication issues - technical Ground	Constant	0.0001
GC032s7	32.7 - Communication issues - misunderstanding	Constant	0.201
GC033s3	33.3 - No or late detection of conflict	Constant	0.0003
GC033s4	33.4 - Inappropriate -separation- instruction provided by ATC	Constant	0.0008
GC033s8	33.8 - Inappropriate crew response to ATC instruction	Constant	0.0004
GC033s9	33.9 - No time to provide separation	Constant	0.00035
GC034b	34.b - Pre-tactical conflict	Constant	0.165
GC034s3	34.3 - Inadequate Planning task fails to remove conflict	Constant	0.087
GC037sx	37.x - Potential for conflict	Constant	0.06

Table 17: Contributing Factors in top 10 Minimal Cut Sets of MAC model.

4.2.3.2. Results

The following table shows the results for the top level Mid Air Collision risk in case individual events have a probability of 0. It also shows the change with respect to the top level risk, which is 4.1E-09 per flight.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Event id	Event name	Original MAC-ER risk	New MAC-ER risk	Change
DC002t1	Undetected loss of Transponder	4.1E-09	3.20E-09	-22%
GC031b	31.b - No Providence	4.1E-09	9.0e-314 i.e. 0	-100%
GC031s2	31.2 - Inappropriate crew response to RA	4.1E-09	1.20E-09	-71%
GC031s3	31.3 - See and avoid is not possible	4.1E-09	1.3e-316 i.e 0	-100%
GC032b	32b - Trajectories still converging	4.1E-09	9.53-317 i.e. 0	-100%
GC032s3	32.3 - No detection by ATCo	4.1E-09	3.20E-09	-22%
GC032s4	32.4 - Inappropriate -collision prevention- instruction provided by ATC	4.1E-09	3.10E-09	-24%
GC032s6	32.6/33.6/37.4 - Communication issues - technical Ground	4.1E-09	3.40E-09	-17%
GC032s7	32.7 - Communication issues - misunderstanding	4.1E-09	2.80E-09	-32%
GC033s3	33.3 - No or late detection of conflict	4.1E-09	3.70E-09	-10%
GC033s4	33.4 - Inappropriate -separation- instruction provided by ATC	4.1E-09	3.20E-09	-22%
GC033s8	33.8 - Inappropriate crew response to ATC instruction	4.1E-09	3.60E-09	-12%
GC033s9	33.9 - No time to provide separation	4.1E-09	3.70E-09	-10%
GC034b	34.b - Pre-tactical conflict	4.1E-09	5.80E-10	-86%
GC034s3	34.3 - Inadequate Planning task fails to remove conflict	4.1E-09	3.00E-09	-27%
GC037sx	37.x - Potential for conflict	4.1E-09	3.6E-09	-12%

Table 18: Resulting RE accident probability after setting Contributing Factors probability to 0.

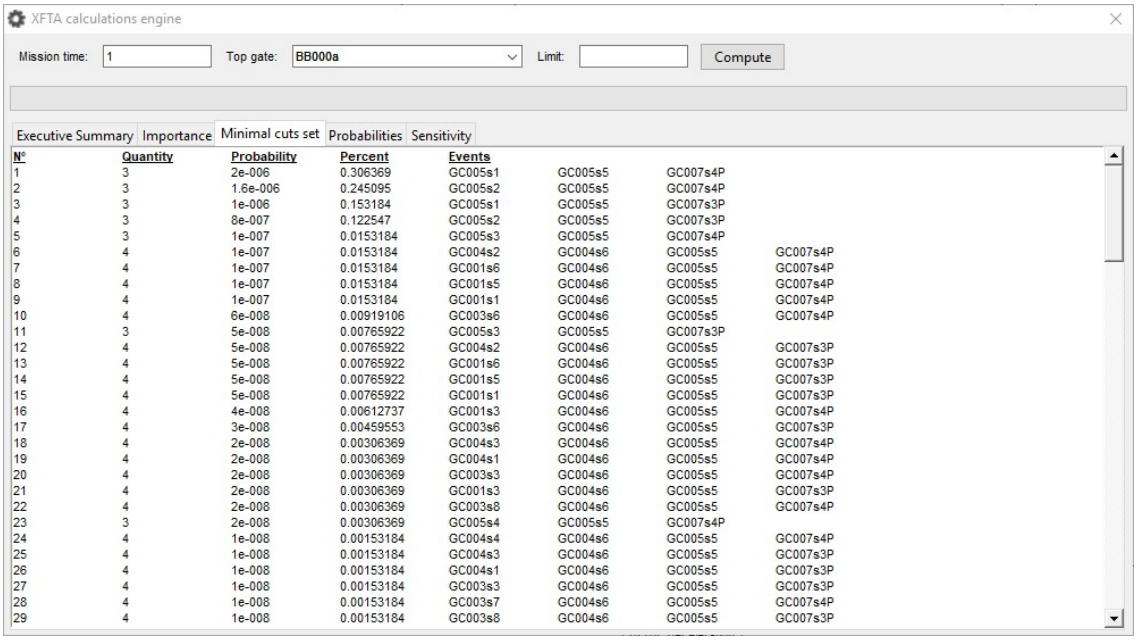
As can be observed from the differences found, all differences are negative, i.e., the top level risk reduces by inhibiting the individual events, as can be expected. Also, there are 5 most impacting events in the range of -70% to -100%.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

4.2.3.3. Runway excursions

4.2.3.3.1. Identification of scenarios on the level of Contributing Factors

Arbre-Analyste identified the following minimal cut sets:



N°	Quantity	Probability	Percent	Events			
1	3	2e-006	0.306369	GC005s1	GC005s5	GC007s4P	
2	3	1.6e-006	0.245095	GC005s2	GC005s5	GC007s4P	
3	3	1e-006	0.153184	GC005s1	GC005s5	GC007s3P	
4	3	8e-007	0.122547	GC005s2	GC005s5	GC007s3P	
5	3	1e-007	0.0153184	GC005s3	GC005s5	GC007s4P	
6	4	1e-007	0.0153184	GC004s2	GC004s6	GC005s5	GC007s4P
7	4	1e-007	0.0153184	GC001s6	GC004s6	GC005s5	GC007s4P
8	4	1e-007	0.0153184	GC001s5	GC004s6	GC005s5	GC007s4P
9	4	1e-007	0.0153184	GC001s1	GC004s6	GC005s5	GC007s4P
10	4	6e-008	0.00919106	GC003s6	GC004s6	GC005s5	GC007s4P
11	3	5e-008	0.00765922	GC005s3	GC005s5	GC007s3P	
12	4	5e-008	0.00765922	GC004s2	GC004s6	GC005s5	GC007s3P
13	4	5e-008	0.00765922	GC001s6	GC004s6	GC005s5	GC007s3P
14	4	5e-008	0.00765922	GC001s5	GC004s6	GC005s5	GC007s3P
15	4	5e-008	0.00765922	GC001s1	GC004s6	GC005s5	GC007s3P
16	4	4e-008	0.00612737	GC001s3	GC004s6	GC005s5	GC007s4P
17	4	3e-008	0.00459553	GC003s6	GC004s6	GC005s5	GC007s3P
18	4	2e-008	0.00306369	GC004s3	GC004s6	GC005s5	GC007s4P
19	4	2e-008	0.00306369	GC004s1	GC004s6	GC005s5	GC007s4P
20	4	2e-008	0.00306369	GC003s3	GC004s6	GC005s5	GC007s4P
21	4	2e-008	0.00306369	GC001s3	GC004s6	GC005s5	GC007s3P
22	4	2e-008	0.00306369	GC003s8	GC004s6	GC005s5	GC007s4P
23	3	2e-008	0.00306369	GC005s4	GC005s5	GC007s4P	
24	4	1e-008	0.00153184	GC004s4	GC004s6	GC005s5	GC007s4P
25	4	1e-008	0.00153184	GC004s3	GC004s6	GC005s5	GC007s3P
26	4	1e-008	0.00153184	GC004s1	GC004s6	GC005s5	GC007s3P
27	4	1e-008	0.00153184	GC003s3	GC004s6	GC005s5	GC007s3P
28	4	1e-008	0.00153184	GC003s7	GC004s6	GC005s5	GC007s4P
29	4	1e-008	0.00153184	GC003s8	GC004s6	GC005s5	GC007s3P

The top level 10 minimal cut sets contain the following relevant events:

ID	Event title		Probability
GC001s1	1.1 – Inaccurate weather forecast available at flight preparation	Constant	0.05
GC001s5	1.5 – Crew performs inappropriate approach preparation	Constant	0.05
GC001s6	1.6 – Crew fails to revise approach strategy, following ATC change request	Constant	0.05
GC003s6	3.6 – ATC requests late RWY change	Constant	0.03
GC004s2	4.2 – Excessive or unstable lateral and vertical path	Constant	0.05
GC004s6	4.6 – No go around	Constant	0.1
GC005s1	5.1 – Inappropriate flare and touchdown	Constant	0.1
GC005s2	5.2 – Inappropriate controls take over (or dual inputs on controls)	Constant	0.08

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

GC005s3	5.3 – Inappropriate use of automation close to flare	Constant	0.005
GC005s5	5.5 – Absence of rejected landing	Constant	0.001
GC007s3P	7.3P – Delayed or inappropriate braking - Partial loss	Constant	0.01
GC007s4P	7.4P – Inadvertent A/BRK deactivation (if A/BRK used) - Partial loss	Constant	0.02

Table 19: Contributing Factors in top 10 Minimal Cut Sets of MAC model.

4.2.3.4. Results

The following table shows the results for the top level Runway Excursion risk in case individual events have a probability of 0. It also shows the change with respect to the top level risk, which is 5.9E-06 per flight.

Event id	Event name	Original RE risk	New RE risk	Change
GC001s1	1.1 – Inaccurate weather forecast available at flight preparation	6.53E-06	5.85E-06	-10%
GC001s5	1.5 – Crew performs inappropriate approach preparation	6.53E-06	6.38E-06	-2%
GC001s6	1.6 – Crew fails to revise approach strategy, following ATC change request	6.53E-06	6.38E-06	-2%
GC003s6	3.6 – ATC requests late RWY change	6.53E-06	6.44E-06	-1.4%
GC004s2	4.2 – Excessive or unstable lateral and vertical path	6.53E-06	6.38E-06	-2%
GC004s6	4.6 – No go around	6.53E-06	5.59E-06	-14%
GC005s1	5.1 – Inappropriate flare and touchdown	6.53E-06	3.53E-06	-46%
GC005s2	5.2 – Inappropriate controls take over (or dual inputs on controls)	6.53E-06	4.13E-06	-37%
GC005s3	5.3 – Inappropriate use of automation close to flare	6.53E-06	6.38E-06	-2%
GC005s5	5.5 – Absence of rejected landing	6.53E-06	6.06E-09	-99.9%
GC007s3P	7.3P – Delayed or inappropriate braking - Partial loss	6.53E-06	4.36E-06	-33%
GC007s4P	7.4P – Inadvertent A/BRK deactivation (if A/BRK used) - Partial loss	6.53E-06	2.18E-06	-67%

Table 20: Resulting RE accident probability after setting Contributing Factors probability to 0.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

As can be observed from the differences found, all differences are negative, i.e., the top level risk reduces by inhibiting the individual events, as can be expected. Also, there is only 1 impacting events in the range of -50% to -100% risk reduction.

4.2.3.5. Discussion

The results of the verification of the usability of the MAC and RE models are provided in Table 18 and Table 20. In those tables it can be found that by setting individual probabilities of Contributing Factors 0, the top level MAC and RE accident probabilities decrease. This also expected: if failures do not exist anymore, the top-level event of the fault tree should decrease. This provides confidence in the right implementation of the logic of the model even if only a subset of the Contributing Factors has been used for the exercise.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

5 CONCLUSIONS

The main purpose for this study has been the integration of the domain-specific risk assessment models, developed in Future Sky Safety P4, into an integrated risk assessment framework.

The ICAO Safety Management Manual (DOC 9859), see [2], provides guidelines on safety management fundamentals. A uniform and complete approach should be envisaged at European level.

This document presents the approach definition to integrate various aviation risks models and to implement the defined approach in the risk observatory. The integration of the domain-specific risk assessment models implies the need to characterize events and associated probabilities, as well as the integration of dynamic complex systems into distinct modules. First, the distinct models were interconnected through interface models. A backbone model approach was used to develop a framework able to integrate risk models from various aviation domains. Results are provided on implementation of this framework in terms of definition of common formats, conversion rules between aviation domain safety indicators, treatment of influencing factors and common causes, management of the uncertainty on the data used to compute safety indicators, and identification of candidates for safety indicator computation tools.

Next, the development of processes for updating the integrated risk assessment framework was considered, playing a critical role in assuring the reliability of the framework, therefore during this part of the study, to assure the reliability of the framework, three update processes are considered, namely: risk scenario creation, model refinement and model update. The framework is though in a way that, ideally, can make these processes use as inputs observed data and relevant external systems. Nevertheless, as these systems or connections may be difficult to accomplish, manual processes are also considered.

Finally, the conceptual framework for risk assessment was verified, by comparing predicted performance indicators with a quantitative verification of the backbone model and a verification of the usability of the framework. A comparison with real data was found to be non-feasible.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

6 REFERENCES

[1] Future Sky Safety - Annex 1 - Description of Action (part A).

[2] ICAO Safety Management Manual (SMM) - 3rd Edition - Doc 9859 AN /460, 2013.

[3] FSS_P4_CIRA_D4.1 - Risk Observatory Requirements, Version v2.0, Issued 26-10-2015.

[4] FSS_P4_INTA_D4.4.1 - Risk model gap analysis, Version v1.0, Issued 24-10-2015.

[5] FSS_P4_NLR_D8.1 - Project Plan P4 Total System Risk Assessment, D8.1-Appendix P4, Version V3.0, Issued 08-12-2015.

[6] Spouge, J. and Perrin, E. , 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, 2006.

[7] B. Ale, L. Bellamy, R. Cooke, M. Duyvis, D. Kurowicka, C. Lin, O. Morales, A. Roelen, and J. Spouge, Causal model for air transport safety, Ministerie van Verkeer en Waterstaat, Directoraat-Generaal Luchtvaart en Maritieme Zaken, 2008.

[8] EASA - CS25.1309 Certification Specifications for Large Aeroplanes CS-25 Amendment 20, 24 August 2017.

[9] Open-PSA model exchange format version 2.0d : https://github.com/open-psa

[10] S. Noh and J. Shortle, Application of Common Cause Failure Methodology to Aviation Safety Assessment Model, ICRAT 2016.

[11] EUROCAE ED-161 - Safety and Performance and Interoperability Requirements Document for ADS-B-RAD Application, 1st of September 2009.

[12] XFTA, see http://www.altarica-association.org/members/arauzy/Software/XFTA.html.

[13] ARBRE ANALYSTE: A FAULT TREE ASSESSMENT SOFTWARE FULLY COMPLIANT WITH OPEN-PSA AND USING XFTA FAULT TREE ENGINE - Congrès LAMBDA-MU 19 (October 2014).

[14] Arbre-analyste, see http://www.arbre-analyste.fr/

[15] B. Iooss and P. Lemaître, A Review on Global Sensitivity Analysis Methods. In G. Dellino and C. Meloni, editors, Uncertainty Management in Simulation-Optimization of Complex Systems: Algorithms and Applications, chapter 5, pages 101–122. Springer US, Boston, MA, 2015.

[16] W. Hoeffding, A class of statistics with asymptotically normal distributions, Annals of Mathematical Statistics, vol. 19, pp. 293–325, 1948.

[17] I. Sobol and S. Kuchereko, Sensitivity estimates for non-linear mathematical models, Mathematical Modelling and Computational Experiments, vol. 1, pp. 407–414, 1993.

[18] A. Saltelli, Making best use of model evaluation to compute sensitivity indices, Computer Physics Communication, vol. 145, pp. 280–297, 2002.

[19] European Commission Flight Path 2050 Europe's Vision for Aviation, Report of the High Level Group on Aviation Research. European Union 2011, ISBN 978-92-79-19724-6; DOI 10.2777/50266.

[20] EASA, Annual Safety Review 2017, 2018.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

[21] D. Barry, FSS P3 D3.10 – Assessing the relative risk of landing veer-off associated with a given set of conditions, FDM workshop, 26th September, 2018.

[22] A. Balk, R. Wever, G. Greene, Total Aviation System Risk Picture 2016, FSS-P4 D4.3, version 2.0, December 2016.

[23] A. Balk, Total Aviation System Risk Picture 2017, FSS-P4 D4.6, version 0.1, 2018.

[24] J. Verstraeten, A. Vozella, E. Perrin, T.A. Rebelo, G.B. van Baren, T. v. Birgelen, M. Morel, FSS - Project Plan P4, Total system risk assessment, FSS Deliverable D8.1, Version 3.0, December 2015.

[25] MAC model - BackBone MAC v5.2, FaultTreeDistribution 180924; FSSP4-MACER_Contributing factors_Backbone 180423influencesadded.xlsx FSS; T4.2.5 Influencing Factors_MAC_4 July 2018.xlsx.

[26] RE model - BackBone RE, FaultTreeDistribution 180924, FSS T4.2.5 Contributing Factors_RE_18_Sept 2018.xls, FSS T4.2.5 Influencing Factors_RE_4 July 2018.xlsx.

[27] W. Rouwhorst, Draft notes of the FSS-P4-Progress Session held at 24th July 2018.

[28] GITLAB, see https://about.gitlab.com/

[29] ICAO Annex 14, Aerodromes, Volume1, Seventh Edition, July 2016.

[30] SCRAM, see https://scram-pra.org/

[31] SESAR P16.01.01 Final Project Report (D23) on Accident Incident Model and Enhanced Safety Target Achievement Roadmap, Issue 1, Edition 00.01.00, 18/08/2014.

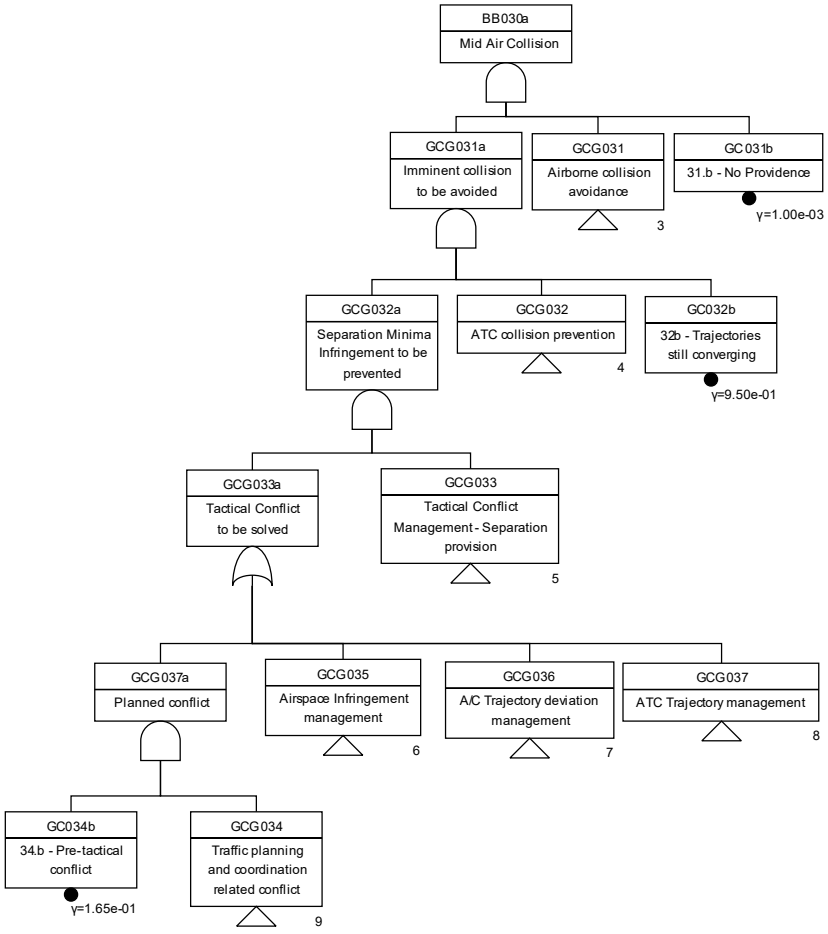
This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Appendix A INTEGRATED RISK ASSESSMENT FRAMEWORK DETAILS

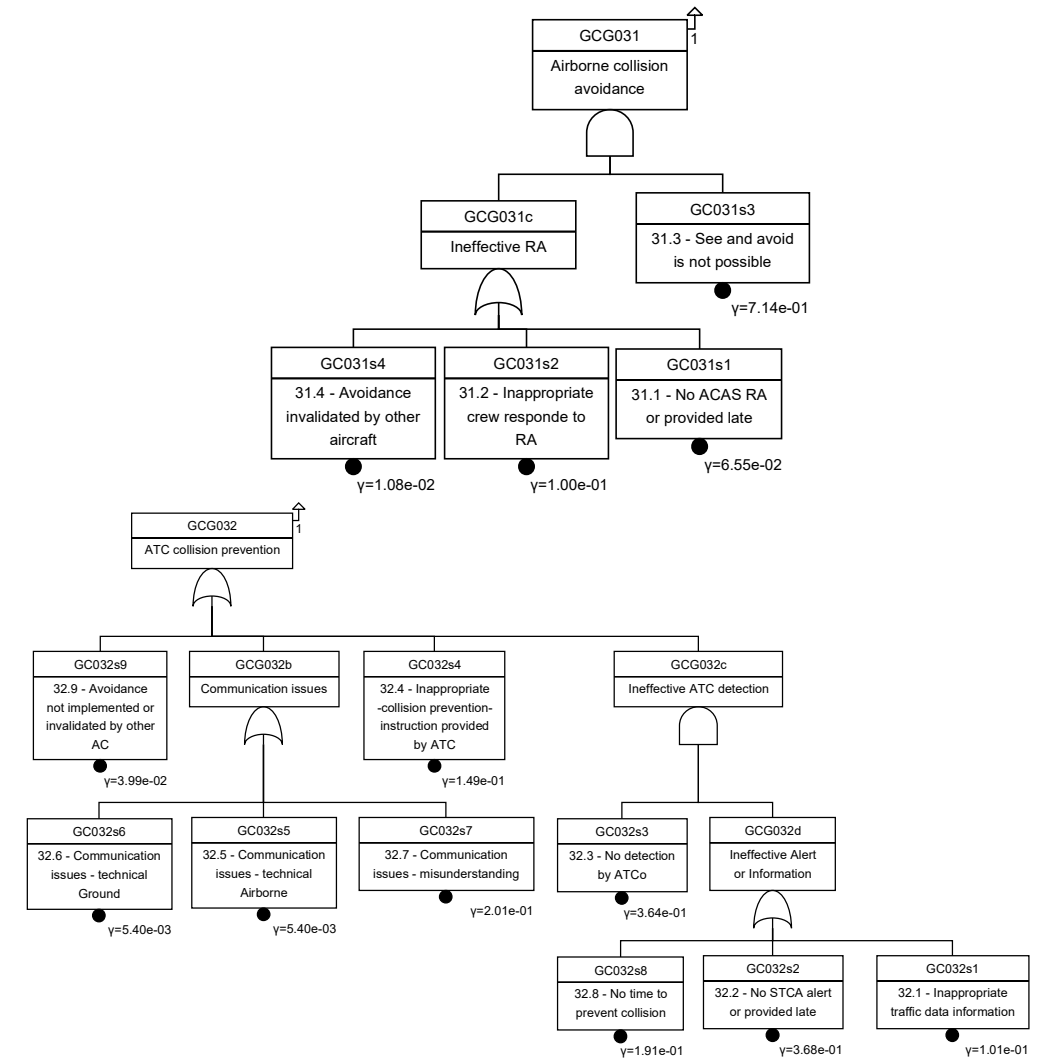
This appendix contains technical details related with the development of the Integrated Risk Assessment Framework.

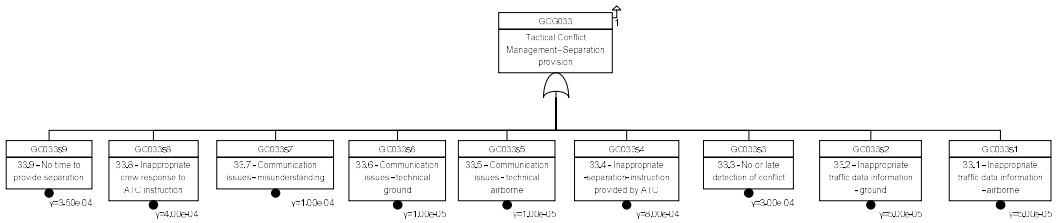
Appendix A.1 Backbone Models

Appendix A.1.1 MAC-ER Backbone fault-trees

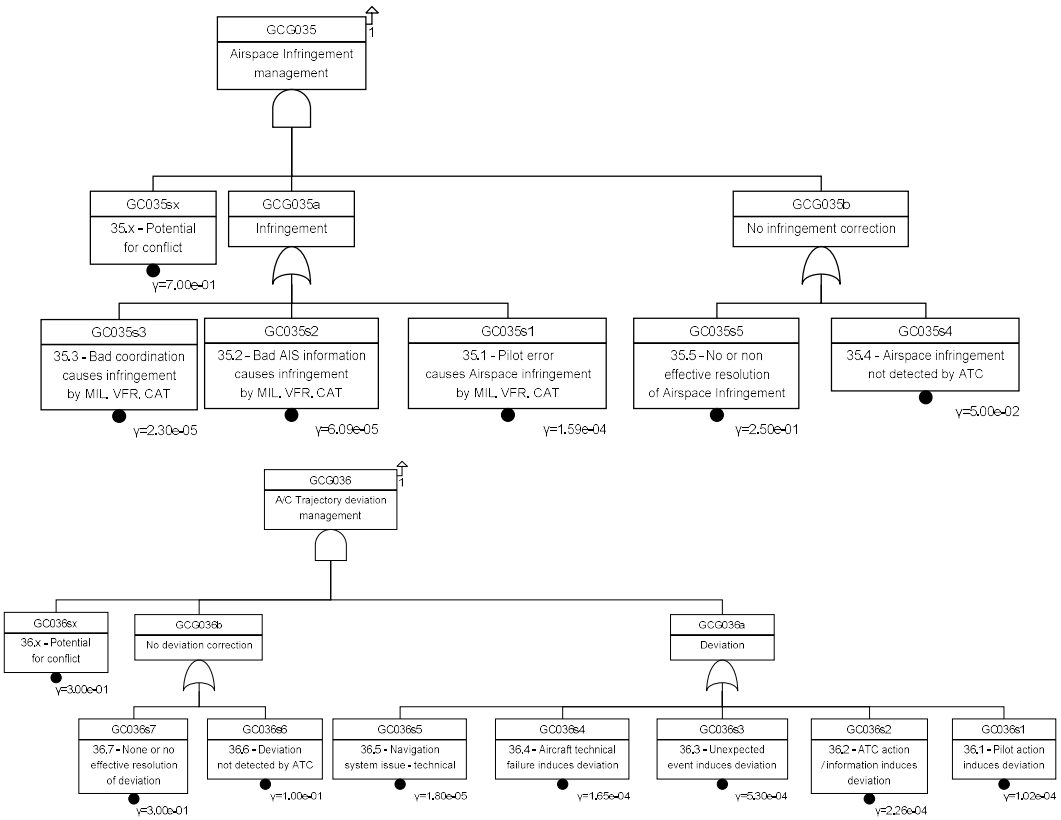


This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

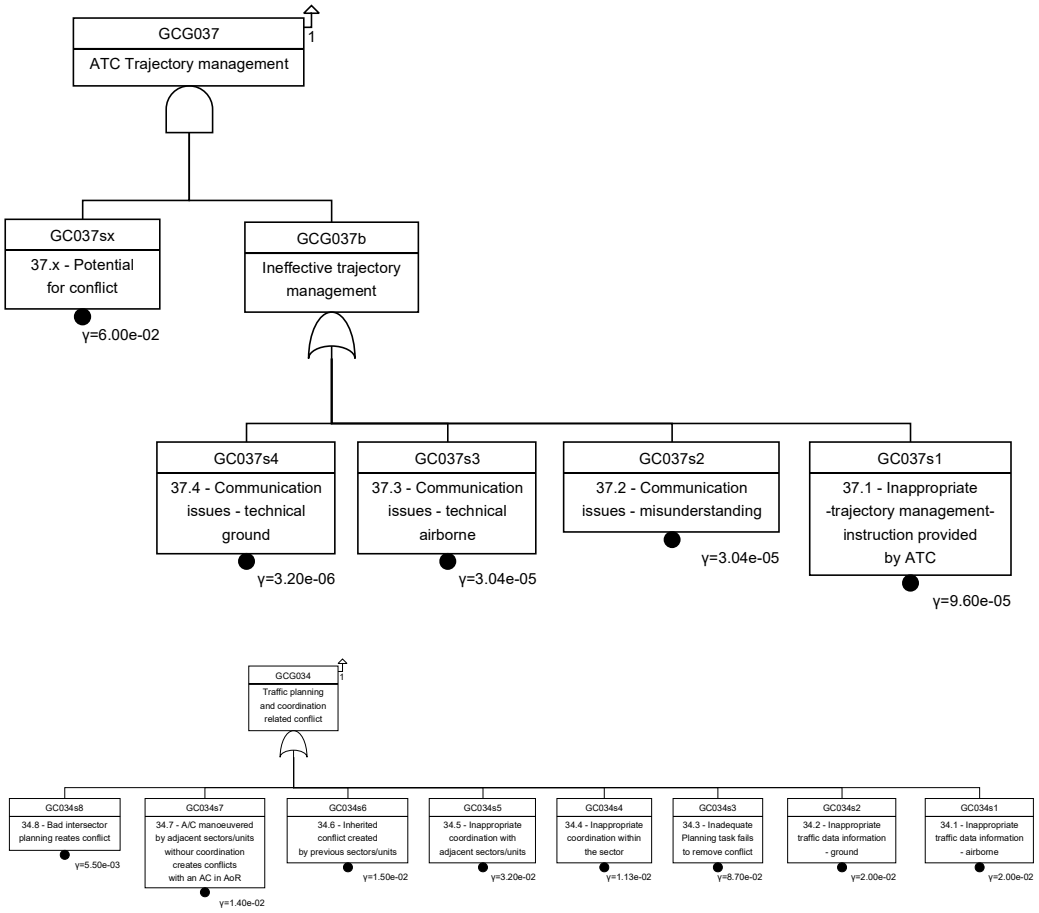




This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

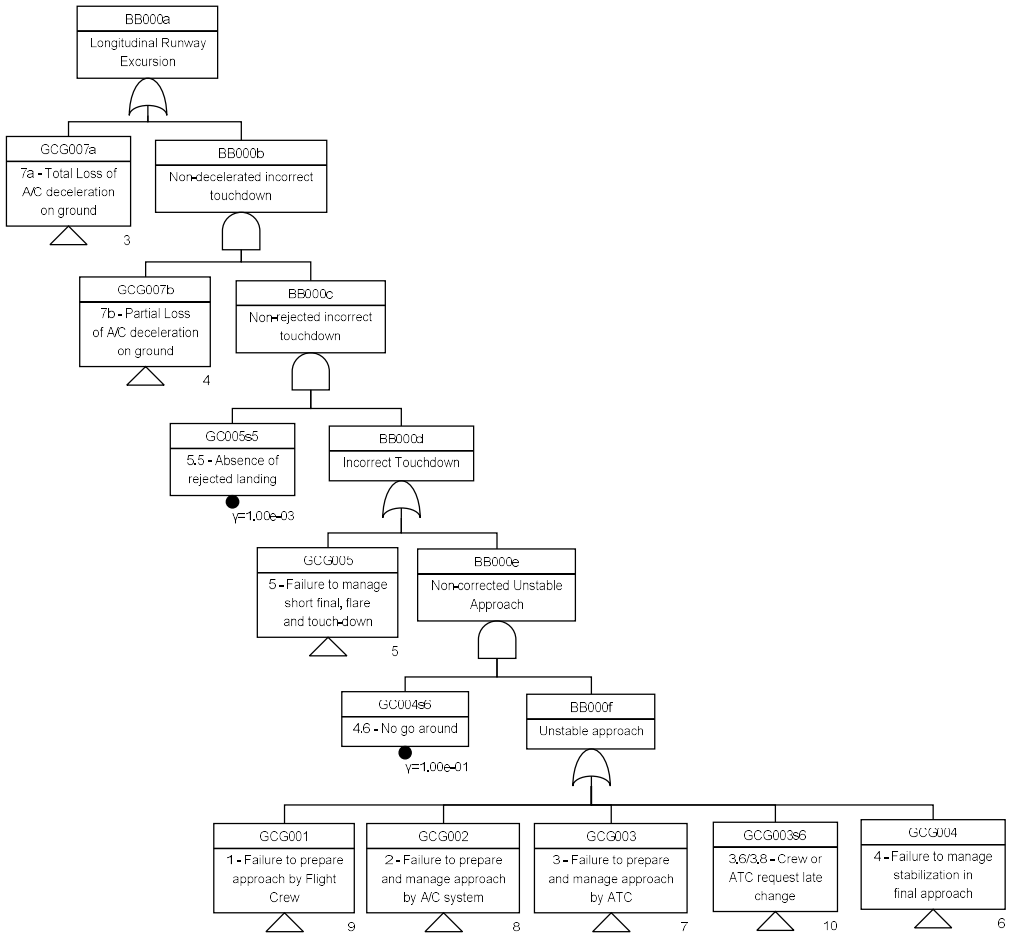


This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

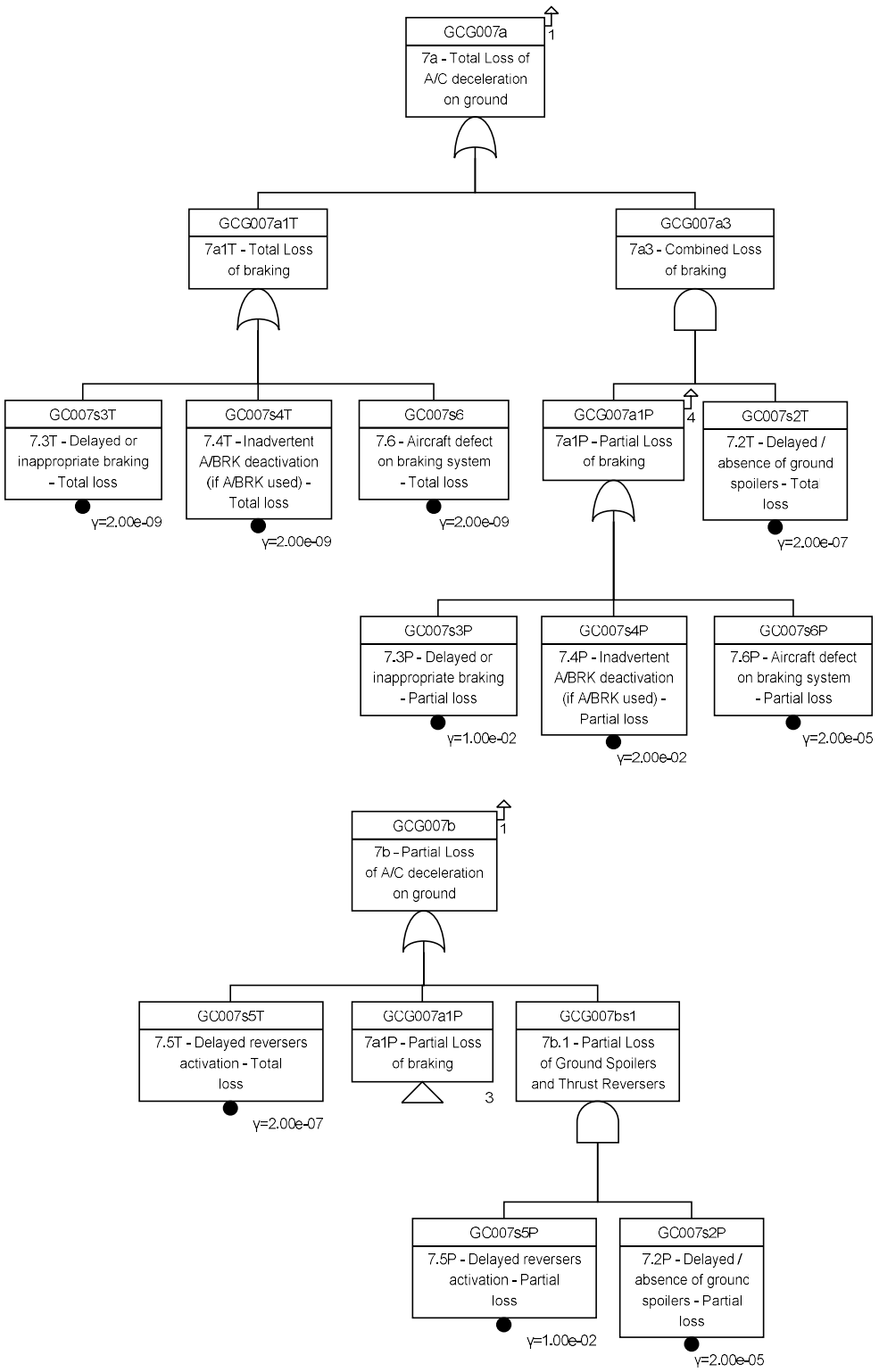


This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

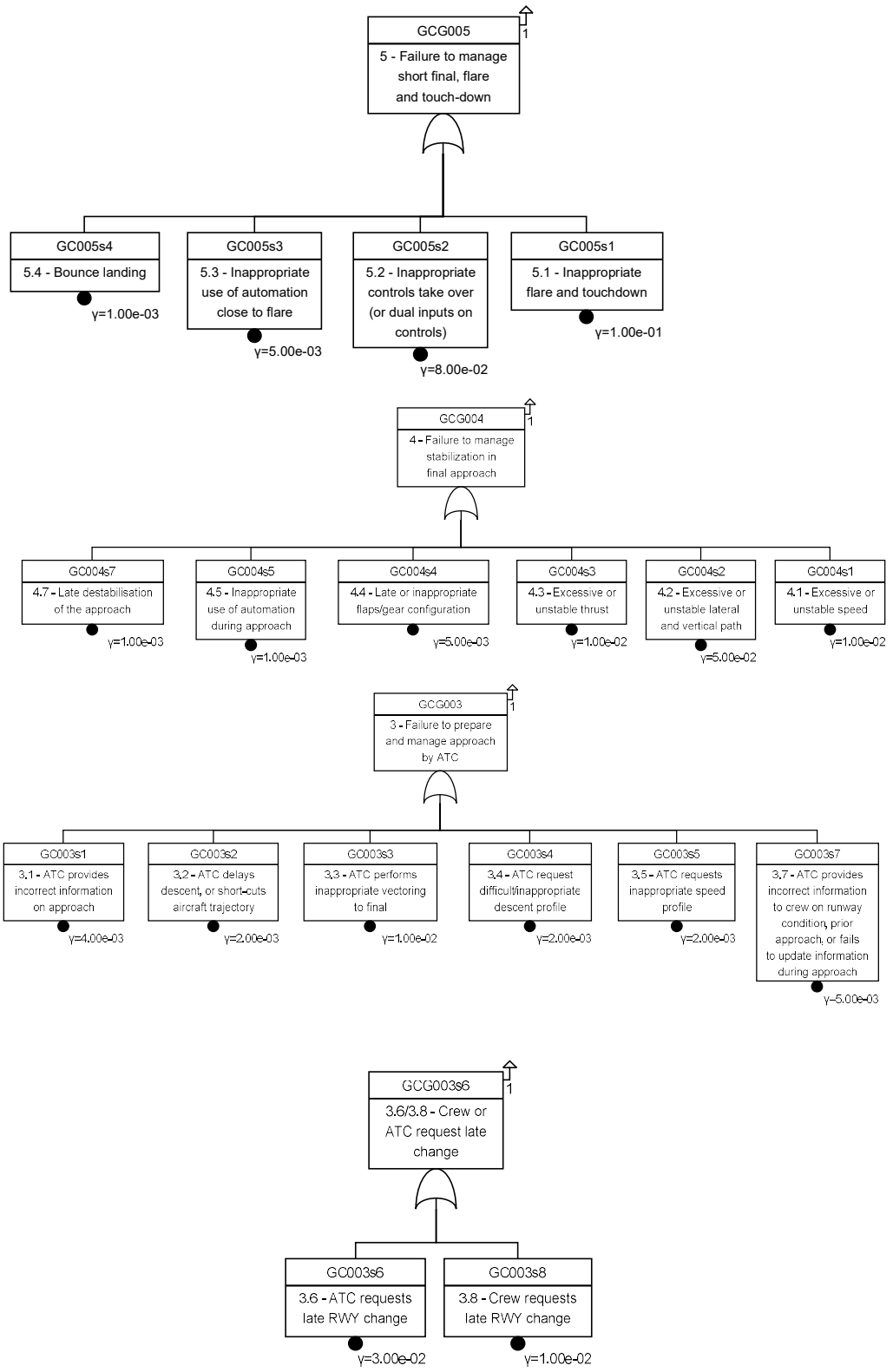
Appendix A.1.2 Runway Excursion Backbone fault-trees



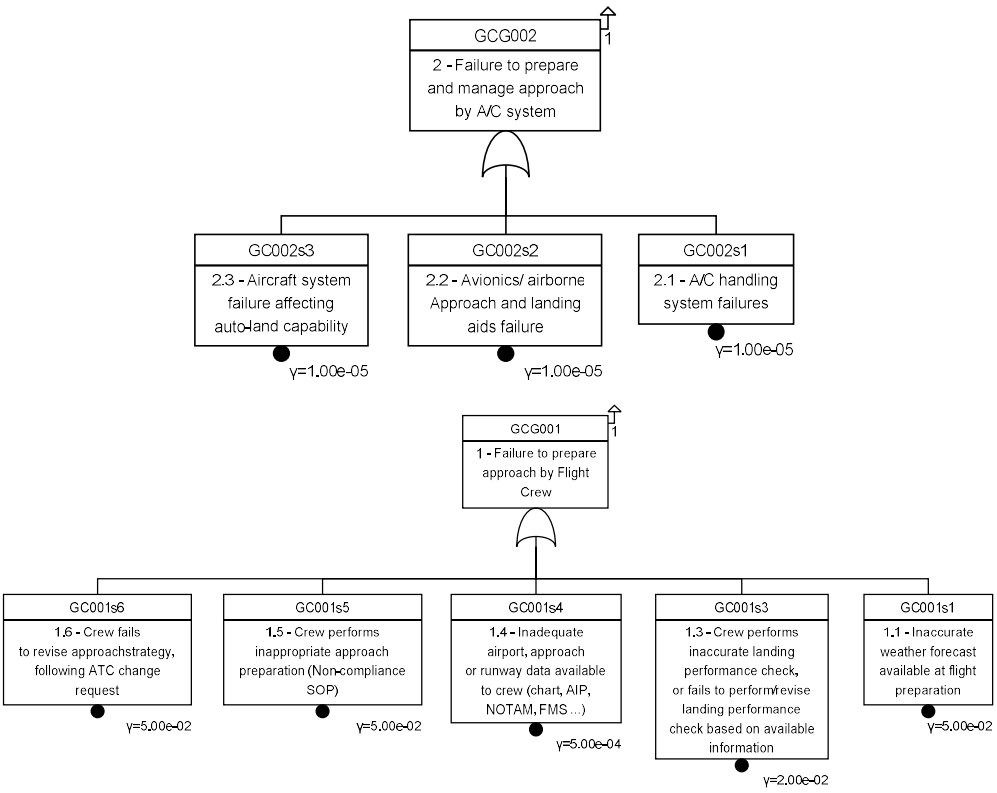
This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.



This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.



This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.



This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Appendix A.2 Table of Influencing Factors, rectified weights and mapped Generic Contributing Factors

This appendix gives detailed explanations illustrated by simple examples on the way to build the two following tables related to the risk of runway excursion and modify their content if necessary:

- The first table includes the rectified weights associated to each Influencing Factor (IF)
- The second table provides a mapping between the Generic Contributing Factors applicable to the risk of runway excursion and their linked IF's.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Table 21: Influencing Factors for MAC with their associated rectified weights

Ref.	Influencing Factors applicable to MAC-ER	Attribute	Definition	Weight	Rate of occurrence	Rectified weight
501	**WEATHER** (500.1, 500.2 and 500.3). Refer to Excel	-	-	-	-	
501.4	Darkness during flight (winter 20%	Northern EUROPE		1,15	35,0%	-
501.4	Darkness during flight (winter 20%	Southern EUROPE		0,95	65,0%	-
501.4 MAC	**Darkness during flight**	-	-	-	100%	**1,02**
501.5	IMC during flight	High (worse since < VFR	> 0.25	1,1	10,0%	-
501.5	IMC during flight	Medium	0.10 - 0.25 (ECAC 0.15)	1	70,0%	
501.5	IMC during flight	Low (better since > VFR	< 0.10	0,95	20,0%	
501.5 MAC	**IMC during flight**	-	-	-	100%	**1**
501.6	Storm clouds along route (winter 15%	High	> 0.04	1,25	5,0%	-
501.6	Storm clouds along route (winter 15%	Medium	0.01 - 0.04 (ECAC 0.02)	1	60,0%	
501.6	Storm clouds along route (winter 15%	Low	< 0.01	0,95	35,0%	
501.6 MAC	**Storm clouds along route**	-	-	-	100%	**0,995**

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to MAC-ER	Attribute	Definition	Weight	Rate of occurrence	Rectified weight
503	**CREW PERFORMANCE (GROUND STAFF, only).** See Excel file of IF's	-	-	-	-	
503.7	ATC training level	High	99%+	0,95	4,0%	-
503.7	ATC training level	Medium	97.5% - 99% (ECAC 98%)	1	94,0%	-
503.7	ATC training level	Low	< 97.5%	1,35	2,0%	-
503.7 MAC	**ATC training level**	-	-	-	100%	**1,005**
503.8	ATC experience level	High	> 95%	0,9	5,0%	-
503.8	ATC experience level	Medium	85% < ATC experience level < 95% (ECAC 87%)	1	90,0%	
503.8	ATC experience level	Low	< 85%	1,1	5,0%	
503.8 MAC	**ATC experience level**	-	-	-	100%	**1**
503.9	ATC situation awareness	High vigilance	Peak traffic - Expected	1,05	18,0%	-
503.9	ATC situation awareness	Normal vigilance	Normal traffic - Expected	0,95	80,0%	
503.9	ATC situation awareness	Low vigilance	Below Expected	1,5	2,0%	
503.9 MAC	**ATC situation awareness**	-	-	-	100%	**0,979**
504	**OPERATIONAL**	-	-	-	-	-
504.1	Airspace	Upper airspace	IFR Aircraft ≥ FL240 not in TMA	0,9	58,0%	-
504.1	Airspace	Lower airspace	IFR Aircraft ≤ FL240 not in TMA	1,1	42,0%	-
504.1 MAC	**Airspace**	-	-	-	100%	**0,984**

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to MAC-ER	Attribute	Definition	Weight	Rate of occurrence	Rectified weight
504.2	Traffic level	High	> 5 sector occupancy	1,2	7,0%	-
504.2	Traffic level	Medium	2-5 sector occupancy	1,1	23,0%	-
504.2	Traffic level	Low	< 2 sector occupancy	0,9	70,0%	-
504.2 MAC	**Traffic level**	-	-	-	100%	**0,967**
504.3	Traffic complexity	High	Area Control Surveillance (ACS) rating > 7.0	1,3	15,0%	-
504.3	Traffic complexity	Medium	ACS rating 4.00-7.00 (ECAC 5.90)	1	46,0%	
504.3	Traffic complexity	Low	ACS rating < 4.0	0,8	39,0%	-
504.3 MAC	**Traffic complexity**	-	-	-	100%	**0,967**
504.4	Traffic saturation	High	> 2.5	1,1	15,0%	-
504.4	Traffic saturation	Medium	1-2.5 (ECAC 1.37)	1	65,0%	-
504.4	Traffic saturation	Low	< 1	0,9	20,0%	-
504.4 MAC	**Traffic saturation**	-	-	-	100%	**0,995**
504.5	Traffic variability	High	> 1.3	1,25	12,0%	-
504.5	Traffic variability	Medium	1.10-1.30 (ECAC 1.22)	0,95	80,0%	
504.5	Traffic variability	Low	1.00-1.10	0,8	8,0%	-
504.5 MAC	**Traffic variability**	-	-	-	100%	**0,974**
504.6	Airspace routing (sector based)	High	High No's crossing points plus traffic concentration	1,3	20,0%	-

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to MAC-ER	Attribute	Definition	Weight	Rate of occurrence	Rectified weight
504.6	Airspace routing (sector based)	Medium	High No's crossing points or traffic concentration	0,9	65,0%	
504.6	Airspace routing (sector based)	Low	Neither High No's crossing points nor traffic concentration	0,7	15,0%	-
504.6 MAC	**Airspace routing (sector based)**	-	-	-	100%	**0,95**
504.7	Airspace complexity (sector based)	High	Division into sectors complex and traffic flows complex	1,2	12,0%	-
504.7	Airspace complexity (sector based)	Medium	Division into sectors complex or traffic flows complex	1	58,0%	-
504.7	Airspace complexity (sector based)	Low	Neither Division into sectors complex nor traffic flows complex	0,85	30,0%	-
504.7 MAC	**Airspace complexity**	-	-	-	100%	**0,979**
504.8	Shared airspace	Very high	High Military VFR and GA-IFR demand	1,5	2,0%	
504.8	Shared airspace	High	Any 2 of above	1,2	8,0%	
504.8	Shared airspace	Medium	Any 1 of above	1	55,0%	
504.8	Shared airspace	Low	None of above	0,85	35,0%	
504.8 MAC	**Shared airspace**	-	-	-	100%	**0,9735**

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to MAC-ER	Attribute	Definition	Weight	Rate of occurrence	Rectified weight
505	**SYSTEM PERFORMANCE**	-	-	-	-	
505.1	STCA coverage	High	> 98%	0,9	10,0%	-
505.1	STCA coverage	Normal	90%-98% ECAC (2005 85%, nowabout 95%)	1	85,0%	-
505.1	STCA coverage	Low	< 90%	1,25	5,0%	-
505.1 MAC	**STCA coverage**	-	-	-	100%	**1,0025**
505.2	Surveillance quality	High	> 99.9%	0,95	4,0%	-
505.2	Surveillance quality	Normal	99.7%-99.9% (ECAC 99.8%)	1	95,0%	
505.2	Surveillance quality	Low	99%-99.7%	2,5	0,9%	
505.2	Surveillance quality	Outage	0% < Surveillance quality < 99%	10	0,0%	
505.2	Surveillance quality	Loss	0%	100	0,0%	-
505.2 MAC	**Surveillance quality**	-	-	-	100%	**1,0123475**
505.3	Plan data quality	High	> 99.5%	0,95	8,0%	-
505.3	Plan data quality	Normal	98% < Plan data quality < 99.5% (ECAC 98.7%)	1	90,0%	
505.3	Plan data quality	Low	0%-98%	1,2	2,0%	
505.3	Plan data quality	Loss	0%	5	0,0%	
505.3 MAC	**Plan data quality**	-	-	-	100%	**1,00019**
505.4	TCAS equipage	TCAS X	Not yet introduced	0,9	0,0%	-
505.4	TCAS equipage	TCAS 3		1	98,0%	-
505.4	TCAS equipage	TCAS 1 (TA only)		1,2	1,5%	

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to MAC-ER	Attribute	Definition	Weight	Rate of occurrence	Rectified weight
505.4	TCAS equipage	No TCAS		1,5	0,5%	-
505.4 MAC	**TCAS equipage**	-	-	-	100%	**0,9875**
505.5	Level of ATC evolution	High (worse)	> 1 major change	1,3	2,0%	-
505.5	Level of ATC evolution	Medium	1 major change (ECAC 0.2)	1	10,0%	
505.5	Level of ATC evolution	Low	No changes	0,9	88,0%	-
505.5 MAC	**Level of ATC evolution**	-	-	-	100%	**0,918**
506	**ATC WORKLOAD**	-	-	-	-	
506.1	Handover score	High	> 15%	1,2	4,0%	-
506.1	Handover score	Medium	5-15% (ECAC 10%)	1	55,0%	-
506.1	Handover score	Low	< 5%	0,95	41,0%	-
506.1 MAC	**Handover score**	-	-	-	100%	**0,9875**
506.2	RTC Score	High	> 3	1,15	10,0%	-
506.2	RTC Score	Medium	1-3 (ECAC 1.9)	1	85,0%	
506.2	RTC Score	Low	< 1	0,9	5,0%	-
506.2 MAC	**RTC Score**	-	-	-	100%	**1,01**
506.3	Instruction score	High	> 2	1,25	5,0%	-
506.3	Instruction score	Medium	0.5-2 (4 ANSP data)	1	75,0%	-
506.3	Instruction score	Low	< 0.5	0,8	20,0%	-
506.3 MAC	**Instruction score**	-	-	-	100%	**0,9725**
506.4	Demand score	Short	< 1 minute (4 ANSP data)	1,1	20,0%	-
506.4	Demand score	Long	≥ 1 minute	1	80,0%	-

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to MAC-ER	Attribute	Definition	Weight	Rate of occurrence	Rectified weight
506.4 MAC	**Demand score**	-	-	-	100%	**1,02**
506.5	Conflict score	High	> 0.2	1,3	10,0%	-
506.5	Conflict score	Few/ Limited	≤ 0.2 (4 ANSP data)	1	90,0%	-
506.5 MAC	**Conflict score**	-	-	-	100%	**1,03**
506.6	Peak traffic score	High	> 8%	1,1	5,0%	-
506.6	Peak traffic score	Moderate	2%-8% (Expert judgement)	1	65,0%	-
506.6	Peak traffic score	Low	< 2%	0,95	30,0%	-
506.6MAC	**Peak traffic score**	-	-	-	100%	**0,99**
506.7	Overload score	Often saturated	> 12.0 (more than once per month) (Expert judgement)	2	3,0%	-
506.7	Overload score	Occasionally saturated	0 < score < 12.0 (up to once per month)	1	90,0%	
506.7	Overload score	Not saturated	0 (never)	0,9	7,0%	-
506.7 MAC	**Overload score**	-	-	-	100%	**1,023**

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Table 22: Influencing Factors for RWY Exc with their associated rectified weights

Ref.	Influencing Factors applicable to Runway Excursions	Abbreviation	Attribute	Definition	Weight	Rate of occurrence winter period	Rate of occurrence summer period	Average rate	Rectified weight
500	**RUNWAY**	-	-	-	-	-	-	-	-
500.1	Runway surface quality	RWY-SURF	Good	Fully in line with ICAO Annex 14 requirements Good draining and braking efficiency when wet.	1	90%	N/A	90%	-
500.1	Runway surface quality	RWY-SURF	Poor	Does not respect ICAO Annex 14 requirements Deteriorated pavement Deteriorated braking action, poor draining when wet.	1,1	10%	N/A	10%	-
500.1	**Runway surface**	**RWY-SURF**	-	-	-	100%	-	100%	**1,01**
500.2	Runway length	RWY-LGTH	Long	RWY length is > 1500 m (Light and long propeller A/C) RWY length is > 2500 m (Light jet A/C) RWY length is > 2600 m (Medium jet	1	40%	N/A	40%	-

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to Runway Excursions	Abbreviation	Attribute	Definition	Weight	Rate of occurrence winter period	Rate of occurrence summer period	Average rate	Rectified weight
500.2	Runway length	RWY-LGTH	Medium	1000 m < RWY length is < 1500 m (Light and long propeller A/C) 1500 m < RWY length is < 2500 m (Light jet A/C) 1800 m < RWY length is < 2600 m (Medium jet A/C) 2200 m < RWY length is < 3000	1,3	40%	N/A	40%	-
500.2	Runway length	RWY-LGTH	Short	RWY length is < 1000 m (Light and long propeller A/C) RWY length is < 1500 m (Light jet A/C) RWY length is < 1800 m (Medium jet	1,5	20%	N/A	20%	-
500.2	**Runway length**	**RWY-LGTH**	-	-	-	100%	-	100%	**1,22**
500.3	Runway width	RWY-WDTH	Normal	RWY width ≥ 30 m (Light A/C) RWY width ≥ 45 m (Medium and Heavy A/C)	1	75%	N/A	75%	-
500.3	Runway width	RWY-WDTH	Narrow	RWY width < 30 m (Light A/C) RWY width < 45 m (Medium A/C) - N/A for heavy A/C	1,5	25%	N/A	25%	-

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to Runway Excursions	Abbreviation	Attribute	Definition	Weight	Rate of occurrence winter period	Rate of occurrence summer period	Average rate	Rectified weight
500.3	**Runway width**	**RWY-WDTH**	-	-	-	100%	-	100%	**1,125**
500.4	Runway slope	RWY-SLPE	Normal	-0.2% ≤ Slope ≤ +0.2%	1	75%	N/A	75%	-
500.4	Runway slope	RWY-SLPE	Downslope	Slope < -0.2%	1,1	20%	N/A	20%	-
500.4	Runway slope	RWY-SLPE	Upslope	Slope > +0.2%	0,9	5%	N/A	5%	-
500.4	**Runway slope**	**RWY-SLPE**	-	-	-	100%	-	100%	**1,015**
500.5	Runway lighting	RWY-LTG-NALS	NALS Day-Good	No lighting (airport not equipped)	1	10%	N/A	10%	-
500.5	Runway lighting	RWY-LTG-NALS	NALS Day-Poor	No lighting (airport not equipped)	1,2	5%	N/A	5%	-
500.5	Runway lighting	RWY-LTG-BALS	BALS Day/ Night-Good	High intensity approach Lighting System (HIALS) between 210 and 419 m either during days or	1	60%	N/A	60%	-
500.5	Runway lighting	RWY-LTG-BALS	BALS Day-Poor	High intensity approach Lighting System (HIALS) between 210 and 419 m during days	1,1	25%	N/A	25%	-
500.5	**Runway lighting**	**RWY-LTG**	-	-	-	100%	-	100%	**1,035**
500.6	Runway Visual Path Guidance	RWY-VISAID	Good	Well-calibrated PAPI in accordance with	1	80%	N/A	80%	-
500.6	Runway Visual Path Guidance	RWY-VISAID	Medium	Visual aid other than	1,1	10%	N/A	10%	-
500.6	Runway Visual	RWY-VISAID	Poor	No visual aid	1,2	10%	N/A	10%	-
500.6	**Runway Visual**	**RWY-VISAID**	-	-	-	100%	-	100%	**1,03**

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to Runway Excursions	Abbreviation	Attribute	Definition	Weight	Rate of occurrence winter period	Rate of occurrence summer period	Average rate	Rectified weight
501	**WEATHER**	-	-	-	-	-	-	-	-
501.1	wind	WIND	Moderate head	Less than 25 kt	0,9	80%	84%	82%	-
501.1	wind	WIND	Strong head	More than 25 kt	0,7	14%	10%	12%	-
501.1	wind	WIND	Moderate tail wind	Less than 10 kt	1,1	5%	5%	5%	-
501.1	wind	WIND	Strong tail wind	More than 10 kt	1,3	1%	1%	1%	-
501.1	wind	WIND	Moderate cross wind (not used	Less than 18 KT	1	0%	0%	0%	-
501.1	wind	WIND	Strong cross	More than 18 KT	1	0%	0%	0%	-
501.1	**WIND**	**WIND**	-	-	-	100%	100%	100%	**0,89**
501.2	Wind shear / Turbulence	WDSHEAR-TURB	None/light	No turbulence is felt by the occupants, smooth aircraft behaviour. In case of light turbulence, slight, erratic	1	80%	90%	85%	-
501.2	Wind shear / Turbulence	WDSHEAR-TURB	Moderate	Changes in altitude and/ or attitude with more intensity than light turbulence. Aircraft	1,1	19,5%	9,5%	14,5%	-

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to Runway Excursions	Abbreviation	Attribute	Definition	Weight	Rate of occurrence winter period	Rate of occurrence summer period	Average rate	Rectified weight
501.2	Wind shear / Turbulence	WDSHEAR-TURB	Severe	Turbulences that cause large, abrupt changes in altitude and/ or attitude. It usually causes large variations in airspeed. Occupants may be forced violently against their seat belts	1,2	0,5%	0,5%	0,5%	-
501.2	**Wind shear /**	**WDSHEAR-TURB**	-	-	-	100%	100%	100%	**1,01**
501.3	Ceiling - Visibility	WIND-VISI	IFR	(Instrument Flight Rules): 1,5 Probabilistic Safety AssessmentFt - 1000 Ft AGL (Above Ground Level)	1	85%	95%	90%	-
501.3	Ceiling - Visibility	WIND-VISI	LIFR	(Low Instrument Flight Rules): Less than 1,5 km OR less than 500 Ft AGL (Above Ground	1,2	15%	5%	10%	-
501.3	**Ceiling -**	**WIND-VISI**	-	-	-	100%	100%	100%	**1,02**
502	**RUNWAY**	-	-	-	-	-	-	-	-
502.1	Runway surface condition	RWY-COND	Very Good	Dry	1	50%	80%	65%	-

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to Runway Excursions	Abbreviation	Attribute	Definition	Weight	Rate of occurrence winter period	Rate of occurrence summer period	Average rate	Rectified weight
502.1	Runway surface condition	RWY-COND	Good	Wet up to 3 mm of water Slush up to 3 mm of water Dry snow up to 3 mm of water	1,15	49%	19%	34%	-
502.1	Runway surface condition	RWY-COND	Medium	Dry snow: More than 3 mm up to 100 mm Wet snow: More than 3 mm up to 30 mm Compacted snow: OAT above -15°C Dry snow over compacted snow Wet snow over compacted snow Slippery when wet	1,3	0,5%	0,5%	1%	-
502.1	Runway surface condition	RWY-COND	Poor	Ice (cold & dry) Consequently, braking deceleration is significantly reduced for the wheel braking effort applied.	2	0,5%	0,5%	1%	-

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to Runway Excursions	Abbreviation	Attribute	Definition	Weight	Rate of occurrence winter period	Rate of occurrence summer period	Average rate	Rectified weight
502.1	Runway surface condition	RWY-COND	Nil	Ice (cold & dry) Water on top of compacted snow dry snow or wet snow over ice. Consequently, braking deceleration is minimal to non-	2	0%	0%	0%	-
502.1	**Runway surface**	**RWY-**	-	-	-	100%	100%	100%	**1,05**
503	**CREW**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
503.1	Flight crew experience-CAPT	CREW-EXP-CAPT	Good	Flight hours as Captain are more than 1000 FH AND Flight hours on Aircraft type is more	1	75%	N/A	75%	-
503.1	Flight crew experience-CAPT	CREW-EXP-CAPT	Medium	Flight hours as Captain are more than 1000 FH AND Flight hours on Aircraft type is less	1,05	15%	N/A	15%	-
503.1	Flight crew experience-CAPT	CREW-EXP-CAPT	Low	Flight hours as Captain are less than 1000 FH	1,1	10%	N/A	10%	-

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to Runway Excursions	Abbreviation	Attribute	Definition	Weight	Rate of occurrence winter period	Rate of occurrence summer period	Average rate	Rectified weight
503.1	**Flight crew**	**CREW-EXP-CAPT**	-	-	-	100%	-	100%	**1,01**
503.2	Flight crew experience-F/O	CREW-EXP-F/O	Good	Flight hours as F/O on multi-engine multi-crew are more	1	80%	N/A	70%	-
503.2	Flight crew experience-F/O	CREW-EXP-F/O	Medium	Flight hours as F/O on multi-engine multi-crew are more than 1000 FH AND Flight Hours	1,1	15%	N/A	25%	-
503.2	Flight crew experience-F/O	CREW-EXP-F/O	Low	Flight hours as F/O on multi-engine multi-crew are less than	1,15	5%	N/A	5%	-
503.2 RW	**Flight crew experience-F/O**	**CREW-EXP-F/O**	-	-	-	100%	-	100%	**1,03 25**
503.3	Flight crew fatigue-short-medium haul operation	CREW-FTG-SMH	Low	Normal duty times (no over-night, no extended duty times) Organized schedules allowing for similar sequences (mornings or afternoons) and appropriate rest periods between flights Regular off days	1	75%	65%	70%	-

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to Runway Excursions	Abbreviation	Attribute	Definition	Weight	Rate of occurrence winter period	Rate of occurrence summer period	Average rate	Rectified weight
503.3	Flight crew fatigue-short-medium haul operation	CREW-FTG-SMH	Moderate	Normal duty times, but some exceptions (long flights, over-night, extended duty times). Many short sectors Schedules featuring some occasional difficulties (reduced layover, positioning…) Varying off days	1,05	15%	20%	18%	-
503.3	Flight crew fatigue-short-medium haul operation	CREW-FTG-SMH	High	Numerous long duties involving early start or late arrivals. Frequent duty extensions Over-night flights.	1,1	10%	15%	13%	-
503.3 RW	**Flight crew fatigue-short-**	**CREW-FTG-SMH**	-	-	-	100%	100%	100%	**1,02 125**

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to Runway Excursions	Abbreviation	Attribute	Definition	Weight	Rate of occurrence winter period	Rate of occurrence summer period	Average rate	Rectified weight
503.4	Flight crew fatigue-long haul operation	CREW-FTG-LH	Low	Organized schedules allowing for similar sequences (westbound or eastbound). Limited number of night flights, night departures or night landings. Low/Moderate jetlag No ultra-long flights	1	80%	70%	75%	-
503.4	Flight crew fatigue-long haul operation	CREW-FTG-LH	Moderate	Organized schedules but some disruptions Probabilistic Safety Assessment or exceptions causing tiring flights. Frequent night flights, night departures and arrivals. Some flights operated with limited crew. Schedules featuring some occasional disruptions (reduced layover, positioning…). Frequent heavy jetlag	1,05	15%	20%	18%	-

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to Runway Excursions	Abbreviation	Attribute	Definition	Weight	Rate of occurrence winter period	Rate of occurrence summer period	Average rate	Rectified weight
503.4	Flight crew fatigue-long haul operation	CREW-FTG-LH	High	Accumulation of night flights. Limited crew. Inappropriate frequent mixing of west/eastbound flights, improper jetlag management. Insufficient lay-over / rest time. Many ultra-long flights (> 13H).	1,1	5%	10%	8%	-
503.4	**Flight crew**	**CREW-FTG-LH**	-	-	-	100%	100%		**1,01**
503.5	CRM (Crew Resources Management)	CREW-CRM	Good	Good CRM standards Shared decision-making Good adherence to SOPs and company procedures	1	75%	N/A	75%	-
503.5	CRM (Crew Resources Management)	CREW-CRM	Medium	Medium CRM standards Some deviations from SOPs and company procedures Some non-standard callouts	1,1	15%	N/A	15%	-

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Influencing Factors applicable to Runway Excursions	Abbreviation	Attribute	Definition	Weight	Rate of occurrence winter period	Rate of occurrence summer period	Average rate	Rectified weight
503.5	CRM (Crew Resources Management)	CREW-CRM	Poor	Poor CRM standards Poor communication between crewmembers, poor sharing of information or decision-making Excessive or insufficient authority gradient Absence of standard callouts	1,2	10%	N/A	10%	-
503.5	**CRM (Crew**	**CREW-CRM**	-	-	-	100%	-		**1,035**
503.6	Crew response	CREW-RESP	Good	Good crew reaction to aircraft	1	60%	N/A	60%	-
503.6	Crew response	CREW-RESP	Medium	Medium crew reaction to aircraft	1,1	20%	N/A	20%	-
503.6	Crew response	CREW-RESP	Poor	Poor crew reaction to aircraft	1,2	20%	N/A	20%	-
503.6	**Crew response**	**CREW-RESP**	-	-	-	100%	-	100%	**1,06**

The following shows the structure of the previous table.

- First column indicates the reference of each cluster of IF's and the reference of each individual IF. As an example IF_500 is the cluster of IF's related to Runway characteristics. This cluster is made of seven individual IF: IF_500.1 refers to 'Runway surface quality' while IF_500.7 refers to the 'Runway Visual path Guidance' Second column indicates the title of the cluster of IF's or the title of each individual IF
- Third column indicated the abbreviation or label used by the models like for example "RWY-VISAID" for "Runway Visual Path Guidance"
- Fourth column provides IF attributes. Each individual IF can take several values. For example IF_500.1 "Runway surface quality" can take two values: 'Good' or 'Poor' while IF_500.2 "Runway length" can take three values: 'Long', 'Medium' or 'Short'. These attributes values are defined in the fifth column "Definition". The definition of each attribute comes from official sources (EASA, ICAO…), Airbus internal sources (operational procedures, Airbus average landing performance effect) and Flight crew experience

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

The last three columns contain numerical values:

- Column 6 provides the weight of each value of an individual IF. Refer to chapter 2, paragraph 2.1.2 for detailed explanations on the weigh as well as to Appendix B of deliverable D4.4.
- Column 7 is the rate of occurrence expressed in % of each value of an individual IF. In the previous example of IF_500.1 "Runway surface quality", first value 'Good' has been assigned a rate of occurrence of 90% while the rate of occurrence of the second value 'Poor' is 10%. These rates have been set by default based on statistics or lessons learnt from in-service occurrences. They can be modified by the RO users. They can also add additional values like for example 'Medium'. In any case the sum of all the rates must be equal to 100%.
- Column 8 provides the calculated 'Rectified weight' of each individual IF. Refer to chapter 2, paragraph 2.1.2 for detailed explanations on the purpose of the rectified weights in the models and the way to calculate their values.

Mapping between the GCF's related to the risk of runway excursion and their linked IF's

FSS T4.2.5 RWY
Excursion Contributor

Table 23: Mapping between the GCF's related to risk of RE Exc. and their linked IF's

Figure A-1 shows the structure of Table 23.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Ref.	Generic contributing factors (2 level of items max.)	Comments	Estimated rate of occurrence (based on data from some Airbus operators on a set of flights over 12 months)	Influencing factor(s) to be considered Either N/A or ref of the main IF
4	Unstable approach (at 1000 ft or 500 feet)			
4.1	Excessive or unstable speed	Rate of occurrence from FDM	1% of flights	503 501.1 501.2 501.4

Figure A-1: Structure of the table describing the mapping between IF and GCF

- First column indicates the reference of each cluster of Generic Contributing Factors (level 1) and the reference of each GCF (level 2). Refer to Appendix A of D4.4 for a detailed description of the GCF's
- Second column indicates the title of the GCF's (level 1 and level 2)
- Third column provides comments like for example a rationale on the source of the estimated rate of occurrence
- Fourth column provides an estimated rate of occurrence that can for instance be based on some Airbus operators on a set of flights over a full year of operations
- Fifth and last column gives the list of all IF's linked to the individual GCF as for example: 503, 501.1, 501.2 and 501.4. In this specific example ref. IF503 is used to indicate that all individual IF's of cluster 503 'Crew Performance', i.e. 503.1 (Flight crew experience-CAPT), 503.2 (Flight crew experience-F/O), 503.3 (Flight crew fatigue-short-medium haul operation), 503.4 (Flight crew fatigue-long haul operation), 503.5 (CRM (Crew Resources Management) and 503.6 (Crew response to failures) are mapped to GCF 4.1.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Appendix A.3 Conversion Rules

Table 24: Conversion Rules on units for different stakeholders

Domain	Input data	Type	Initial unit	Target reference unit	Parameters	Conversion function	Reverse conversion function	Comment
Aircraft Manufacturer	Proba of occurrence	Likelihood	Flight	Flight Hour	Tf = average flight time in [hour]	P [per flight hour] = P[per flight] / Tf	P [per flight] = P[per flight hour] * Tf	[per Flight] unit is used by Aerodrome operators and ANSP at Aerodrome/Approach level
Aircraft Manufacturer	Proba of occurrence	Likelihood	Flight	Cycle	Tf = average flight time in [hour]	P [per cycle] = P[per flight hour] * Tf	P [per flight hour] = P[per cycle] / Tf	[per Flight] unit is used by Aerodrome operators and ANSP at Aerodrome/Approach level
ANSPs	Proba of occurrence	Likelihood	controlled flight hours per sector	Flight Hour	Nac = average number of aircrafts controlled by 1 ATS unit (~ one sector) Xt = average exposure time (average number of minutes flight length in sector)	P[per controlled flight hours per sector] = P[flight hour] * Nac * Xt / 60	P[flight hour] = P[per controlled flight hours per sector] * 60 / (Nac * Xt)	[per controlled flight hours per sector] unit is used by ANSPs for EnRoute/Approach control
ANSPs	ATCO Incident report							
Airlines	Pilot Incident report							
Airlines	FDM x							
Airlines	FDM y							

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Appendix A.4 Coverage of WP4.2 Recommendations by WP4.3 Activities

- **[REC1]** The notion of **influencing factors** would need to be further developed, completing the list of those factors as necessary and investigating the way they relate to the several models. This could be done at different levels: backbone model level or/and specific domain model level. The potential impact of those influencing factors in not only one type of risk but several of them at the same time should also be investigated.
    - **Coverage**: yes, the Influencing Factor concept was refined it can now be used in the quantification of safety indicators.

- **[REC2]** To **ensure completeness** with respect to the user requirements, the same process should be applied for the other risks to be addressed within the scope of the P4 in order to be implemented in the RO prototype the full set (i.e. MAC-TMA, RE-take off, CFIT, LOC-I, RI and FIRE).
    - **Coverage:** yes, a review of existing models in CATS and AIM for other risk categories was performed. It was assessed that the Backbone model approach is applicable for most of the risk categories.

- **[REC3] Common causes** between models have not been addressed in the work performed in WP4.2 and reported in this document. This should be further investigated when addressing 'interoperability' between the models to be used.
    - **Coverage**: partially, examples of common causes at the levels of generic contributors and domain specific contributors were provided and as well as how to deal with common causes. But a general review of the Backbone and Domain specific models should be performed in order to carefully identify potential common causes in the models that were developed.

- **[REC4]** A more **detailed evaluation of the use of a backbone model** (as per Streams 1 and 2) or a specific model (as per Stream 3 using a physical model instead) should be conducted in order to better assess the benefits and disadvantages in each case.
    - **Coverage**: partially, it is difficult to compare the backbone model approach with alternative approaches such as physical model because partners developing alternative approaches do not contribute to WP4.3

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

- **[REC5]** There should be a way to indicate the type of input data used in each model (including the backbone models) in order to provide an **indication of the 'reliability/uncertainty' of the obtained results** a risk level (i.e. certification specification, operational monitoring, expert judgement, etc.).
    - **Coverage**: yes, a way to perform sensibility analysis on the basis of a Backbone model was proposed.

- **[REC6]** MAC-ER and RWY-EXC have been independently considered and the results obtained from the several models addressing them have been presented separately for each case. Any **relationship between models** should be evaluated in order to better define the outcomes of the modelling functionality within the RO.
    - **Coverage**: Yes, a way to align the two BB models so that they are described using the same kind of format and that they are able to compute the same kind of indicators to align both was proposed.
- **[REC7]** The potential for a **common risk index** taking into account the several risks addressed in the RO should also be investigated.
    - **Coverage**: no, the definition of a global risk index could be covered by the task developing the dashboard of the RO

- **[REC8] Interface consistency** between models should be verified especially in terms of units.
    - **Coverage**: yes, see REC10

- **[REC9] Data** for the models should be updated and fed by operational data (occurrences, FDM, ATC data).
    - **Coverage**: yes, this recommendation is related with T4.3.2 & T4.3.3.
    - **Work performed**: to propose technical means to relate data (FDM, safety reports, etc) with generic and domain-specific contributors.

- **[REC10]** There is a need to **address / compute the risk of both ground and air segments**. There is a need to consistently manage probability of failure occurrences per time unit for the ground segment versus airborne segment (i.e. per operational hour or operational sector hour or flight hour).
    - **Coverage**: yes, conversion rules between the various units used in computations in the different domains are proposed.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Appendix B PROCESSES AND PRACTICES FOR FRAMEWORK UPDATE

The framework technical update follows the best practice defined for software version control. Version control, also known as revision control, or source control; is a component of software configuration management; is the task of tracking and controlling changes in the software, part of the larger cross-disciplinary field of configuration management.

The main version control goals are:

- **Configuration identification** - Identifying configurations, configuration items and baselines.
- **Configuration control** - Implementing a controlled change process. This is usually achieved by setting up a change control board whose primary function is to approve or reject all change requests that are sent against any baseline.
- **Teamwork** - Facilitate team interactions related to the process.
- **Defect tracking** - Making sure every defect has traceability back to the source.

All to be achieved through a version control system (VCS).

Within the RO version control process use is made of a distributed version control (also known as distributed revision control) which is a form of version control where the complete codebase - including its full history - is mirrored on every developer's computer.

This allows branching and merging to be managed automatically, increases speeds of most operations (except for pushing and pulling), improves the ability to work offline, and does not rely on a single location for backups.

The VCS used is GitLab [28]. Within GitLab the Risk Observatory prototype is created as a project and it is where the codebase is hosted.

Access and permissions to the project codebase are established through defined access profiles – Administrator; Technical lead; Integrator and Developer.

Within the RO project repository, there is one master branch which is “immaculate” – it has the last tested and approved version of the code. The master is always production-like and deployable.

The merge to the master branch is done only by the integrator; no other user interacts with it.

Considering the selected versioning workflow and that the work is done using a prototype, in addition to the master branch, there are only features branches.

As said, anything in the master branch is always deployable. Because of this, every new feature branch is created off of master when working on a feature or a fix.

Once the branch is created, developers start making changes. Whenever adding, editing, or deleting a file, a commit is made, and added to the branch. This process of adding commits keeps track of progress as work is done on a feature branch.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU’s Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.

Each commit has an associated commit message, which is a description explaining why a particular change was made. Furthermore, each commit is considered a separate unit of change. This allows rolling back changes if a bug is found, or if it is decided to head in a different direction.

Once there is some work done in the feature branch it is a best practice followed to create a merge request without assigning it to anyone. This indicates that the merge request is not ready to be merged yet, but feedback is welcome. Team members are then welcome to comment on the merge request in general or on specific lines with line comments. The merge request serves as a code review tool, and no separate code review tools are needed. If the review reveals shortcomings, anyone can commit and push a fix. Usually, the person to do this is the creator of the merge request. The diff in the merge request automatically updates when new commits are pushed to the branch.

When the feature branch is ready to be merged, the merge request is assigned to the named integrator.

Once a Merge Request has been opened, the person or team reviewing the changes may have questions or comments. After the changes have been verified and tested, it is time to merge the code into the master branch.

At this point of the project, there is no progress through release branches or environment branches as everything is kept in the development environment.

This document is the property of Future Sky Safety and shall not be distributed or reproduced without the formal approval of Coordinator NLR.
Future Sky Safety has received funding from the EU's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 640597.