



Guidance to Apply SESAR Safety Reference Material

Topic: SESAR SRM
Consortium coordinator: EUROCONTROL
Edition date: 14 December 2018
Edition: 00.03.01

Founding Members



Founding Members



Authoring & Approval

Authors of the document

Name/Beneficiary	Position/Title	Date
Bruno RABILLER/ EUROCONTROL	PJ 19-4 Safety member	14 December 2018
Nicolas FOTA/ EUROCONTROL	PJ 19-4 Safety member	14 December 2018
Laura CARBO/ EUROCONTROL	PJ 19-4 Safety member	14 December 2018

Reviewers internal to the project

Name/Beneficiary	Position/Title	Date
Marta LLOBET LOPEZ/ EUROCONTROL	PJ 19-4 Safety member	14 December 2018

Approved for submission to the SJU By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date
Jose Manuel CORDERO GARCIA / ENAIRE	PJ19 WP04 Lead	14 December 2018

Rejected By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date
------------------	----------------	------

Document History

Edition	Date	Status	Author	Justification
00.03.00	09/05/2016	Final	SESAR 1 Authors	Approved SESAR 1 version (Project 16.06.01 Deliverable D27) used in Wave 1 of SESAR 2020
00.03.01	14/12/2018	Final	See above	SRM update considering feedback from SESAR 2020 Wave 1 and new EASA regulation (EU N° 2017/373)

Table of Contents

Executive Summary	8
Guidance A <i>Introduction of Safety Assurance Activities</i>.....	10
A.1 Detailed safety assurance activities for the safety planning (<i>i.e.</i> ATM operational Solution Safety Plan – VALP Part II and Technological Solution Safety Plan – TVALP Appendix A)	10
A.2 Detailed safety assurance activities for the SESAR Solution at operational level.....	13
A.3 Detailed safety assurance activities for the SESAR Solution initial design level	20
A.4 Detailed safety assurance activities for the SESAR solution refined design level	28
Guidance B <i>On describing the Operational Environments</i>	36
B.1 Introduction.....	36
B.2 En-route and Terminal Area Operations.....	36
B.3 Airport Operations	37
Guidance C <i>On Safety scoping and change assessment</i>.....	38
C.1 Process	38
C.2 Tailored Safety Assurance Objectives and Activities per type of change	45
Guidance D <i>On defining Safety Criteria</i>.....	47
D.1 Overview	47
D.2 SAC defined at Solution level	47
D.3 Closing the loop between the Solution and Transversal Areas Project.....	51
D.4 Example for SESAR Concept “Airport Safety Nets”	54
Guidance E <i>On Pre-existing Hazards & Operational Services mitigating them</i>	55
E.1 Introduction.....	55
E.2 Suggested list of Pre-existing Hazards	55
E.3 On describing the Operational services & their contribution to mitigate the Pre-existing Hazards.....	56
Guidance F <i>On Setting Safety Objectives (success approach)</i>	59
F.1 Introduction.....	59
F.2 Process for Setting Safety Objectives (success approach).....	59
F.3 Example of Application.....	60
Guidance G <i>On setting Safety Objectives (failure approach)</i>.....	66
G.1 Introduction.....	66
G.2 Process for Setting Safety Objectives (failure approach)	67
G.3 Severity Classification Schemes	74

G.4	AIM-based Risk Classification Schemes	81
Guidance H	<i>On deriving Safety Requirements (success approach)</i>	87
H.1	Introduction.....	87
H.2	Process for deriving Safety Requirements (success approach).....	88
H.3	Example of Application.....	88
Guidance I	<i>On system-engineering models</i>	92
I.1	Accident Incident Model.....	92
I.2	EATMA Operational Activity Model (diagram NOV 5)	94
I.3	EATMA System Functionality and Flow model (NSV-4 diagram)	96
I.4	Logical Model.....	98
I.5	Thread Analysis model	100
Guidance J	<i>On the usage of Resilience Engineering</i>	104
J.1	Overview	104
J.2	Introduction.....	104
J.3	Core Principles	104
J.4	When to use Resilience Engineering in the SRM process	105
J.5	Description of the RE Activities	106
Guidance K	<i>On the usage of Dynamic Risk Modelling</i>	111
K.1	Forewords and introduction	111
K.2	Pre-requisite and selection criteria	112
K.3	Description of the method.....	113
K.3.1	Preparatory activities	113
K.3.2	Develop the dynamic risk model	114
K.3.3	Develop risk decomposition	115
K.3.4	Implement the dynamic risk model into software	116
K.3.5	Run Monte Carlo simulations.....	116
K.3.6	Assess bias and uncertainty	116
K.3.7	Develop safety risk results.....	116
K.4	Required skills and competence.....	117
K.5	Conclusions.....	118
K.6	Additional References	118
Guidance L	<i>On Safety and Human Performance (HP)</i>	119
L.1	Introduction.....	119
L.2	Safety and HP assessment	119
L.2.1	HP assessment overview	119

L.3	Causal analysis of Operational Hazards – Human Error	122
L.3.1	Hybrid Fault Tree method	123
Guidance M	<i>On gaining safety insights in real-time simulations</i>	129
M.1	Introduction	129
M.2	About the usage of real-time simulations in validation	129
M.3	Purpose of this Guidance	130
M.4	Process Steps and measurements	130
Guidance N	<i>Safety Management of VLD: an ANSP and Network Manager perspective</i>	133
N.1	Objectives	133
N.2	Introduction	133
N.3	VLD safety assurance	135
N.4	The VLD Safety Plan	135
N.5	Structuring the VLD Safety Case – generic guidance for ANSPs / NM	136
N.6	End-users & Regulatory Authorities: engagement & co-ordination	138
Guidance O	<i>Technological Solutions</i>	139
O.1	Why Technological Solutions need a dedicated Safety process	139
O.2	Overview of the process and link with SRM activities/outcomes	140
O.3	Description of the safety activities to be done per TRL and the corresponding expected outcomes	142
References	147	
Acronyms	148	
For Further Reading – Safety Assurance in SESAR	152	
1	Introduction	152
2	Generic Principles – fundamental aspects	153
3	Generic Safety Assurance Objectives (about the satisfaction of principles)	154

List of Tables

Table 1: Detailed safety assurance activities for safety planning	12
Table 2: Detailed safety assurance activities for the SESAR solution at operational level	19
Table 3: Detailed safety assurance activities for the SESAR's solution initial design	27
Table 4: Detailed safety assurance activities for the SESAR Solution's refined system design	35
Table 5: Maximum Operational Hazard Numbers per Severity Class	70

Table 6: Risk Classification Scheme for Mid Air Collision (TMA and En-Route).....	82
Table 7: Risk Classification Scheme for Runway Collision related to Incursions	83
Table 8: Risk Classification Scheme for CFIT	84
Table 9: Risk Classification Scheme for Taxiway Collision	85
Table 10. Risk Classification Scheme for Wake induced accident on Final Approach	86
Table 11: Frequency & level of criticality.....	125
Table 12: HP Assessment Evidence Quality considerations.....	128

List of Figures

Figure 1: Selection of safety assurance activities from a change assessment.....	46
Figure 2: Identification of pre-existing hazard and relevant AIM risk models.....	49
Figure 3: The base events affected in the AIM fault tree for each barrier	50
Figure 4: Interactions with Performance Framework - process overview.....	52
Figure 5. Representation of the Operational Services provided by the ATM/ANS functional system .57	
Figure 6. Illustration of several Operational Services mapped onto the AIM MAC in TMA simplified model	58
Figure 7. EATMA Process Model (NOV 5) used for analysing the change and the contribution to Operational Services	61
Figure 8: Severity Classifications for the MAC model (ER and TMA).....	75
Figure 9: Severity Classifications for the RWY Collision accident model	76
Figure 10: Severity Classification Scheme for the CFIT accident model	77
Figure 11: Severity Classifications for the Taxiway Collision accident model.....	78
Figure 12: Severity Classifications for the Wake Induced accident on Final Approach model.....	79
Figure 13: Severity Classifications for the Runway Excursion model	80
Figure 14. Illustration of Safety Requirements (success) derivation – extracted from Point Merge design	90
Figure 15: AIM, helicopter view.....	92
Figure 16: Main elements of the AIM barrier models illustrated with Mid-Air Collision	93
Figure 17: Elements of an EATMA Operational activity model (diagram NOV-5)	95
Figure 18: Operational activity model (NOV-5) for PJ07-03 Use Case “Mission Trajectory (MT) Management in Short Term Planning”	96

Figure 19: System Functionality and Flow diagram (NSV-4) created from an Operational activity model (NSV-4)	97
Figure 20: Typical Logical Model for the TMA ATC functional system instantiated to support PM operations design.....	99
Figure 21: Example of a Thread Diagram (complementing the Logical Model for the TMA ATC functional system instantiated to support Pont Merge operations design).....	101
Figure 22: The RE activities are organised into 5 main steps	106
Figure 23: Example of a propagation of criticality for an AND gate	124
Figure 24: Gates and phases of SESAR Solution development life cycle	134
Figure 25: Safety Assurance Structure	153

Executive Summary

The purpose of this document is to provide practical guidance to support the safety assessment activities as defined in the SESAR Safety Reference Material (SRM). This document should be used in conjunction with the SRM.

This version of the Guidance to apply the SRM (Ed 00.03.01) is based on the SESAR 1 Guidance to apply the SRM (Project 16.06.01 deliverable D27 Ed 00.03.00) developed within SESAR 1 and used during SESAR 1 and Wave 1 of SESAR 2020. It has been updated considering feedback and comments received during its application in particular with regards to V3 safety assessment. Furthermore some new guidance have been introduced (e.g. for setting Safety Objectives and deriving Safety Requirements from the success approach, for safety assessment of technological Solution) and some have been suppressed because not used within SESAR projects.

The detailed safety assurance activities are shown in **Table 1 to Table 4 in Guidance A.1 to A.4 for ATM Solutions and in Table 1 in Guidance A.1 and in Guidance O for Technological Solutions**. The Safety Assurance Activities are guide only and are intended to be neither prescriptive nor exhaustive. They would need to be revised for specific SESAR Solutions as per the Scoping and Change Assessment process detailed in **Guidance C**.

It should be noted that information necessary for many of the Safety Assurance Activities described in this section might already be available as part of the normal operational, project-management and /or systems-engineering processes. Where possible maximum use should be made of such information provided sufficient confidence is shown in its completeness and correctness, for safety purposes. Such information includes but is not limited to:

- *In the Solutions' OSED part of the SPR-INTEROP/OSED: (i) operational environment; (ii) existing (baseline) ATM/ANS / functional system; (iii) how the change under consideration changes the ATM/ANS / functional system; (iv) normal and abnormal conditions; and (v) Operational scenarios*
- *In the Solutions' SPR-INTEROP part of the SPR-INTEROP/OSED: required functionality & performance of the ATM/ANS / functional system*
- *In the Solutions TS's: system requirements*
- *From the System Engineering tools:*
 - *Enterprise Architecture Models i.e. a set of consistent "views" labelled "performance", "business", "service" etc. of a database comprising the docs/records detailing and organising the SESAR concept and its artefacts;*
 - *Requirements data describing operational and system requirements with traceability, also incl. performance and TA requirements;*
 - *Validation & Verification data containing the summary results of V&V objectives, evidence and status (though not the detailed results);*
 - *Etc.*

Such Safety Assurance Activities have their reference numbers annotated thus "*", in the assurance Tables Guidance A.1 to A.4 below.

Initial Guidance included in these Tables in **Guidance A.1 to A.4** is expanded in further Guidance as referenced from the appropriate parts of the Tables.

Finally, this document provides the logic applied to derive the safety assurance activities which produce the required evidence in the "**For Further Reading**" section.

Safety practitioners could contact the SESAR 2020 Transversal Area project when conducting safety assessments in accordance with this document. The Safety Community of Practice (CoP) could be used for any clarification relative to applying this guidance [4].

Safety Plan and Safety Assessment Report Templates are available on the SESAR Programme Library [5].

Guidance A Introduction of Safety Assurance Activities

Forewords:

1. All Safety Assurance Activities presented in Table 1 to Table 4 of this guidance are relevant for ATM operational Solutions. Concerning Technological Solutions, only safety assurance activities presented in Table 1 in this guidance are to be considered. The complete list of safety activities relevant to Technological Solutions is provided in Guidance O.

2. Table 1 to Table 4 include cross-references to the set of Principles (P_x) and Safety Assurance Objectives (AO_y) defined in section **For Further Reading**. This is for completeness and traceability. **For Further Reading** section provides background information and rationale on the list of Principles, Safety Assurance Objectives and Safety Assurance Activities.

Solution Project should concentrate on safety assurance activities (a_z) that are grouped under the different stages of the safety assessment process (Safety planning, Safety assessment at operational level and safety assessment at design level).

3. Safety Assurance Activities involving information that might already be available as **part of the normal operational, project-management and /or systems-engineering processes** have their reference numbers **annotated “ * ”**, in the assurance Tables **Guidance A.1 to A.4** below.

A.1 Detailed safety assurance activities for the safety planning (*i.e.* ATM operational Solution Safety Plan – VALP Part II and Technological Solution Safety Plan – TVALP Appendix A)

Ref			Safety Assurance Activities	Guidance and Proposed Tools & Techniques
Safety Scoping & Change Assessment				
P1	AO1	a1*	Describe what the Solution is seeking to achieve (e.g. understand the operational concept, the technological concept, benefits delivered in capacity, efficiency, costs and/or safety, Implementation strategy)	See Items #1 to #5 in Guidance C on “scoping the safety assessment and change assessment”. This shall be done in coordination with other Transversal Activities. For Technological Solutions this corresponds to safety activity 2.1 in Guidance O.3.1 .
P1	AO2 & AO3	a1	Perform an initial assessment of the safety implications of the Solution: - Baseline for the change assessment - Operational Environment for the change (incl. Identify other parts of the ATM/ANS operations that will be affected) - Details of the change - Depth and breadth of the change	Item #6, #7, #8, #9 and #10 in Guidance C Step 1 of the Resilience Engineering method described in Guidance J supports the development of an initial understanding of the work-as-done in the current operations and of the way that future ATM operations are expected to be done.

Ref			Safety Assurance Activities	Guidance and Proposed Tools & Techniques
			- Need for new or modified Regulations Specifically for Technological solutions: - The operational applications, (i.e. the related ATM operational Solutions)	For Technological Solutions this corresponds to safety activities 2.2 and 2.3 in Guidance O.3.1.
Determination of Safety Criteria				
P2		a1	Define the safety strategy in addressing the change through: For ATM Solutions: - Identification of the pre-existing hazards and risks that fall within the scope of the safety assessment (i.e. the aviation pre-existing hazards and risks that ATM/ANS is intended to mitigate) - Definition and justification of appropriate Safety Criteria (SAC), according to the scope of the safety assessment (i.e. what is “safe” in the context of the Solution and, in broad terms, the strategy for demonstrating safety) and incl. the usage of field data	For ATM Solutions: - Pre-existing hazards - Item #11 in Guidance C. By definition, these aviation hazards exist in the operational environment before any form of ATM de-confliction has taken place. It is therefore the primary purpose of the relevant Solution operational services to mitigate (some of) them. See Guidance E.2. - Safety Criteria - Item # 12 in Guidance C. Eventually, the SAC will be used to set measurable and quantifiable safety performance objectives. See Guidance D SACs are to be documented in the Safety Plan (as per assurance activity P2-a2) but also as requested in the Performance Assessment Report (as per the OSED Part V – PAR template) <u>Note:</u> In case the subsequent analysis carried out in the other lifecycle phases (as described in Guidance A.2, A.3 and A.4 below) shows that a SAC needs to be modified or a new SAC is identified, that would require an iteration for updating the list of SAC with the subsequent cascading effect in terms of safety objectives and safety requirements.

Ref			Safety Assurance Activities	Guidance and Proposed Tools & Techniques
			For Technological Solutions: • Definition of the Technical System Safety Specification • Identification of applicable safety-relevant regulation.	<u>Note</u>: the Validation Objectives related to safety set at the level of the Solution (not for a specific validation exercise, but for the whole concept addressed in the Solution) need to be defined in line with those SACs. Those safety validation objectives are to be capture in the core of the VALPlan. For Technological Solutions this corresponds to safety activity 2.3 in Guidance O.3.1. More information on the Technological System Safety Specification is provided in Guidance O.2. Safety relevant regulatory requirements are also to be identified (see Item # 12 in Guidance C).
Safety planning				
P2		a2	Definition of the safety assurance activities, safety deliverables, accountability and responsibility	The results of activities within this Guidance A.1 will allow to issue a Safety Plan aimed at specifying the safety assurance activities to be carried out, whilst recording the relevant safety assessment information available at this initial stage (to be further used as input to the Safety Assessment Report). See also items #13, 14 & 15 in Guidance C. For ATM Solutions: Results from activities in Guidance A.1 are to be documented in accordance with the VALP Part II – Safety Plan template. For Technological Solutions: Results from activities in Guidance A.1 and Guidance O.3.1 are to be documented in the TVALP Appendix A –Safety Plan (even if no template is currently available). This corresponds to safety activity 2.4 in Guidance O.3.1.

Table 1: Detailed safety assurance activities for safety planning

A.2 Detailed safety assurance activities for the SESAR Solution at operational level

Ref			Operational Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
Operational level specification under normal operations				
P3P4	AO1	a1*	Identify and describe the Solution operational services aiming at mitigating the risks associated to the pre-existing hazards defined in P2_a1 .	Operational Services are provided by the ATM/ANS Functional System to the User i.e. an aircraft or a group of aircraft. The analysis should start with the identification of all the operational services relevant for the Solution scope, i.e. which contribute to the mitigation of the pre-existing hazards defined in P2_a1. Not all these services are necessarily impacted by the change brought by the Solution and this will be the scope of the next activity (P3P4 AO1 a2*) to identify the impacted ones (safety objectives functionality and performance – related to the ‘success’ approach under normal conditions). The delivery of the operational services and sub-services (if relevant) can be mapped onto the Accident Incident Model (AIM) barriers (ATM layers) – see Guidance E.3.
P3P4	AO1	a2*	Define the safety objectives (functionality and performance – related to the ‘success’ approach) specifying the above operational services under normal conditions. Safety objectives are defined in order to mitigate the pre-existing risks under normal operations, i.e. those conditions that are expected to occur on a day-to-day basis.	The definition of the safety objectives (success approach) under normal conditions can be achieved following the Guidance F. The full range of possible operational scenarios / use cases as defined in the OSED for the normal conditions need to be consider It is required to check the completeness of the OSED list of operational scenarios / use cases by describing the relevant phases of a typical normal flight as a continuous process and addressing in particular the transition modes (if relevant, e.g. inputs/outputs, separation responsibilities, etc.). In case new operational scenarios / use cases are identified, or corrections to the existing ones are necessary, the Project should be informed in order to update the OSED (and the corresponding EATMA operational layer models) and additional safety objectives should be defined. In particular attention should be paid to additional operational scenarios /

Ref			Operational Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
				use cases related to variations in key Operational Environment (OE) conditions as identified with the ‘Scoping and Change assessment’ process (Guidance C). Step 2 of the RE Method described in Guidance J supports the identification of the varying conditions, inherent in complex systems such as ATM, which the new design will need to handle. To assess the impacts of the Solution operations on adjacent airspace or on neighbouring ATM Systems, check the changes in the Operational Environment to host the Solution operations and derive any required additional safety objectives (functionality and performance) for compatibility (e.g. Service Level Agreement (SLA)). <u>Note:</u> In case the subsequent analysis carried on at high-level design (as described in Guidance A.3 below) identifies additional normal operational scenarios/use cases or another need for new or modified Safety Objectives (functionality and performance), that would require an iteration for updating the list of Safety Objectives.
Operational level specification considering abnormal conditions				
P3P4	AO1	a3*	Identify external abnormal conditions, e.g. aircraft emergency, RWY closure / change, sudden change in WX conditions, severe WX, sudden activation of restricted airspace, low-performance aircraft, aircraft encounters TCAS RA, etc.	Abnormal conditions are those under which the system has to operate in a reversionary mode due to, for example: 1) Conditions of the operation environment that the system may exceptionally encounter 2) Equipment failures external to the ATM system concerned, 3) Maintenance interventions – out of scope for SESAR Development Phase Abnormal conditions are normally identified in the OSED but it is the role of this activity to ensure the completeness of those conditions as far as possible. In particular attention should be paid to additional operational scenarios / use cases

Ref			Operational Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
				related to variations in key OE conditions as identified with the ‘Scoping and Change assessment’ process (Guidance C). Guidance J provides additional techniques for identifying the varying conditions which may be expected in the operational environment.
P3P4	AO1	a4*	For each abnormal condition identify existing/define new Safety Objectives (functionality and performance) specifying the above operational services.	This is done by assessing the immediate operational safety effect, considering the mitigations provided through the Safety Objectives (functionality & performance) derived for normal conditions (as per P3P4_AO1_a2 above). If necessary, new Safety Objectives (dedicated to abnormal conditions) need to be derived. If, during this activity, detailed mitigating solutions (i.e. anticipating the high-level design) are identified, they need to be captured as candidate Safety Requirements to be further confirmed at high-level design. Under an abnormal condition of the OE, the System may be allowed to enter a degraded state provided that it can easily be recovered when the abnormal condition passes. The specified SOs shall be sufficient for mitigating the safety risk associated to the abnormal condition occurrence and the subsequent recovery. Step 3 of the RE method in Guidance J supports the description of the strategies which operators may use to deal with the varying conditions in the current and future ATM operation. <u>Note:</u> In case the subsequent analysis carried on at high-level design (as described in Guidance A.3 below) identifies additional abnormal conditions or another need for new or modified Safety Objectives (functionality and performance), that would require an iteration for updating the list of Safety Objectives.

Ref			Operational Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
Operational level specification in faulted conditions				
P3P4	AO2	a1	Identify Operational Hazards caused by failures internal to (i.e. generated by) the system	This is the application of the SAM FHA carried out at the operational level. Alternatively, the Operational Hazard Assessment (OHA) process from ED-78A may be adapted for the purpose. The Operational hazards are defined at the level of the Operational services i.e. a level that is independent of the system design and is related to the failure of an operational service. Note that we refer here to “system-generated” hazards, which result from failure of the ATM/ANS functional system affected by the Change brought in by the Solution. An initial way for identifying these operational hazards is based on the analysis of the corresponding operational services (refer to previous assurance activity P3P4.AO1.a1) and by considering, for each safety objective from the success approach (refer to previous assurance activity P3P4.AO1.a2 and a4), what would happen if the objectives were not satisfied (i.e. negate the safety objectives derived with the success approach). The standard questions related to the SWITF/HAZOP/HAZID/etc. processes at an FHA/OHA workshop should be enriched considering the following: 1) The Resilience Engineering method described in Guidance J (in particular Step 2 on varying conditions) 2) Questions from the HP Issue Analysis (see HP RM, Appendix E)
P3P4	AO2	a2	Assess the severity of the effects from each Operational Hazard, using the AIM-based Severity Classification Schemes. Since the severity classification approach considers the most probable effects from hazard occurrence, the efficiency of the forthcoming barriers must be captured as consequential (protective) mitigations (which accounts for the external mitigation means)	Guidance is provided in Guidance G.3 .

Ref			Operational Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
P3P4	AO2	a3	Set Safety Objectives (failure approach) (expressed as the tolerable probability of occurrence of each Operational Hazard) driven by the AIM-based Risk Classification Schemes	Guidance is provided in Guidance G.2 and G.4 . If during the activities P3P4 AO2 a1 to a3 , detailed mitigating solutions (i.e. anticipating the high-level design) are identified, they need to be captured as candidate Safety Requirements to be further confirmed at high-level design (see Guidance A.3)
Completeness and correctness of operational level specification				
P3P4	AO C&C ¹	a1	Verify that the Safety Objectives (both functionality & performance properties from the success approach as well as efficiency of mitigation measures for the failure approach) are complete and correct by reference to the Safety Criteria by: - Ensuring forward and backward traceability between SO to SAC - Definition of observable and measurable safety validation objectives in the VAL Plan - Collection from the validation exercise (VAL Report) the required evidence with respect to the safety validation objectives and amend (or otherwise) the set of safety objectives.	Traceability is ensured by mapping the Safety Objectives (functionality and performance) for normal and abnormal conditions to the Safety Criteria. <u>Note</u>: there is here no need to ensure the traceability of the SO (integrity / reliability) to the SAC since this is implicitly achieved by using the AIM-based RCS schemes. Safety-related Validation Objectives for the several validation exercises and activities are to be defined based on the Safety Objectives (functionality & performance derived for normal and abnormal conditions as well as mitigations measures for the failure approach), together with the information captured within the operational level. The subsequent analysis carried out at high-level design (as described in Guidance A.3 below) will allow to further refine and complement this set of safety-related Validation Objectives. The type of data to be collected during the validation activities and the means for doing that also needs to be defined and described in the Validation Plan.

¹ This Assurance Objective is called “C&C” (Completeness&Correctness) and is associated to the outcome of the previous Assurance Objectives (AO1 and AO2).

Ref			Operational Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
				The collected data from the validation exercises is then to be analysed and summarised. It represents the evidence showing the satisfaction (or not) of the corresponding safety-related Validation Objectives. The existing list of safety objectives is then to be completed/updated as necessary. All those results and conclusions are to be documented in the Validation Report, but also in the Safety Assessment Report. A summary of those results is also to be documented in the Performance Assessment Report as per the corresponding template (OSD Part V – PAR). For detailed guidance on gaining safety insights from real-time human-in-the-loop simulation (RTS) see Guidance M. Coordination with HP is here required in: - ensuring a consistent set of validation objectives and associated success criteria (as per the VAL Plan Template); as well as - analysing the evidence being collected against the validation objectives. For guidance on gaining safety insights from validation exercises, consider Guidance M.
P3P4	AO3	a1	Present directly, and/or by reference, all the assumptions on which the safety objectives depend.	Assumptions usually relate to matters outside of the direct control of the organisation responsible for the Safety Assessment but which are essential to the completeness and/or correctness of the safety assessment results. They may also be matters that have to be assumed in one stage of the lifecycle (e.g. at operational level) until they are verified in a later stage (e.g. high-level design). Assumptions as they arise during the safety assessment will be captured as follows: - Description - Source (where and when raised) - Rationale / reason for the Assumption - How and when the Assumption was (or will be) validated

Ref			Operational Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
Safety Process Verification				
P3P4	AO4	a1	Ensure that the safety assessment results at operational level correspond to the applicable Solution OSED version	Satisfaction of this objective requires maintaining consistency between safety assessment results at operational level and the evolution of successive Solution/OSED versions.
P3P4	AO5	a1	Ensure that the safety assessment results at operational level are trustworthy	Backing evidence is obtained from the properties of the processes by which Direct Evidence (products) was obtained, and shows that those processes, tools and techniques, human resources etc. were appropriate, adequate and properly deployed. Evidence must be shown to be trustworthy, by demonstrating, amongst other things: - the suitability of the processes, tools and techniques etc. that are used to generate the evidence obtained from the safety assessment - the correct application of those processes, tools and techniques - the competence of the personnel applying those processes, tools and techniques.

Table 2: Detailed safety assurance activities for the SESAR solution at operational level

A.3 Detailed safety assurance activities for the SESAR Solution initial design level

			Initial design Safety Assurance Activities	Guidance and Proposed Tools and Techniques
Initial Design representation				
P5P6	AO1	a1*	Produce an initial design model (high-level) to interpret the operational-level specification or use an existing design engineering model in case there is an obvious architectural design available.	Guidance on engineering design models is given in Guidance I. Such models could be EATMA model, SPR-level model or logical model. A Hierarchical Task Analysis (HTA), to be developed by HP experts (see HP Reference Material, chapter 3.4.6.4), should support the process of developing and explaining the initial design representation. The HTA should be enriched by applying the resilience engineering principle ‘work –as- done’ (see Guidance J, Step 1). Describe the components of the initial design. Main human tasks, information exchange and interfaces with machine-based functions will be generated by the HTA.
Initial Design analysis under normal operations				
P5P6	AO1 & AO2	a2*	Specify initial safety requirements (functionality and performance properties from the success approach) for each element of high-level design, including external elements as necessary under normal operations	In case, there are not yet high-level formalized requirements available, the first step is to derive in a static way an initial list of safety requirements by mapping each Safety Objective (Functionality and Performance) to the initial design elements (technical, human and procedural). See Guidance H for the derivation of Safety requirements from the success approach. For each scenario/used case (incl. those related to varying conditions, see Guidance J Step 2), describe how the elements of the initial design (equipment functions, human tasks and data) combine to deliver the aspects of the air navigation services associated with the scenario Thread analysis (see I.5 of Guidance I) is one of the recommended static techniques for this assurance activity. This analysis should consider Resilience Engineering (see Guidance J) which can support the description of work-as-done in the current

			Initial design Safety Assurance Activities	Guidance and Proposed Tools and Techniques
				operation and use this to inform the way that future ATM operations are expected to be done. Deliberate under-specification might sometimes be necessary in order to optimise the behaviour of the system – for example, allowing a human element of the system some discretion in when / how to execute a task according to his/her professional judgement and experience. On the other hand, unintentional under-specification can be a source of unwanted variability and coupling in the system that could be a source of system-generated risk. Where necessary (e.g. for the relevant sub-set of scenarios / use cases) check that the performance properties are complete, correct and mutually consistent by bringing into play dynamic risk modelling. Specific guidance on Dynamic Risk Modelling is given in Guidance K including a set of criteria to be used to decide on whether DRM is required to generate the evidence. Update/complement the existing list of safety requirements as necessary. Where the external entities are pre-existing and fixed, and/or beyond managerial control / sphere of influence, then their safety properties may be assumed provided such Assumptions are shown to be valid. <u>Note:</u> In case the subsequent analysis carried on during the refined design phase (as described in Guidance A.4 below) identifies need for new or modified Safety Requirements (functionality and performance), that would require an iteration for updating the list of Safety Requirements.
Initial Design analysis considering abnormal conditions				

			Initial design Safety Assurance Activities	Guidance and Proposed Tools and Techniques
P5P6	AO3	a1*	Specify operational scenarios that are sufficient to fully describe the abnormal operational environment in which the ATM/ANS functional system will be required to operate	Each scenario should identify all the abnormal operational conditions / range of inputs that system might encounter exceptionally and under which the system may be allowed to enter a degraded state provided that it can easily be recovered when the abnormal condition passes and the risk during the period of the degraded state is shown to be tolerable within the context of satisfying the Safety Criteria – cf normal conditions under P5P6_AO1 & AO2_a2* above. Check the scenarios against the OSED, if one is available.
P5P6	AO3	a2	For each scenario, assess the degree and extent to which the elements of the initial design (equipment functions, human tasks and data) can continue to deliver the aspects of the air navigation service associated with the scenario	Thread analysis (see I.5 of Guidance I) is the recommended technique for this Activity. Update the initial safety requirements (functionality and performance properties from the success approach) as necessary.
P5P6	AO4	a1	Where it is shown that the ATM/ANS functional system could not continue to operate as required, assess the risk associated with degradation in the system performance	This is a form of system-generated risk, albeit that the initiating cause is (by definition) external to the system in question. The risk assessment must take account of the likelihood that the abnormal events would occur in the first place.
P5P6	AO4	a2	Where the system could not continue to operate as required, describe the conditions and mechanisms for recovering the system to its full functionality and performance	Thread analysis (see I.5 of Guidance I) and Resilience Engineering (see Guidance J) are the recommended techniques for this Activity Update the initial safety requirements (functionality and performance properties from the success approach) as necessary
Initial Design analysis in faulted conditions				
P5P6	AO5	a1	Identify all potential causes of each operational hazard derived under Assurance objectives P3P4_AO2_ above (deductive analysis)	This is the application of the SAM PSSA. This is a top-down (i.e. deductive), apportionment process and needs to be supplemented by Assurance activity P5P6_AO5_a5 below.

			Initial design Safety Assurance Activities	Guidance and Proposed Tools and Techniques
P5P6	AO5	a2	Specify initial Safety Requirements (Integrity property from the failure approach) and / or Assumptions for the causes of each operational hazard, such that the Safety Objectives (and/or SAfety Criteria) are satisfied, taking account of any internal mitigation means.	This is the application of the SAM PSSA. Safety Requirements are always preferred to Assumptions. However, where the mitigations relate to items that we don't need to change (because they already exist) or cannot change (because they lie outside our managerial control / sphere of influence) then capturing their safety properties as Assumptions would normally be acceptable provided evidence is presented to show that each Assumption is valid. <u>Note:</u> In case the subsequent analysis carried on during the refined SESAR design phase (as described in Guidance A.4 below) identifies need for new or modified Safety Requirements (integrity) that would require iteration for updating the list of Safety Requirements.
P5P6	AO5	a3	Capture all internal mitigations as either functional, performance or safety requirements (integrity property from the failure approach) or Assumptions, as appropriate	This is the application of the SAM PSSA.
P5P6	AO5	a4	Check that the system can actually operate safely under, and recover from, all degraded modes of operation implicit in P5P6_AO5_a1 .	Guidance J provides a method to examine variations in ATM System performance which may coincide and combine to generate unexpected conditions which the System can be expected to deal with. Step 3 of the RE method outlines an approach to identifying the strategies used by operators to adapt to these varying conditions. This takes account of the fact that in many industries (including ATM) a disproportionate number of accidents seem to occur when the system concerned was in a degraded mode of operation immediately before the accident.

			Initial design Safety Assurance Activities	Guidance and Proposed Tools and Techniques
				Validation exercise based on a real-time human-in-the-loop simulation (RTS) are an efficient means to validate safety in degraded modes of operation and associated recovery (see Guidance M)
P5P6	AO5	a5	Show that all other possible failure modes associated with the initial design have been identified and mitigated such that Safety Objectives, derived under Assurance Objective P3P4_AO2 above are still met	This is a bottom-up (i.e. inductive) analysis process additional to Assurance activities P5P6_AO5_a1 above. It is looking for emergent properties of the design that may not be revealed by top-down (deductive) techniques such as Fault Tree Analysis Some of the failure modes can be generated by seeding failed or incorrect functions / transactions in the scenarios / threads of Assurance activity P5P6_AO1_a2*. Otherwise a Failure Modes Effects & Criticality Analysis (FMECA) – for more information see SAM Guidance, Part IV, Annex D
Initial design non-safety elements, emergent properties and impact on safety nets				
P5P6	AO6	a1	Show that non-safety functions of the initial design (if any) do not impact the safety performance of the functional system	Perform a design analysis to show that non-safety elements cannot adversely affect safety related elements. Any element of the initial design which is not required for the safety of the operational system but required for other purposes (e.g. recording element for maintenance) must be identified and assessed from a safety point of view. It must be shown that this element and associated data flows in normal/abnormal conditions cannot impact the safety performance of the functional system. It must be shown also that in case of failure the safety performance of the remaining functional system is not impacted and performance not degraded. Update the safety requirements as necessary.
P5P6	AO7	a1	For the initial design, show also that there are no emergent properties of the design that could allow non-safety functions to interfere with safety functions and data sources / flows	This can be done with: a static perceptive using, for example, thread analysis – see Guidance I.5, the RE method – see Guidance J, and/or

			Initial design Safety Assurance Activities	Guidance and Proposed Tools and Techniques
				a dynamic perceptive using, for example, real-time and fast-time simulations (see Guidance M)
P5P6	AO8	a1	Check that the system design operates in a way that does not have a negative effect on the operation of related ground-based and airborne safety nets	It requires confirmation that no modes of operation of the ATM/ANS functional system that could reduce the effectiveness of safety nets could be triggered by normal operation or by external abnormal events.
Completeness and correctness of initial safety requirements				
P5P6	AO C&C ²	a1	Verify that the initial Safety Requirements (both functionality & performance properties from the success approach as well as efficiency of mitigation measures for the failure approach) are complete and correct by reference to the Safety Objectives by: - Ensuring backward traceability between SR to SO - For each scenario, identify those aspects / properties of the high-level design that it has not been possible to model in the above (static) analyses - From those, define observable and measurable safety validation objectives in the VAL Plan	Traceability is done by mapping the Safety Requirements (functionality and performance) for normal and abnormal conditions to the corresponding Safety Objectives. Fast-time and Real-time Simulations (FTS and RTS) are usually the validation activities to be used at that stage. Where significant HF issues are involved, specific HF Lab techniques can be used to supplement the data from simulations (see Guidance M). Human factors (see Guidance L) and timing properties issues are examples of issues that may require dynamic modelling (see Guidance K). Safety-related Validation Objectives for those validation exercises and activities are to be redefined based on the Safety Requirements (functionality & performance derived for normal and abnormal conditions as well as mitigations measures for the failure approach), together with the information captured within the operational level and the high-level design.

² This Assurance Objective is called “C&C” (Completeness&Correctness) and is associated to the outcome of the previous Assurance Objectives (from AO1 to AO8).

			Initial design Safety Assurance Activities	Guidance and Proposed Tools and Techniques
			- Checking that the system design operates correctly in a dynamic sense, under all conditions (although only a subset of conditions can be modelled in RTS) - Collection from the validation exercise (VAL Report) of the required evidence with respect to the safety validation objectives and amend (or otherwise) the set of safety requirements.	The type of data to be collected during the validation activities and the means for doing that also needs to be defined and described in the Validation Plan. The collected data from the validation exercises is then to be analysed and summarised, they are the evidence showing the satisfaction (or not) of the corresponding safety-related Validation Objectives. The existing list of safety requirements is then to be completed/updated as necessary. All those results and conclusions are to be documented in the Validation Report, but also in the Safety Assessment Report. A summary of those results is also to be documented in the Performance Assessment Report as per the corresponding template (SPR-INTEROP/OSD Part V – PAR). Coordination with HP is here required in: - ensuring a consistent set of validation objectives and associated success criteria (as per the VAL Plan Template); as well as - analysing the evidence being collected against the validation objectives.
P5P6	AO C&C ³	a2	Show that all Assumptions that have been made in the previous lifecycle phases, on which the high-level Safety Requirements depend, are necessary and valid	Two matters are crucial to the safety assessment: firstly, as the Assumptions have an impact on the way the Safety Objectives were set, then the latter are valid only if the former are met; and secondly, therefore, these Assumptions must be properly recorded, demonstrated as being valid / satisfied prior to operations, and then continuously monitored and confirmed in operational service, along with the Safety Requirements. See SAM Part IV Annex I – Safety Case Development Manual [15].

³ This Assurance Objective is called “C&C” (Completeness&Correctness) and is associated to the outcome of the previous Assurance Objectives (from AO1 to AO8).

			Initial design Safety Assurance Activities	Guidance and Proposed Tools and Techniques
Safety Process Verification				
P5P6	AO9	a1	Show that all assurance in Guidance A.3 applies to a known system configuration and which is consistent with the system configuration of Assurance activities belonging to P3P4_AO4 .	Satisfaction of this objective requires careful configuration control of the various representations of the system throughout the lifecycle. See also SAM, PSSA Introduction, section 6
P5P6	AO10	a1	Show that the evidence for the initial safety requirements is trustworthy	Backing evidence is obtained from the properties of the processes by which Direct Evidence (products) was obtained, and shows that those processes, tools and techniques, human resources etc. were appropriate, adequate and properly deployed. Evidence must be shown to be trustworthy, by demonstrating, amongst other things: • the suitability of the processes, tools and techniques etc. that are used to generate the evidence obtained from the safety assessment • the correct application of those processes, tools and techniques • the competence of the personnel applying those processes, tools and techniques.

Table 3: Detailed safety assurance activities for the SESAR's solution initial design

A.4 Detailed safety assurance activities for the SESAR solution refined design level

Ref			Refined system design Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
Refined design representation and analysis under normal operations				
P7	AO1 & AO2	a1	Refine the Safety Requirements (Functionality and Performance properties from the success approach) for the refined system design of the solution	* Ensure the existence of an adequately refined system design representation of the SESAR solution. The refined system design representation is the one where the achievement of full V3 (TRL6) maturity has to be verified which authorises then the transition to Industrialisation and Deployment. The refined design representation is a refinement of the initial design. It describes and details specifications covering functional, non-functional and interface requirements addressing the “what” and not the “how”. The aim is not for the technical elements to specify the physical design of the functional block which remains with industry, but the functional description and necessary logical interfaces with other functional blocks. <u>Note</u>: this should be derived from engineering activities; it is not a process specifically undertaken by safety specialists. * Refined Safety Requirements are derived considering the refined design and requirements derived at initial design (P5P6_AO1& AO2) *Provide traceability between initial design elements and final system design elements/subsystems * Establish bi-directional traceability between the initial design Safety Requirements (success approach) and the refined system design safety requirements (new, modified or existing)
P7	AO1 & AO2	a2	Show that the proposed HMI requirements are fit for purpose in supporting controller and other ATC staff tasks	* Carry out HF expert review of HMI supported by expanded task analysis based on operational procedures

Ref			Refined system design Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
				* Perform evaluation of prototype and HMI displays (can be combined with staff training and procedure-validation simulations) This is a further step in the Human Factors analysis discussed in Guidance L, and can either use existing task analysis information or extend this information as required, following the HP Reference Material (HPRM) [8]. The RE method in Guidance J can support the review of HMI requirements through an analysis of current work-as-done, adaptive capacity changes and the capture of design recommendations to strengthen the resilience of the design.
P7	AO1 & AO2	a3	Refine or define new ATC /flight crew procedures requirements	* Requirements for procedures to be developed by analysis of the refined system design (for example, any operational procedures needed in connection with the proposed system HMI). * Review of all new and modified procedural requirements and HMI design by expert controller group. * Provide traceability of procedural requirement to initial design SRs and any further SRs derived from refined system design features * Any deliberate under-specification of Human actions that is done for safety reasons should be associated to a substantial net safety benefit * Any deliberate under-specification of Human actions that is done for non-safety reasons cannot have adverse effect on safety <u>Note:</u> Under-specification is a principle of Resilience Engineering. Guidance J may support the identification of scenarios where under-specification occurs and can

Ref			Refined system design Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
				assist in identifying the strategies adopted by operators to a range of varying conditions which can inform the design.
P7	AO1 & AO2	a4	Define Controller Competence Requirements	In close coordination with HP and by using the HP Reference Material: • Derive requirements for Controller training, as necessary • Derive requirements for Controller licensing, as necessary • Derive requirements for Controller selection & management, as necessary • Show that all three sets of requirements together are sufficient to satisfy the relevant safety requirements (functionality and performance properties from the success approach) placed on human elements in the initial design. See also SAM, SSA Introduction, section 3.1.2A [15].
P7	AO1 & AO2	a5	Show that all new, expanded or refined ATC/flight crew procedures requirements are necessary for the operation of the Technical System under all normal operating conditions	Knowledge of the final system design, that was not available at the time that the initial design was defined and analysed, can often lead to additions to, or refinement of, the Human tasks that in turn may lead to new, expanded or refined requirements for ATC Procedures Normal conditions are those under which the system is operating as designed, with full functionality and performance
Refined Design analysis considering abnormal conditions				
P7	AO3	a1	Refine the Safety Requirements (Functionality and Performance properties from the success approach) for the refined system design of the SESAR solution considering abnormal conditions	Refined Safety Requirements are derived considering the refined design and requirements derived at initial design level (P5P6_AO3)
P7	AO4	a1	Show new, expanded and refined ATC/flight crew procedures requirements are sufficient to ensure the safest operation of the Technical System under all	Abnormal conditions are those under which the system has to operate in a reversionary mode due to, for example: 1) Abnormal conditions external to the ATM system concerned

Ref			Refined system design Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
			abnormal operating conditions, <u>and</u> recovery from those conditions	2) External Equipment failures, 3) Maintenance interventions – out of scope for SESAR Development Phase For instance this can be achieved with the following: - Analyse abnormal external conditions and develop procedure requirements (use information from initial design analyses of abnormal external conditions) - Use results of FMEA and existing knowledge to identify failures internal to the technical system. - Identify appropriate operational response to system failures and define requirements (normally there will be some level or levels of fallback system) - Identify necessary actions when system has been restored to full operation and define requirements for recovery procedures
Refined Design analysis in faulted conditions				
P7	AO5	a1	Refine the Safety Requirements (integrity properties from the failure approach) for the refined system design of the SESAR solution	Refined Safety Requirements are derived considering the refined design and requirements derived at initial design level (P5P6_AO5) - Identify all hazardous failure modes of the technical system at the functional-requirements level - Identify functions which have no safety effect. - Provide traceability of equipment level failure modes to initial design failure analyses and reconcile any discrepancies.

Ref			Refined system design Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
P7	AO5	a2	Identify all reasonably foreseeable sources of common cause or other dependent failures	For instance: • Perform Common Cause Failure Analysis (including identification of CCF groups from minimal cutsets of fault tree and expert judgement). • Perform design HAZOPS applied to system elements and their interactions • Perform Single-point-of failure-analysis (part of FTA). • Perform FMEA at design element level to confirm that there are no unexpected consequences of individual element failures (bottom-up analysis)
P7	AO5	a3	Show that measures are in place to mitigate sources of dependent failure	• Design reviews. • Review of engineering procedures/activities which might affect multiple equipment at the same time; design of procedures
Refined System design non-safety elements, emergent properties and impact on safety nets				
P7	AO6	a1	Show that non-safety elements of the refined system design do not adversely affect safety	Same activity detailed in P5P6_AO6_a1 but for the refined design.
P7	AO7	a1	For the refined design, show also that there are no emergent properties of the design that could allow non-safety functions to interfere with safety functions and data sources / flows	Same activity detailed in P5P6_AO7_a1 but for the refined design.
P7	AO8	a1	Check that the refined system design operates in a way that does not have a negative effect on the operation of related ground-based and airborne safety nets	Same activity detailed in P5P6_AO8_a1 but for the refined design.
Refined Safety Requirements realism				
P7	AO9	a1	Show that all Refined Safety Requirements are capable of being satisfied in the targeted physical	• For Safety Requirements related to hardware and software, evidence could be obtained by analogy with known equipment for which similar Safety

Ref			Refined system design Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
			system comprising hardware, software, people and procedures	Requirements have already been satisfied or, where this is not available, by consulting the appropriate ATM/ANS equipment technical experts. - For the human tasks identified in the Safety Requirements, it would be appropriate to use some form of Tasks Analysis to show that the tasks are reasonable for the conditions under which they are expected to be performed and to use some form of Human Reliability Assessment to show that the integrity required of (or assumed for) each task is itself reasonable given the nature of the task and the conditions under which it is expected to be performed – see Guidance L and HP Reference Material (HPRM) [Ref. [8]] - For Safety Requirements related to procedures, evidence could be obtained by analogy with existing, proven procedures or, where this is not available, by consulting the appropriate operational experts
Completeness and correctness of refined safety requirements				
P7	AO C&C ⁴	a1	Verify that the Refined Safety Requirements (both functionality & performance properties from the success approach as well as efficiency of mitigation measures for the failure approach) are complete and correct by reference to the initial Safety Requirements by: Ensuring backward traceability between Refined SR to Initial SR	Traceability is done by mapping the Safety Requirements (functionality and performance) for normal and abnormal conditions to the corresponding Safety Objectives. Real-time Simulations (RTS – see Guidance M) and Life Trials (see Guidance N) are usually the validation activities to be used at that stage. Where significant HF issues are involved, specific HF Lab techniques can be used to supplement the data from simulations (see Guidance L). Human factors and timing properties issues are examples of issues that may require dynamic risk modelling (see Guidance K).

⁴ This Assurance Objective is called “C&C” (Completeness&Correctness) and is associated to the outcome of the previous Assurance Objectives (from AO1 to AO9).

Ref			Refined system design Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
			- For each scenario, identify those aspects / properties of the refined design that it has not been possible to model in the above (static) analyses - From those, define observable and measurable safety validation objectives in the VAL Plan - Checking that the system design operates correctly in a dynamic sense, under all conditions - Collection from the validation exercise (VAL Report) of the required evidence with respect to the safety validation objectives and amend (or otherwise) the set of refined safety requirements.	Safety-related Validation Objectives for those validation exercises and activities are to be redefined based on the Refined Safety Requirements (functionality & performance derived for normal and abnormal conditions as well as mitigations measures for the failure approach), together with the information captured within the operational level, the defined system level design. The type of data to be collected during the validation activities and the means for doing that also needs to be defined and described in the Validation Plan. The collected data from the validation exercises is then to be analysed and summarised, they are the evidence showing the satisfaction (or not) of the corresponding safety-related Validation Objectives. The existing list of refined safety requirements is then to be completed/updated as necessary. All those results and conclusions are to be documented in the Validation Report, but also in the Safety Assessment Report. A summary of those results is also to be documented in the Performance Assessment Report as per the corresponding template (SPR-INTEROP/OSED Part V – PAR). Coordination with HP is here required in: - ensuring a consistent set of validation objectives and associated success criteria (as per the VAL Plan Template); as well as - analysing the evidence being collected against the validation objectives
P7	AO C&C ⁵	a2	Show that all Assumptions that have been made in the previous lifecycle phases, on which the refined Safety Requirements depend, are necessary and valid	Same activity detailed in P5P6_C&C_a2. Validate all assumptions including any additional assumption identified at the refined design level.

⁵ This Assurance Objective is called “C&C” (Completeness&Correctness) and is associated to the outcome of the previous Assurance Objectives (from AO1 to AO9).

Ref			Refined system design Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
Safety Process Verification				
P7	AO10	a1	Show that all assurance in Guidance A.4 applies to a known system configuration and which is consistent with the system configuration of Assurance activities belonging to P5P6_AO9 .	Satisfaction of this objective requires careful configuration control of the various representations of the system throughout the lifecycle. See also SAM, PSSA Introduction, section 6.
P7	AO11	a2	Show that the evidence for the refined safety requirements is trustworthy	Backing evidence is obtained from the properties of the processes by which Direct Evidence (products) was obtained, and shows that those processes, tools and techniques, human resources etc. were appropriate, adequate and properly deployed. Evidence must be shown to be trustworthy, by demonstrating, amongst other things: - the suitability of the processes, tools and techniques etc. that are used to generate the evidence obtained from the safety assessment - the correct application of those processes, tools and techniques - the competence of the personnel applying those processes, tools and techniques.
Note on P8, P9 and P10			Safety Assurance objectives and activities related to Principles P8, P9 and P10 refer to V-cycle stages post V3. As a result there are not further developed in this Guidance document.	

Table 4: Detailed safety assurance activities for the SESAR Solution's refined system design

Guidance B On describing the Operational Environments

B.1 Introduction

Describing the Operational Environments in a generic manner is an unfeasible activity. However several examples can be provided, i.e. a typical description of the Operational Environments for En-route, Terminal Area operations and Airport operations, which would normally include some or all of the points listed in paragraphs **B.2** and **B.3** below.

Wherever the operational environment remains unchanged with the Solution introduction, it should be stated in the description.

Note that there should be consistency between what is in the environment description and what is shown as external entities in the design engineering models (e.g. EATMA, logical model).

The methodology in **Guidance J**, in particular Step 1, describes how important it is to build an understanding of how work is currently performed in the operational environment, which includes a detailed description of the later.

B.2 En-route and Terminal Area Operations

Include a description of the following, as applicable:

- Airspace structure and Boundaries
- Types of airspace / ICAO classifications
- Route structures (as applicable) and any restricted airspace (temporary or otherwise)
- Airspace users – e.g. commercial jets, military aircraft (flying as OAT) general aviation, very-light jets, unmanned aerial vehicles etc.
- Flight rules – IFR and/or VFR and/or OAT
- Traffic levels and complexity
 - Low complexity
 - Medium complexity
 - High complexity
 - Very high complexity
- Significant weather and other meteorological conditions
- Local terrain features, obstacles etc.
- Environmental constraints
- ATM/ANS Services to be provided (with special focus on the applicable separation minima, stating whether they are existing or proposed)
- Aircraft ATM capabilities
- Ground ATM capabilities (as far as they are out of the scope of the changed/impacted ATM/ANS functional system introduced by the Solution; for more details see **Guidance C**).

Include also any other points (*i.e.* not listed above) that are relevant to the safety assessment in question.

B.3 Airport Operations

Include a description of the following, as applicable:

- Airspace structure and boundaries relevant to airport operations (including classification of airspace adjacent to the airport)
- Runway, taxiway, apron and/or stands configuration, geometry and dimensions
- Runway-Taxiway and/or Taxiway-Apron interface
- Airport category (in terms of movements)
 - Small
 - Medium
 - Large
 - Very Large
 - Others
- Traffic distribution in time
- Traffic distribution in space around airport
- Effect of other airports in the vicinity including military airfields
- Airport users – e.g. commercial jets, military aircraft (flying as OAT) general aviation, very-light jets, unmanned aerial vehicles etc.
- Aircraft characteristics and ATM capabilities – mix of aircraft types using airport.
- Traffic characteristics (passenger, freight, training, general aviation and others)
- Local terrain features, obstacles etc.
- Weather / other meteorological and visibility conditions
- Navigation / landing aids
- Environmental constraints
- ATM/ANS Services to be provided (with special focus on the applicable separation minima, stating whether they are existing or proposed)
- Aircraft ATM capabilities
- Ground ATM capabilities (as far as they are out of the scope of the changed/impacted ATM/ANS functional system introduced by the Solution; for more details see **Guidance C**).

Include also any other points (*i.e.* not listed above) that are relevant to the safety assessment in question.

Guidance C On Safety scoping and change assessment

C.1 Process

Safety Scoping & Change Assessment is the preparatory process of identifying the main safety issues associated with a specific Solution as soon as possible after an Operational or Technological Concept has been developed and to help in deciding whether a full (i.e. carrying out all safety assurance activities defined in **Guidance A.2, A.3, and A.4** for ATM Solutions, or safety activities defined in Guidance O for technological Solutions) safety assessment is required.

It undertakes an initial identification of the scope of the change and provides an initial assessment of the safety implications of the Solution. It should address, amongst other things:

- what the Solution is seeking to achieve (e.g. to deliver benefits in capacity, efficiency and/or safety),
- the extent, boundaries and interfaces of the functional system subject to the change (i.e. being considered in the scope of the Solution), encompassing affected parts of the remainder air navigation services and underlying functional systems, its intended functions as well as the context (operational environment) in which the change is intended to operate,
- the possible impact on safety (in general terms only, since a safety assessment would not have been started at this stage),
- the criteria for deciding what is “safe” in the context of the Solution (this mainly apply to ATM Solutions)
- and, in broad terms, the strategy for demonstrating safety.

The results of this process will allow to issue a Safety Plan (in accordance with SAF PLN template for ATM Solutions⁶) aimed at specifying the safety assurance activities to be carried out by the Solution, whilst recording the relevant safety assessment information available at this initial stage (to be further used as input to the Safety Assessment Report).

The process described herein will be carried out within a workshop with the various projects belonging to the relevant Solution and involving also the HP expertise to ensure full co-ordination between SAF and HP. The different steps in the process are shown in the following table. The tasks are logically organized. However, the dynamic of the workshop might lead to some adaptations in order, merging, etc.

Note that even if the process described herein is applicable for all type of SESAR Solutions, it is mainly oriented to ATM operational Solutions; specific notes for Technological Solutions are then included as necessary in order to provide specific guidance to those Solutions.

⁶ Note that there is currently no Safety Plan template for the Technological Solutions, however the safety plan shall be documented in Appendix A of the TVALP.

Task	Guidance
General Solution Issues	
#1 Determine the content, deliverables, scope and major milestones for the Solution.	Refer to the general Project documentation for the Solution
#2 Determine who the Solution Stakeholders are and what: • expectations • issues • responsibilities towards the Solution they may have	Refer to the general Projects documentation and elicit further during the Safety Scoping & Change Assessment workshop.
#3 Understand the Operational / Technological Concept	An outline should be presented at the Safety Scoping & Change Assessment workshop to ensure a common understanding / agreement.
#4 Describe the benefits expected from the Solution in terms of: Capacity, Environment, Efficiency, Economy, Safety, Interoperability, etc.	Refer to the general Project documentation, including its Business Case. The benefits sought by the stakeholders, incl. users requirements, may vary between different ANSPs – e.g. the introduction of automation may be used to improve safety by one ANSP and to improve capacity by another ANSP – therefore, agreement amongst members of the Solution at this stage is essential to ensuring that the aim of the safety aspects of the Solution is established in the most beneficial way. For Technological Solutions potential benefits, and in particular safety, are mainly to be described through the corresponding operational use(s) of the technical concept.
#5 If the Solution has to deliver a safety benefit, determine what is expected and how achievement will be judged. If the Solution is to be safety neutral, how is this to be expressed?	Refer to the general Project documentation and elicit further during the Safety Scoping & Change Assessment workshop. This documentation includes but is not limited to e.g. Validation Strategy, the Solution Validation Plan, initial version of the OSED to get a first understanding of how the declared (if relevant) safety benefits will be assessed (e.g. specification of suitable and measurable validation objectives in the validation plans), etc. Same as for item #4 for Technological Solutions.

Task	Guidance
Change assessment	
#6 Determine the baseline (reference) for the Change Assessment, i.e. what exists before the change in terms of: • Operational Environment (OE) • ATM/ANS & underlying functional systems and operations • applicable regulations (safety and general) and standards (safety, operational and equipment)	Guidance is provided in Guidance B for the description of the 'specimen' OE. Key variability in OE conditions can be captured here by using the method described in Guidance J (Step 2). Any change is, by definition, assessed relative to what existed before the change. The baseline (reference) for the assessment may be what exists at the time of the assessment or, in some cases, what will exist when the change will be deployed. Clearly, not all ANSPs will be starting from the same current OE and system configuration and, therefore, stakeholder agreement at this stage is essential to ensuring that the baseline for the Solution is established in the most beneficial way. Refer to the general Projects documentation and elicit further during the Safety Scoping & Change Assessment workshop. For Technological Solutions the main purpose here is to determine: - the related ATM solutions which address the operational uses of the corresponding Technological concept. - The applicable regulations and standards.

Task	Guidance
#7 Determine the modified Operational Environment (OE) in which the new/modified ATM/ANS Functional System is intended to operate, if that is a pre-requisite to the change.	Refer to the Operational Concept and elicit further during the Safety Scoping & Change Assessment workshop. Guidance is provided in Guidance B. The introduction of the Solution might request certain adaptations to the Operational Environment, compared to the baseline (reference). These OE changes need to be clearly identified and agreed. Important note on OE: The properties of the OE are crucial to a safety assessment – specifically, a safety assessment that is valid for one OE may not be valid for a different OE. Thus, in order to be complete, a safety assessment cannot be generic – it has to be specific, to a particular OE – therefore, stakeholder agreement at this stage is essential to ensuring that the OE selected for the Solution is established in the most beneficial way. Indeed a set of safety requirements satisfying a set of safety criteria can only be true for a given environment. Changing the environment might invalidate the demonstration of the requirements-satisfaction. The SESAR work programme should define the given environment for which the validation activities will be carried out, identifying any modification between the Reference and the Solution. Eventually, i.e. once a Solution is declared an eligible candidate to move to V4, then ANSPs in particular would have to adapt the SESAR assessments to take into account the local environments where the Solutions will be hosted. This is not directly applicable to Technological Solutions, but it can be taken into account if necessary through the ATM Solutions identified in previous item #6.

Task	Guidance
#8 Elicit the details of the change(s) to be brought by the Solution, with respect to the baseline (see item 6 above) including: • Human actors' roles and responsibilities • Operating methods (procedures, airspace structure, etc.), tasks, practices • Technical systems (architecture, functionalities and performance) • Human and technical systems ○ Allocation of tasks (man-machine) ○ New or modified HMI • Change in Teams and Communication • Change in HP-related transition factors (staffing, competence, acceptance and job satisfaction)	Definitions available in HP Reference Material (HP RM) For Technological Solutions the main Human Performance aspects to be addressed are those related to HMI, but any other relevant factor impacted by the Technological concept also needs to be identified and addressed.
#9 On that basis, summarize what is removed, added and modified at the level of: • Operational level Specification • Design (High level architectural representation of the system design)	This is an initial assessment only but must be rigorous enough to decide to which extent the safety assessment of the Solution will be conducted (proportionality or scalability). As an example, an Operational Project Solution dealing with the Remote Tower might involve no change in end user requirements and operational specification but radical change of the functional system design. For Technological Solutions, the purpose here is to identify the elements in the high level architecture of the ATM Operational Solution(s) identified in item#6 that are relevant with respect to the Technological concept.
#10 Identify the need for new or modified regulations	This is an initial assessment only but must be rigorous enough to assess whether changes to regulations (incl. PANS-ATM, PANS-OPS, etc.) is required

Task	Guidance
Safety Strategy	
#11 Determine the relevant pre-existing (aviation) hazards that the Solution operational services have to mitigate in the relevant operational environment.	By definition, these aviation hazards exist in the operational environment before any form of ATM de-confliction has taken place. It is therefore the primary purpose of the relevant Solution operational services to contribute in mitigating (some of) them. See Guidance E.2. Note: this is not applicable to Technological Solutions.
#12 Determine and justify the Safety Criteria, including criteria as per Guidance D but also, where applicable, the safety-relevant regulatory and organisational requirements as well as any standards to be applied (e.g. ICAO Annexes)	General guidance on Safety Criteria is given in Guidance D.2. This shall be done in coordination with Transversal Activities to ensure the consistency of the safety criteria across all Solutions. This is achieved by using the Accident-Incident Models (AIM) and the methodology to allocate performance requirements to generate quantitative Safety Performance Targets. As the Safety Criteria are directly related to the consideration of safety benefits, or to the consideration of other benefits whilst maintaining current safety levels, stakeholder agreement at this stage is essential. For Technological Solutions, Safety Criteria as described in Guidance D are not to be defined. Instead, those Solutions have to : - Define the Technological System Safety Specification, which mainly encompasses the relevant requirements that the technological concept has to comply with. More detail on the TSSS is provided in Guidance O.2 and O.3.1. - The applicable safety-relevant regulatory requirement also have to be identified.
#13 Decide the safety deliverables to be produced and for whom (i.e. for which stakeholders) they are intended and agree on planning	Determine the main safety assessment activities to be conducted in the operational specification and design stages corresponding to the level of maturity (V1 to V3) expected for the Solution, in order to be able to outline the intended content of the safety deliverables to be produced. It is very important to get stakeholder agreement on these so that what is produced is of more benefit to them.

Task	Guidance
#14 Determine whether or not the Solution affects, and/or depends on, the safety assessment and validation activities associated with other Solutions or on-going operations.	This will help to determine the scope of the Safety Assessment
#15 Record any other safety/HP issues or uncertainties that were identified during the Safety Scoping & Change Assessment process and which need to be addressed during the subsequent safety assessment.	Any safety issues (identified in the workshop and not explicitly covered by the Safety Criteria or the Technological System Safety Specification) need to be recorded, and further monitored as the safety assessment is progressing HP issue analysis (see Appendix E of the HP RM[8] and record in HP Log – Appendix B of the HP RM).

C.2 Tailored Safety Assurance Objectives and Activities per type of change

The Safety Assurance Objectives and Activities presented in **Guidance A** are all generic. This means that they cover the case of a change to the ATM/ANS functional system that is so fundamental that all of the Safety Assurance Objectives (but not necessarily all of the Activities) specified in this document need to be completed.

In many cases, however, the scope of the change is smaller, affecting only some parts of the ATM/ANS functional system, but not impacting the operational environment, the user requirements and even the operational service delivered. For such cases it would probably not be cost effective to carry out all the Safety Assurance Objectives and Activities at the operational and design levels – rather, it would be better to focus resources on Implementation.

However, it has been emphasized in the main body of this document that the Safety Assurance Objectives and ultimately the Activities are driven by the Principles – not the other way around. Therefore, if we wish to “miss out” some of the generically defined Objectives and Activities then we must justify that.

In the case of Technological Solutions, i.e. mainly related to a purely technology-replacement, safety activities presented in **Guidance A.2 to A.4** does not apply as it would normally have no effect on the operational environment, the user requirements, the service delivered, or the functional or logical aspects of the functional system design. For Technological Solutions a dedicated set of generic safety activities is presented in **Guidance O**.

For both ATM and Technological Solutions there are two aspects to the process:

- execution of an Initial Change Assessment as part of the Safety Scoping & Change Assessment process, as described in **Guidance A.1** (and in **Guidance O.3.1** for Technological Solutions) and further detailed in **C.1**.
- definition of a tailored set of assurance activities: see **Figure 1** below for the process related to ATM operational Solutions; no specific schema is provided for Technological Solutions, but the an equivalent process is to be applied to tailor the set of assurances activities from the list provided in **Guidance O**, i.e. deciding to implement or not each of them and justifying why for each decision.

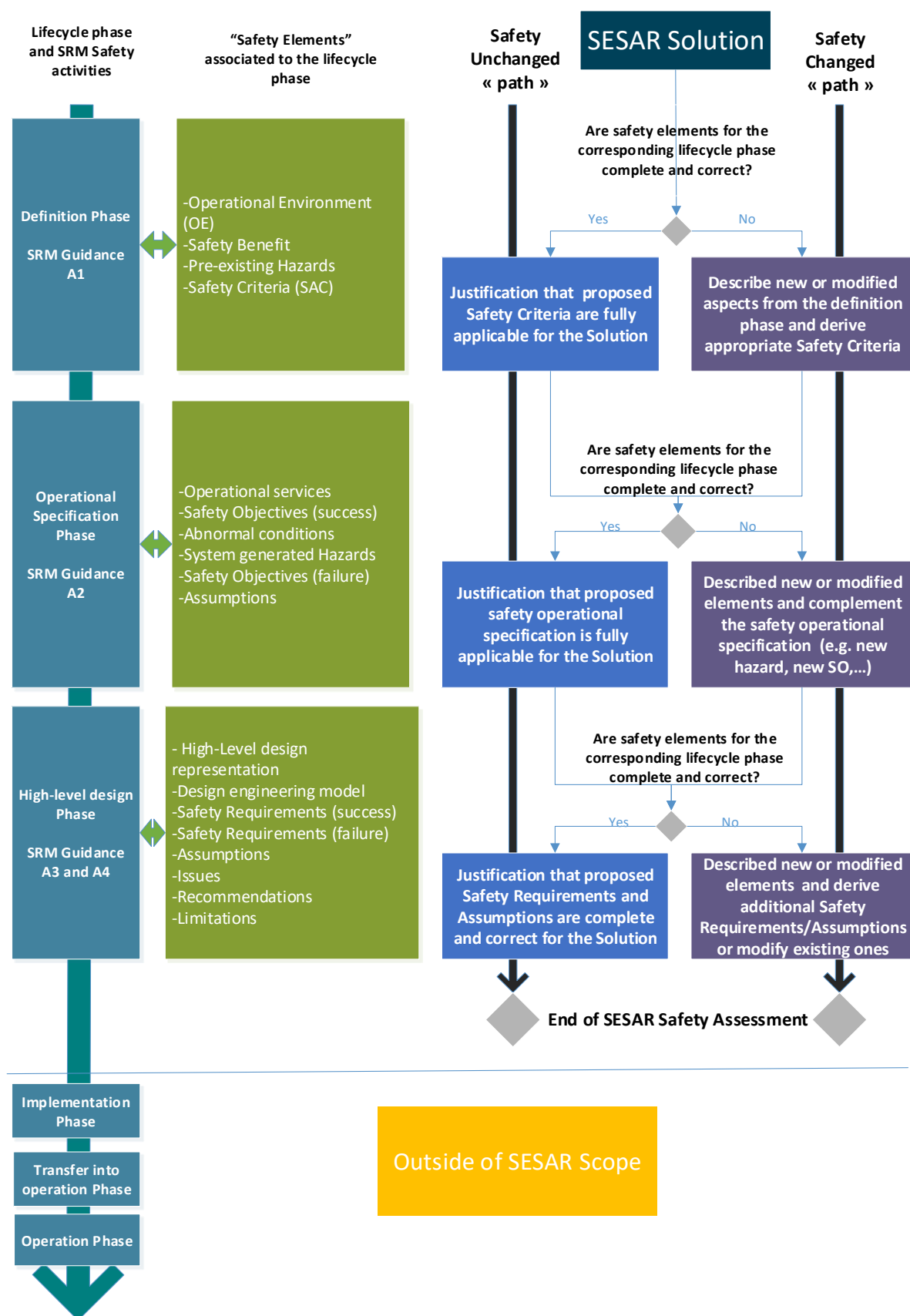


Figure 1: Selection of safety assurance activities from a change assessment

Guidance D On defining Safety Criteria



As per the SRM definition:

‘Safety Criteria’ shall mean explicit and verifiable criteria, the satisfaction of which results in tolerable safety following the change. They may be either qualitative or quantitative and either absolute or relative. They include not just specific risk targets but also safety (and other) regulatory requirements, operational and equipment standards and practices.

Note that despite the terms Safety Criteria – SAC is used here this guidance only focuses on the risk targets part of the SAC.

Note that Safety Criteria is to be defined for ATM Solutions. Technological Solutions have to define the Technological System Safety Specification instead, as explained in **Guidance A.1**, **Guidance C.1** and **Guidance O**.

D.1 Overview

One of the first actions after identifying the nature and scope of the Solution is the setting of safety criteria that define what is considered tolerably safe for the change being introduced by the Solution and permit the validation of the expected safety impact of a Solution on ATM provision. In SESAR, due to the multitude of operational projects involved and to the necessity to assure that overall SESAR Safety Performance Ambition for future ATM is to be satisfied at the different concept development steps, it is essential that these safety criteria are identified and described based on a common framework. In SESAR, this framework is provided by the **Accident Incident Model (AIM)** detailed in **Guidance I.1**.

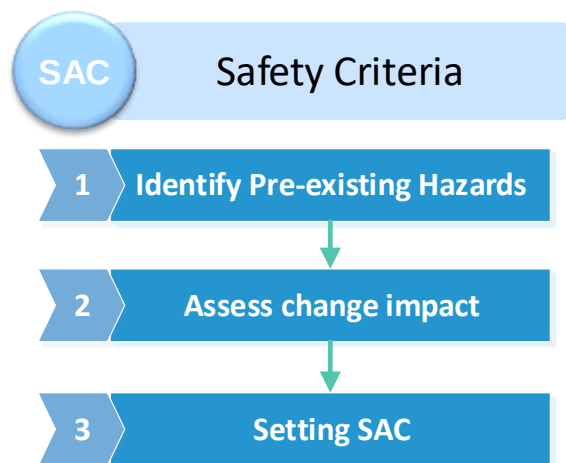
The AIM risk model provides a set of templates (one for each accident type) that are used to identify where and how each the operational improvements that each Solution are making will impact the safety of ATM provision. The method involves the identification of those parts in the risk models that would be impacted and thereby the measurable elements that would be either increased if safety was reduced, decreased if safety improved or unchanged in the case of operational changes that should not impact safety.

The SAC setting process described in this guidance is based on the used of AIM. It is important thought to note that, for each Solution, safety criteria need to be defined for all the safety risks impacted by the Solution, even for those for which no AIM model is yet available.

D.2 SAC defined at Solution level

SAC are set during the Scoping and Change Assessment activities (see **Guidance C**) that are part of the safety planning process. AIM models are used by safety experts within the Solution team with the assistance of operational and technical experts on the changes involved.

The definition of Safety Criteria is done in three steps:



1. Identify pre-existing Hazards: based on safety and operational expert judgement during dedicated Scoping and Change Assessment workshop, the relevant pre-existing hazards for the Solution are identified in order to select afterwards the relevant AIM models and risks to be considered for setting the SAC.

2. Safety impact assessment of the operational change: the potential safety impact of the Solution is first qualitatively assessed at the level of those identified AIM model (at the barrier, contributors and precursors level). This impact is then quantified as a % of improvement / reduction in barriers performances or contributors and thus on precursors occurrences. Traffic has to be considered in this process by taking into account any change in capacity that the Solution may also envisage to provide

3. Setting the SAC: once the safety impact of the change is understood, the Safety Criteria, defining the tolerable safety following the change, are to be set at the level of the corresponding precursors in the models, indicating the expected benefit, neutrality or degradation, and taking into account the potential traffic increase.

The three steps mentioned here are described in more detail in the next sub-sections. An example of the process for setting the SAC as described in this guidance is provided in **D.4**.

D.2.1 Identify Pre-existing Hazards

For the ATM/ANS system the pre-existing hazards and risks are generally those that are inherent in aviation and for which the main “raison d’être” of ATM/ANS is to provide as much mitigation as possible. These hazards, called also “aviation hazards”, pre-exist in the operational environment before any form of ATM/ANS planning, de-confliction or other form of mitigation has taken place.⁷

⁷ The purpose of most safety-related systems is to mitigate the hazards (and associated risks) that are pre-existing in the operational environment of the system concerned. These hazards are, therefore, not caused by the system – rather, the main purpose of introducing the system is to eliminate those pre-existing hazards or at least maintain the associated risks at a tolerably low level.

Only the pre-existing ATM/ANS hazards and risks that fall within the scope of the safety assessment, i.e. which are relevant for the Solution, need to be identified.

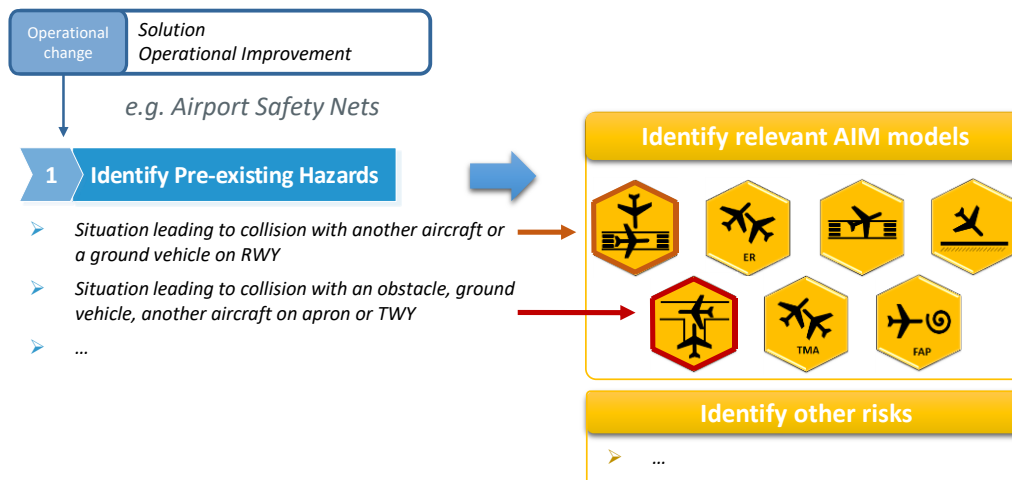


Figure 2: Identification of pre-existing hazard and relevant AIM risk models

A list of pre-existing hazards based on the SESAR 1 and SESAR 2020 safety assessment experience is provided in Guidance E.2.

Based on those pre-existing hazards, the relevant Accident-Incident Models (AIM) are to be identified. For example, as show in Figure 2, if the Solution has to deal with the pre-existing hazard related to 'Situation leading to collision with another aircraft or a ground vehicle on Runway' then the AIM model Runway Collision (RWY-Col) is to be used for setting the SACs.

Any other risk relevant to the Solution, but for which an AIM risk model is not (yet) available has also to be identified.

D.2.2 Impact assessment of the Change

The qualitative assessment is performed by the safety experts within the Solution team on the basis of the relevant AIM models identified in previous step. But it also requires the participation of operational and technical experts that have a good understanding of the ATM concepts brought by the Solution and processes / procedures involved.

The objective of the assessment (as shown in **Figure 3**) is to identify where the operational change will impact the ATM risk, at the level of the base events (lowest level risks) in the relevant model(s) for each impacted barrier(s) and induced precursor(s). Both the potential contribution to the degradation of the efficiency of the barriers of the ATM/ANS functional system when it would work as specified in the Solution (success approach) and when it would deviate from the specification (failure approach) need to be considered in the analysis. For that, detailed information available in the OSED (for example description of the operational change but also scenarios identifying particular abnormal conditions or failures, if available) is to be used.

For completely new concepts (such as Conformance Monitoring) the AIM model has additional base events to permit the impacts to be modelled in the future systems. It is of course necessary in such cases for the operational experts to determine the impact of these new ATM elements on the risks of the considered baseline at the barrier level.

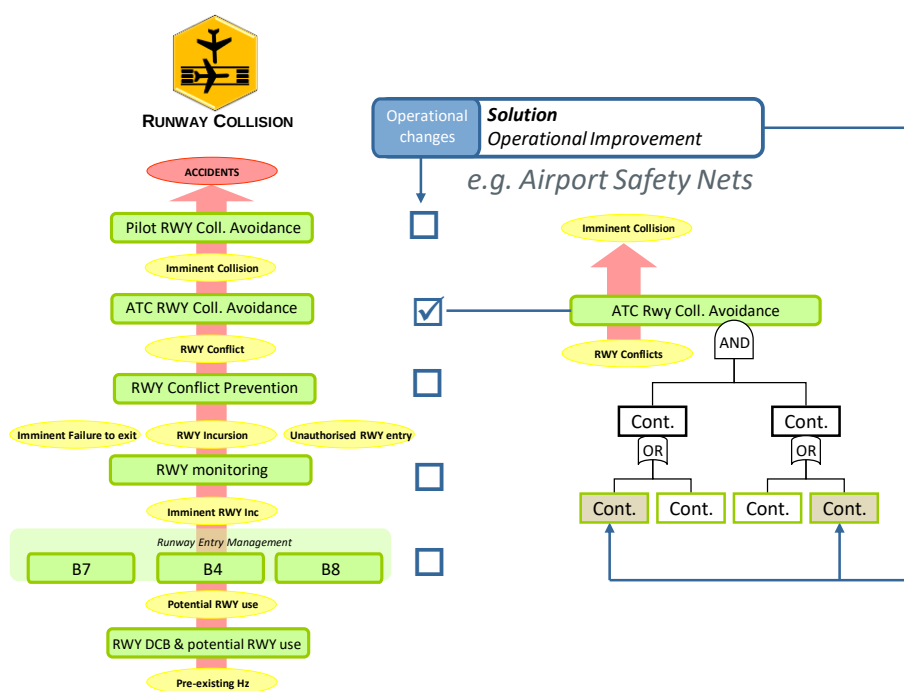


Figure 3: The base events affected in the AIM fault tree for each barrier

Afterwards, for each identified element in the AIM model(s) that the operational change will impact it is necessary to first qualitatively estimate if the result will be an increase or decrease in risk or if an increase is expected and that the result must be neutral (i.e. the increase has to be mitigated). Identification of whether there is a safety benefit or safety degradation and an estimate of the level of the safety impact (significant, minor, neutral) enables to agree the extent to which this could be translated into a percentage effect on safety.

Then experts have to decide on a quantitative estimate of the impact. This would normally result in a percentage improvement or deterioration on corresponding barriers performance and/or induced events occurrence. This estimate will be used to determine the predicted safety impact on precursors and thereby allow the setting of quantified SAC. It is acknowledged that the quantification of the expected level of the impacts may move the assessor into an area of uncertainty in particular in the early stage of a project.

Preliminary assessment done by the Transversal Areas project may provide an initial indication of this quantification. Outcomes from the Benefit Mechanisms performed by the Solution team are also to be taken into account.

	While performing this assessment, the impact of any change should include the effects of traffic increase on risk. Besides, not only safety aspects are to be taken into account for the setting of the Safety Criteria. Other relevant aspects concerning traffic increase and other KPAs are also to be identified and considered in these discussions (e.g. impact on airspace capacity).
---	--

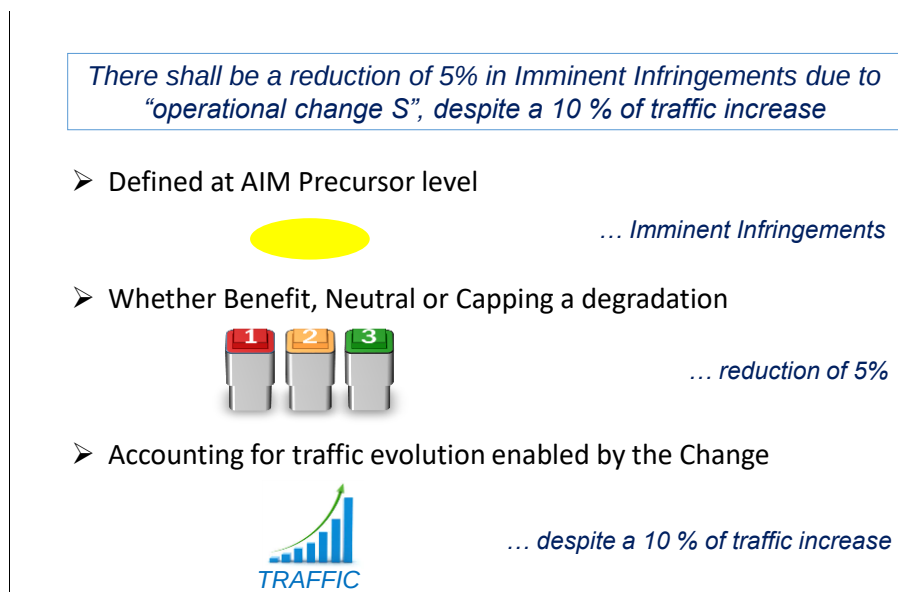
	As the Safety Criteria are directly related to the consideration of safety impacts, stakeholder agreement is essential in this process.
--	---

D.2.3 Setting the Safety Criteria

Once the qualitative and quantitative assessment have been done, the Safety Criteria are to be defined. The main three elements to be taken into account when defining the SAC are:

- To be defined at AIM precursor level
- To indicate whether a safety benefit is to be achieved, if the impact has to be safety neutral or if it is capping a degradation.
- To account for the traffic evolution enabled by the Change (if applicable).

See example below:



SACs can be expressed in a relative way (as in the example above) or in an absolute way (e.g. *Imminent Infringement shall be less than 5e-5 per flight hour (with the introduction of “operational change X”, taking into account a % traffic increase)*). In both case the potential traffic increase enabled by the corresponding Solution has to be taken into account.

Note that SAC(s) need to be defined for an operational Solution even when the impact is estimated as safety neutral and the level of traffic remains unchanged.

D.3 Closing the loop between the Solution and Transversal Areas Project

The Performance Ambition target for safety in SESAR is that given the implementation of SESAR, the absolute number of accidents (per year) shall not increase despite the increase in traffic as per the respective Airspace and Airport capacity targets for 2035.

One of the main purposes of Transversal Areas Project (TA) is to show that the safety provided by all the Solutions will contribute to achieve this ambition target at the end. For that, TA defines Safety Validation Targets for each Solution ensuring they are consistent with the SESAR safety Performance Ambition target.

Unlike for the other KPAs, the approach applied for defining the safety validation targets has a large amount of “bottom-up” assessment of the performance contribution from the Solutions.

As shown in Figure 4, this approach applied within TA is mainly based on two processes:

- Safety Performance Assessment at Programme level
- Setting the Safety Validation Targets for each Solution

Interactions between Solutions and those processes are also shown in Figure 4 and described in the next sub-sections.

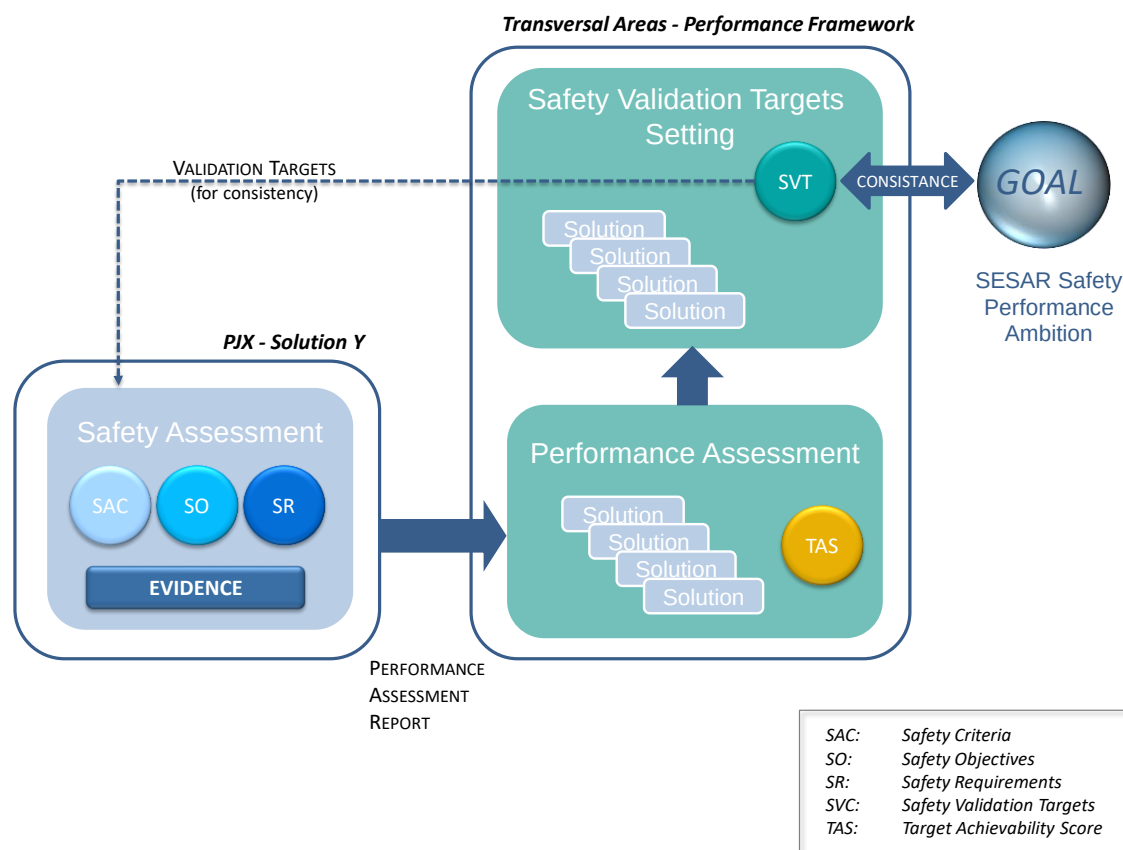


Figure 4: Interactions with Performance Framework - process overview

More details on these processes as well as the results of those tasks are available in corresponding Transversal Area - Performance Framework documentation.

Note: Please check in SESAR extranet for the latest version of the documents.

D.3.1 Solutions supporting Performance Assessment

In order for Transversal Areas Project to assess the safety performance being delivered by the Solutions, relevant information needs to be provided to TA Performance Framework by each Solution. The information to be provided includes:

- the detailed SAC, obtained through the process defined above plus any other SAC defined for the Change in the Solution,
- the justification for each SAC (using the AIM models or other data sources or tools)
- the evidence from the safety assessment and validation activities ensuring SACs are to be met (they vary depending on the V phase maturity).

All this information should already be available in the different Safety documents of the Solution, i.e. the Safety Assessment Report (SPR-INTEROP/OSED Part II) and the Safety Plan (VALP Part II). It is also to be provided from the Solutions to Transversal Areas through the following means (as planned by the Solution or on request):

- SPR-INTEROP/OSED Part V - PAR : Performance Assessment Report
- Estimation of Performance Assessment Questionnaire developed and managed by the TA Project

Based on this information, two types of measures are then calculated and used to show the results of the assessment in the Performance Assessment And Gap Analysis Report (PAGAR):

- **Process progress score:** this shows progress on the safety assessment process, being 100% a complete safety assessment at V3, providing full specification at high-level system design level and corresponding evidence ensuring SACs achievability.
- **Target achievability score:** this measure is the combination of the Safety Validation Target (SVT) allocated for each Solution and the process progress score mentioned above. The total of all those scores is then used to show achievability or potential gap with respect to the Ambition Safety Target.

D.3.2 Safety Validation Targets defined by the Transversal Areas

As mentioned before, the Safety Validation targets are defined following a bottom-up process, that means they are set based on the safety performance information mainly reported by Solutions through the Performance Assessment process explained above.

From all this information, mainly SAC and their justification are used to perform a consolidated impact assessment. As per the SACs at Solution level, this is done by Transversal Areas Project using the AIM risk models but this time for All the Solutions. Capacity Validation Targets are also taken into account in this assessment. The overall safety impact obtained for the whole Solutions is then compared with the Safety Performance Ambition, as the purpose is to ensure the target is met. In case it is not, specific Solutions for which additional safety benefit could be requested are identified and requested to update their SACs consequently. This iterative process stops when the Safety Performance Ambition is finally met.

Safety Validation Targets are expressed as *a percentage defining the expected reduction due to SESAR in the “total number of fatal accidents per year” with ATM contribution with respect to a potential outcome in a hypothetical “do nothing” case (no changes to ATM safety, while traffic is allowed to increase)*. They are defined at overall accident risk level and per type of accident.

The Safety Validation Targets are then the corresponding translation of the SACs defined by each Solution at AIM barriers/precursors level.

D.4 Example for SESAR Concept “Airport Safety Nets”

As per the allocation done within the SESAR Transversal Area Project, “Airport Safety Nets” (in the SESAR Step 1 framework) is expected to provide an overall safety improvement of 4.9% (safety improvement meaning, as explained above, reduction of potential number of fatal accidents per year with respect to a hypothetical “do nothing case”). This improvement is decomposed as follows:

- 4.8% reduction of Runway Collision
- 0.1% reduction of Taxiway Collision

These values have been determined taking into account the traffic increase foreseen for Step 1 which is 14% with respect to the SESAR 1 baseline.

In order to obtain these safety benefits defined above, the following improvements are needed in the performance of the barriers of AIM listed here after:

Concerning Runway collision model:

- 2.5% improvement of barrier B3A: Runway Monitoring
- 10% improvement of barrier B3: Runway Conflict Prevention
- 17.5% improvement of barrier B2: ATC Runway Collision Avoidance
- 5% improvement of barrier B1: Pilot Runway Collision Avoidance

Concerning Taxiway collision model:

- 5% improvement of barrier B3: Taxiway Conflict Management
- 25% improvement of barrier B2: ATC Taxiway Collision Avoidance
- 5% improvement of barrier B1: Pilot Taxiway Collision Avoidance

By applying these improvements in those barriers the impact on the corresponding precursors are (on which the SACs are usually defined) for Runway collision model (the ones for the Taxiway are not shown here but are defined in the same way):

SACs are expressed with respect to the ‘do nothing’ case described above:

- SAC#1 : There shall be a reduction of 3 % of the Runway Incursions due to the introduction of the Airport Safety Nets concept Step 1, taking into account the traffic for Step 1.
- SAC#2 : There shall be a reduction of 7% of the Runway Conflicts due to the introduction of Airport Safety Nets concept Step1, taking into account the traffic for Step 1.
- SAC#3: There shall be a reduction of 27% of the Imminent Runway Collisions due to the introduction of Airport Safety Nets concept Step1, taking into account the traffic for Step 1.

The same SACs can also be expressed in an absolute way, as shown here after for SAC#1:

- SAC#1 : Runway Incursions shall be less than $3.2e-5$ per movement with the introduction of the Airport Safety Nets concept Step 1, taking into account the traffic for Step 1.

As explained before, these SAC are the starting points for the Solution safety assessment. They need to be reviewed in detail by the Solution team, and split as necessary into the different Working Areas or projects being part of the same Solution.

In case a difference is found during this review, the Transversal Activities has to be informed in order to update safety validation targets and recheck the satisfaction of the SESAR Safety Performance Ambition.

Guidance E On Pre-existing Hazards & Operational Services mitigating them

E.1 Introduction

This Guidance focuses on two aspects of the safety specification of the ATM/ANS functional system at the operational level, in the Solution scope:

- Identification of the Pre-existing (Aviation) Hazards – covered by sub-section **E.2**. Error! Reference source not found.
- Description of the Operational services and their contribution to mitigate the Pre-existing Hazards – covered by sub-section **E.3**.

E.2 Suggested list of Pre-existing Hazards

The following pre-existing (aviation) hazards have been identified within the SESAR 1 and SESAR 2020 safety assessment to date (the list might be further completed).

For **En Route** operations the pre-existing (aviation) hazards will normally include the following:

- situation in which the intended trajectories of two or more aircraft are in conflict
- incursion in ARES (infringement by non-participating IFR traffic)
- ARES borders excursion by traffic using it
- encounters with adverse weather
- fuel shortage

For **Terminal Area** operations (encompassing Final Approach and Initial Departure), the pre-existing (aviation) hazards will normally include the following:

- situation in which the intended trajectories of two or more aircraft are in conflict (either down to IAF or during interception or during final approach or during initial departure or along the SID)
- situation where the intended trajectory of an aircraft is in conflict with terrain or an obstacle
- penetration of unauthorized airspace
- situation leading to wake vortex encounter (WVE)
- encounters with adverse weather

For **Runway / Taxiway** operations⁸, the pre-existing hazards (aviation) may include the following:

⁸ Runway operations are assumed to start soon after an aircraft is stabilised on Final Approach

- situation leading to collision with another aircraft or a ground vehicle on RWY (e.g. the intended trajectory of a landing aircraft is conflicting with another aircraft or vehicle on the runway area; the intended 3-D route of a taxiing aircraft would lead to collision with a ground vehicle or another aircraft on RWY or close to ground on landing / take-off)
- situation where the intended trajectory of an aircraft is in conflict with terrain or an obstacle
- another aircraft or vehicle inside the OFZ during a Cat II / III instrument approach
- another aircraft or vehicle inside landing-aid protection area during Cat II / III instrument approach
- situation leading to wake vortex encounter (WVE)
- situation leading to collision with an obstacle, ground vehicle, another aircraft on apron or TWY (e.g. situation in which the intended 3-D⁹ route of a taxiing aircraft would lead to collision with an obstacle, a ground vehicle or another aircraft on apron or TWY) ground or close to ground on landing / take-off
- situation in which the aircraft veer off, undershoot or overrun off the runway surface during landing
- adverse weather conditions like violent wind effects (thunderstorm, windshear) affecting aircraft vertical speed or tailwind or severe crosswind on landing / take-off
- birds close to / in path of aircraft, or animal on the runway
- Foreign Object Debris within the Runway protected area
- low runway-surface friction
- snow / slush on runway (high rolling drag situation)
- aircraft landing in/taking off from a wrong/closed runway
- aircraft using a closed taxiway
- aircraft attempts a landing with undercarriage retracted.

It should be noted that the list for Runway / Taxiway operations was derived for SESAR and some hazards might therefore appear to be beyond the scope of “traditional” airport ATM.

E.3 On describing the Operational services & their contribution to mitigate the Pre-existing Hazards

The Operational Service is what exists in the interface between the ATM/ANS Functional System and the Airspace Users. Operational Services are provided by the ATM/ANS Functional System to the User i.e. an aircraft or a group of aircraft.

⁹ In the horizontal dimensions and time

The ATM/ANS functional system contributes to the mitigation of the pre-existing hazards/risks (which are inherent to aviation) through the delivery of Operational Services to the aircraft. For that reason the Safety Objectives need to be defined at a level as close as possible to the Operational Services.

In order to grasp the safety contribution of an ATM/ANS functional system of a specific Solution, it can be represented at a high level as a black box (see Figure 5):

- the operational services delivered to aircraft represent outputs - WHAT is delivered to aircraft,
- whilst HOW are the operational services performed (the design of the ATM/ANS functional system in terms of system elements, their functionalities and interactions) is hidden.

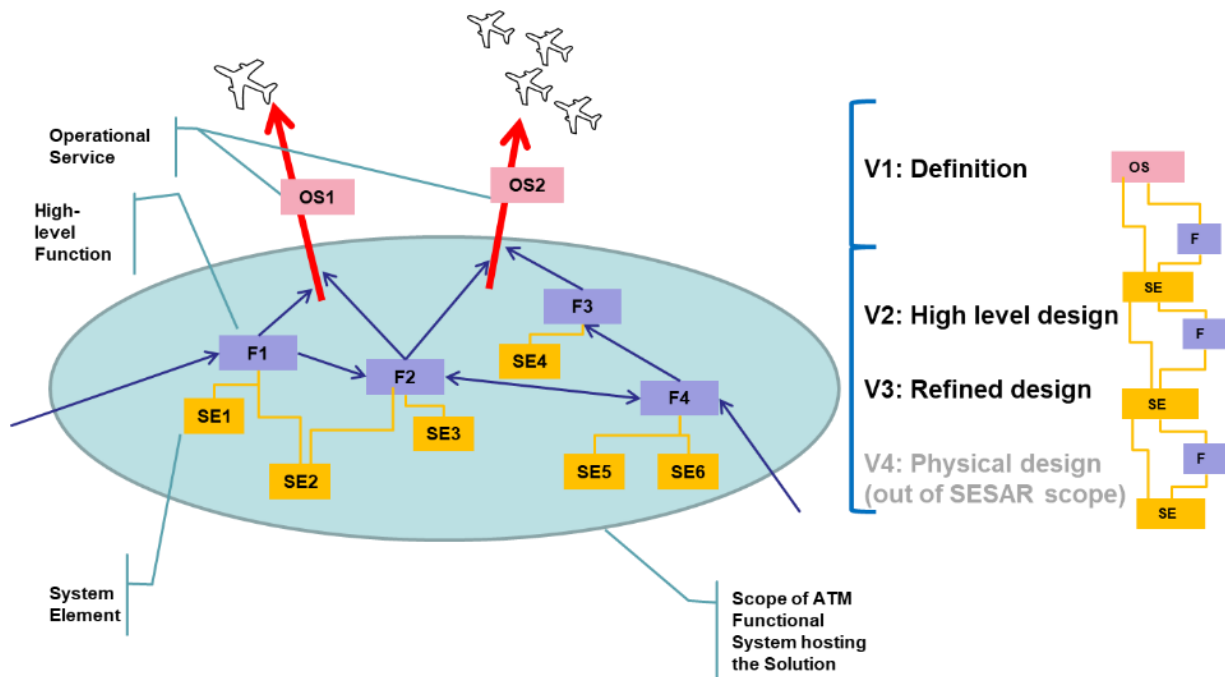


Figure 5. Representation of the Operational Services provided by the ATM/ANS functional system

Most of the Operational Services provided by the ATM/ANS functional system contribute to the mitigation of the aviation pre-existing hazards / risks. Consequently they can be represented through a mapping on the barriers/precursors of the AIM models.

For illustration purposes, the Figure 6 below proposes a list of Operational Services mapped onto the AIM MAC in TMA model.

Note that the list is not complete and the safety assessors need to perform an exhaustive identification of the operational services that are relevant for the scope of each Solution, considering all the relevant pre-existing hazards (listed E.2 above) and associated AIM models where available. As an example, the following operational services are also relevant for operations in Terminal Area:

- provide separation from terrain/obstacles
- prevent entry into unauthorized areas
- minimize wake-vortex encounters
- avoid adverse-weather encounters
- ...

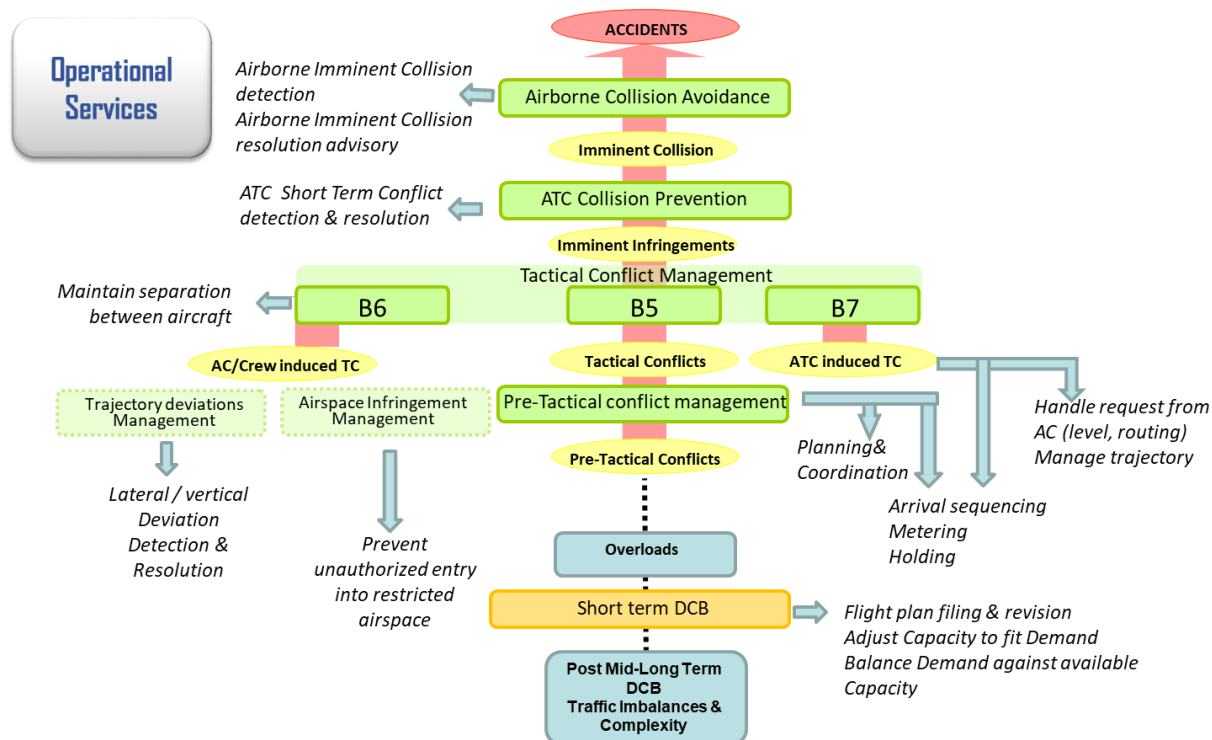


Figure 6. Illustration of several Operational Services mapped onto the AIM MAC in TMA simplified model

In describing the Operational services, in relation to the pre-existing hazards, it is important to explain to whom (i.e. to which airspace users) the services are provided, according to (for example) the types of user, the flight rules (IFR, VFR, OAT etc.) and the class of airspace concerned.

Guidance F On Setting Safety Objectives (success approach)

F.1 Introduction

This guidance is about setting **Safety Objectives (success-approach)** in order to mitigate the pre-existing aviation risks under Normal and Abnormal operational conditions such as to meet the Safety Criteria already set in **Guidance D**.

The Safety Objectives can be seen as the highest layer of safety requirements, representing the desired safety behaviour of the change at its interface with the operational context.

The Safety Objectives (success approach) specify formally the fundamental safety properties of the ATM/ANS functional system, in terms of functionality and performance, to ensure that this will actually happen in the subsequent design and implementation of the system.

F.2 Process for Setting Safety Objectives (success approach)

Setting the Safety Objectives (success approach) starts by the interpretation of the OSED Operational Concept specification (i.e. how the new concept contributes to the aviation safety).

The setting of the safety objectives is supported by the use of the EATMA representation considering the Operational layer (each Use Case being modelled through a process model made up of activities interacting via information flows – diagrams NOV 5 as per sub-section I.2).

This analysis is performed following and making use of the OSED Use Cases and their representation through EATMA Process Models (diagrams NOV 5) as defined by the Project. The purpose is to derive a complete list of Safety Objectives in terms of functionality and performance (for the conditions covered by the OSED Use Cases- namely all the Normal conditions, and potentially some Abnormal conditions), allowing to specify the Change involved by the Concept at the operational service level. That is performed by considering the operational concept introduced by the Solution as a series of continuous processes described through the Use Cases. That allows showing how the Safety Objectives participate in the achievement of the relevant operational services and contribute to safety barriers (in the relevant AIM models) i.e. how they contribute to meeting the Safety Criteria.

The following working method should be applied to derive the functionality & performance Safety Objectives (as part of the success approach) for the conditions covered by the OSED Use Cases (namely all the Normal conditions, and potentially some Abnormal conditions):

Step 1:

- For each Activity included in the Use Case (described via an EATMA Process Model, i.e. diagram NOV 5 as presented in next Figure 7):
 - Identify to **which Operational Service(s)** that Activity contributes to (operational services that need to be defined within the safety assessment as per SRM Guidance E.2.3),
 - Identify whether the Activity is **new or modified** and describe what is the change if possible,
 - Whether necessary, refine the information by highlighting specific information flows produced or consumed by the Activity,

- Based on the findings above (i.e. new or modified Activity), retain (if new or modified) or not (if the activity is not changed compared to current operations) the Activity and the related information as relevant input to the Safety Objectives derivation.

Step 2:

- Consolidate the information outcome from Step 1 above according to Use Cases and Operational services
- For each Operational Service within each Use Case:
 - Check whether the identified change(s) **is (are) safety relevant** (i.e. could the change impact the efficiency of a safety barrier or the occurrence of a safety precursor? the previously identified operational services are a necessary but not sufficient indication, given their link to the AIM models),
 - Derive one or several Safety Objectives in order to describe the safety-relevant changes in the delivery of that operational service by the Solution.

Note: Regarding the **Abnormal conditions which are not covered by dedicated OSED Use Cases**, the derivation of Safety Objectives (success approach) should be performed as per Guidance A.2 ref. P3P4 AO1 a3 and a4 (i.e. first identify the applicable external abnormal conditions and then identify existing/define new Safety Objectives functionality and performance such as to mitigate the safety effect).

F.3 Example of Application

The activities in each Use Case will be marked with the following coloured labels for traceability to the related Operational Services:

Legend	ID	Operational Service
	FPL#1	Flight plan preparation, filing, validation and distribution (focusing on Mission Trajectory in planning phase, including ARES cross check)
	ASM#1	Adjust the Capacity (to the extent where it is available) to fit the predicted Demand
...		

The activities and flows are codified (for easier referencing) using the following principle:

UCx-yz

UCx	x corresponding to the number of the related Use case
y	y corresponding to an activity (a) or to a flow (f)

z	z corresponding to correlative numbers from 1 to n
---	--

The activities identified as impacted by the change (i.e. either new or modified) will be highlighted in the EATMA Process Models with the following symbol: ★

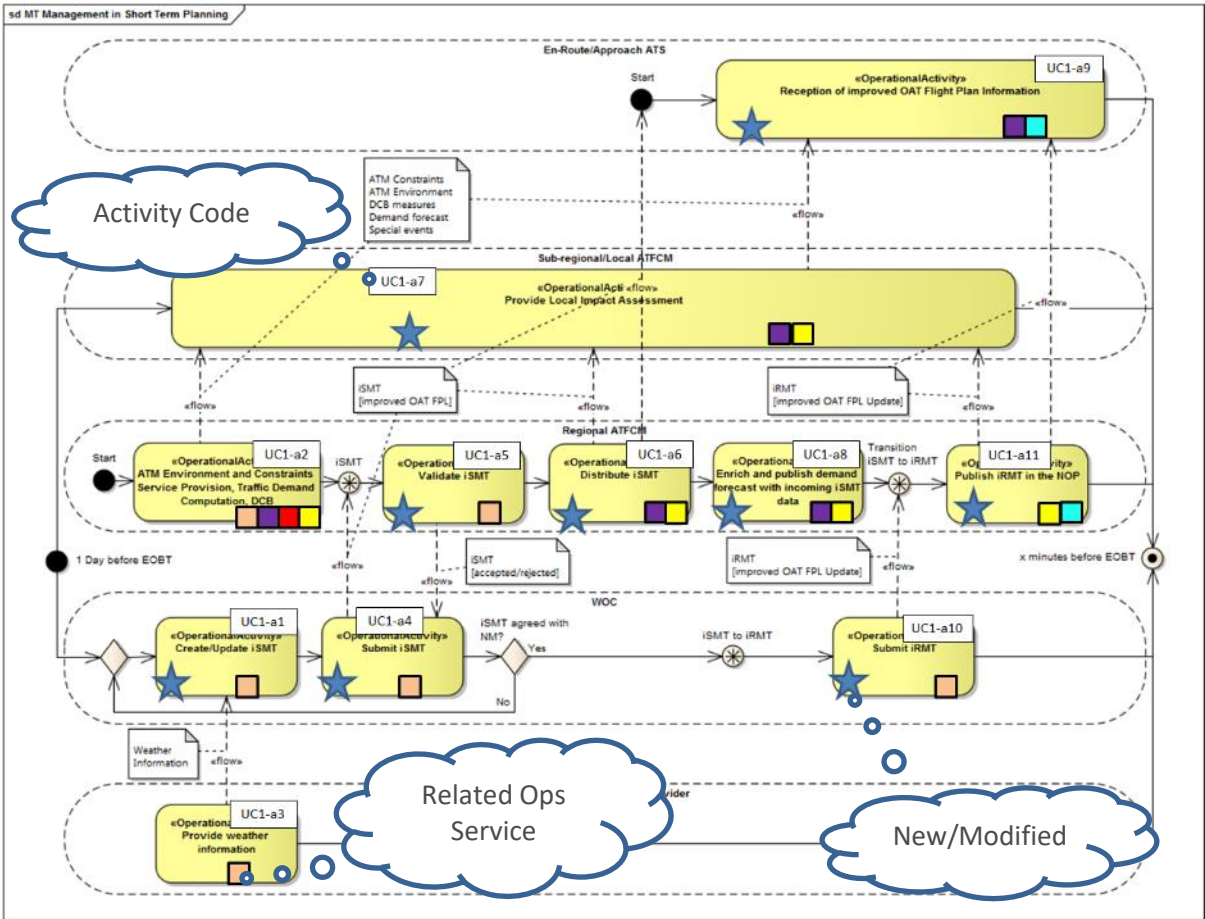


Figure 7. EATMA Process Model (NOV 5) used for analysing the change and the contribution to Operational Services

Example Outcome of the analysis

The table below shows an extract of a working table used for deriving the Success SO for Use Case 1 “MT Management in Short Term Planning” from PJ07.03 Mission Trajectory Driven Processes, where a change AND a safety impact were identified for a number of activities. Note that this working table is usually included in one of the Appendices of the SAR.

As it can be seen in the example below, for some EATMA activities that have been identified to be impacted by the new concept no safety objective was derived since the changes only have performance implications (see Activity UC1-a9).

The PJ07.03 SACs referenced in the table are detailed herein:

SAC#01a: The number of moderate and severe overloads shall not increase despite the x% increase in ENR sector(s) capacity enabled by PJ07.03 supported by PJ18.01 (mainly via the enabled reduction in sector capacity buffer).

SAC#01b: The number of moderate and severe overloads shall not increase in TMA sector(s)

SAC#05a: The number of Planning conflicts shall not increase despite the x% increase in ENR sector(s) capacity enabled by PJ07.03-18.01 (mainly via the enabled reduction in sector capacity buffer)

SAC#05b: The number of Planning conflicts shall not increase in TMA sector(s).

Operational Service	EATMA Use Case- Activity or Flow		Achieved by / Safety Objective [SO xx]	Related SAC# (AIM Barrier or Precursor)
UC1: Mission Trajectory Management in Short Term Planning Phase				
FPL#1: Flight plan preparation, filing, validation and distribution (focusing on Mission Trajectory in planning phase, including ARES cross check) phase)	Create/update iSMT	UC1-a1	SO 001: WOC shall submit (and resubmit if any update is needed) iSMT in time for enabling reliable traffic prediction	SAC#01a (B12: Short Term DCB)
	Submit iSMT	UC1-a4		SAC#01b (B12: Short Term DCB)
	Validate iSMT	UC1-a5	SO 002: Regional ATFCM shall validate iSMT in accordance with the applicable ATM constraints	SAC#01a (B12: Short Term DCB) SAC#01b (B12: Short Term DCB)
	Submit iRMT	UC1-a10	SO 003: WOC shall submit iRMT in full consistency with the validated trajectory	SAC#01a (B12: Short Term DCB) SAC#01b (B12: Short Term DCB) SAC#05a (B10-B11: Traffic Planning & Synchronization) SAC#05b (B10-B11: Traffic Planning & Synchronization)
ASM#1: Adjust the Capacity (to the extent where it is available) to fit the predicted Demand	Distribute iSMT	UC1-a6	SO 004: Regional ATFCM shall distribute the iSMT to Sub-regional/local ATFCM and ENR/APP ATS and update demand forecast accordingly	SAC#01a (B12: Short Term DCB)
	Enrich and publish demand forecast with incoming iSMT data	UC1-a8		SAC#01b (B12: Short Term DCB)
	Provide Local Impact Assessment Note: This operational service is not concerned with the iRMT, because too late for the sectors configuration to account for the iRMT	UC1-a7	SO 005: Sub-regional/local ATFCM shall receive iSMT and integrate it in the local impact assessment in view of appropriate Capacity adjustment and Demand balancing	SAC#01a (B12: Short Term DCB) SAC#01b (B12: Short Term DCB)

Operational Service	EATMA Use Case- Activity or Flow	Achieved by / Safety Objective [SO xx]	Related SAC# (AIM Barrier or Precursor)
	Reception of improved OAT flight plan information UC1-a9 Note: Inside this activity the iSMT reception is considered for Capacity adjustment purposes whilst the iRMT is considered for ATC service purposes (see "ATC services" below)	No specific safety objective, given the mitigation offered by ATFCM measures (e.g. STAM) in case of an inadequate sectors configuration	
...	...	...	...

Example of consolidated view in the main body of the SAR

The table below shows an extract of the SO (success approach) table, which is included in the main body (i.e. in section 3.6) of the SAR. It is mainly a consolidated version of the working table shown in the previous section.

ID	Safety Objective (success approach)	EATMA FP- Activity or Flow	Operational Service	Related SAC# (AIM Barrier or Precursor)
SO 001	WOC shall submit (and resubmit if any update is needed) iSMT in time for enabling reliable traffic prediction	UC1-a1 UC1-a4	FPL#1: Flight plan preparation, filing, validation and distribution (focusing on Mission Trajectory in planning phase, including ARES cross check))	SAC#01a, SAC#01b (B12: Short Term DCB)
SO 002	Regional ATFCM shall validate iSMT in accordance with the applicable ATM constraints	UC1-a5	As above	SAC#01a, SAC#01b (B12: Short Term DCB)
SO 003	WOC shall submit iRMT in full consistency with the validated trajectory	UC1-a10	As above	SAC#01a, SAC#01b (B12: Short Term DCB) SAC#05a, SAC#05b (B10-B11: Traffic Planning & Synchronization)
SO 004	Regional ATFCM shall distribute the iSMT to Sub-regional/local ATFCM and ENR/APP ATS and update demand forecast accordingly	UC1-a6 UC1-a8	ASM#1: Adjust the Capacity (to the extent where it is available) to fit the predicted Demand Balance the predicted Demand against the available Capacity	SAC#01a, SAC#01b (B12: Short Term DCB)
SO 005	Sub-regional/local ATFCM shall receive iSMT and integrate it in the local impact assessment in view of appropriate Capacity adjustment and Demand balancing	UC1-a7	As above	SAC#01a, SAC#01b (B12: Short Term DCB)
...	...	...	...	...

Guidance G On setting Safety Objectives (failure approach)

G.1 Introduction

This guidance is about setting **safety objectives (failure-approach)** in terms of an operational hazard's maximum tolerable frequency of occurrence/probability, derived from the severity of its effect. This is based on the usage of Hazard Severity Classification and Risk Classification Schemes (RCS). A Risk Classification Scheme (RCS) is based on:

- an assessment of the effects a hazard may have on the safety of aircraft, as well as an assessment of the severity of those effects, using the Severity Classification Scheme (SCS) provided, and
- the determination of their tolerability, in terms of the hazard's maximum probability of occurrence, derived from the severity and the maximum probability of the hazard's effects.

However, experience has shown that a potential of misunderstanding by the user as to how this RCS was originally derived can lead to inappropriate use and incorrect Safety Objectives. If RCS are used, it is important that the user understands:

- at what level in the ATM System engineering hierarchy (i.e. hazards not always defined at the operational/service level), and within what scope (e.g. phase of flight), the values are intended to be applied (i.e. the level at which the operational hazards have to be defined);
- where the probability / frequency values used in the scheme came from and whether they are (still) valid (e.g. airport operation-related hazards using schemes with field data from, say, an en-route environment);
- to what operational environment the values apply – e.g. type of airspace, traffic patterns, traffic density, spatial dimension, phase of flight, separation minima etc.; and
- how the aggregate risk can be deduced from analysis of individual hazards, in restricted segments of the total system.

The Accident Incident Model (AIM) includes a set of incidents of different severities, which are precursors¹⁰ of each accident category¹¹. As such, AIM models contain built-in SCSs. These can be used to derive quantitative targets for such severities. The use of a common accident precursor based RCS (derived from AIM) would solve many of the underlying problems (mentioned above) existing in current RCS approaches when applied to a program as wide reaching as SESAR. Namely it would provide a common template across a wide range of projects based directly on accident modelling. In more details, AIM-based RCSs offer a number of advantages over many risk-classification schemes as follows:

- they are based on real, historical accident and incident data;
- they can provide valid safety targets at many levels in the ATM system hierarchy and for specific phases of flight; and

¹⁰ A precursor is an occurrence that remained an incident but that might recur in different conditions and become an accident (Skybrary).

¹¹ More information is available in Guidance I and in [references to AIM model from 16.1.1].

- they can provide safety targets that take account of future changes to the ATM system and / operational environment, rather than being tied to the past / current situation.

AIM-Based RCSs are determined on the basis of a risk based approach as they are based on the conditioned probabilities / effectiveness already contained in AIM.

The process for setting Safety Objectives (failure approach) based on these RCSs is described in the following sections below.

G.2 Process for Setting Safety Objectives (failure approach)

The following steps apply for setting safety objectives for the failure approach using an accident precursor based Risk Classification Scheme:

1. Identification of Operational Hazards (see detail in **G.2.1**).
2. Determine the relevant Severity Class of the operational hazards (see detail **G.2.2**)
3. Calculate the corresponding Safety Objective (see detail **G.2.3**)

Two examples of how to apply this process are presented in section **G.2.4**.

G.2.1 Operational Hazards identification

The Operational Hazards, as per SRM definition (section 10.3), shall be defined at the operational level (level of the operational services i.e. a level that is independent of the system design) and describe the failure of operational services. Note that we refer here to “system-generated” hazards, which result from failure of the ATM/ANS functional system affected by the Change brought in by the Solution (and not to “pre-existing hazards”).

An initial way for identifying these operational hazards is based on the analysis of the corresponding operational services (ref to assurance activity) and by considering, for each safety objective from the success approach (ref to assurance activity), what would happen if the objectives were not satisfied (i.e. negate the safety objectives derived with the success approach),

Then, this list of operational hazards is to be completed / updated using standard methods (e.g. HAZOP, HAZID, SWIFT (Structured What-If Technique) etc.) as per SAM FHA, mainly through a dedicated FHA workshop. It has to be noted that those methods may require additional “compilation” in order to define the hazards at the appropriate operational service level as mentioned above. Alternatively, the Operational Hazard Assessment (OHA) process from ED-78A may also be adapted for the purpose.

The standard questions related to the HAZOP/HAZID/etc. processes at a FHA workshop should be enriched considering the following principles from Resilience Engineering (**Guidance J**):

- Work-as-done (Resilience Principle # 1).
- Margins and adaptive capacity (Resilience Principle # 5)
- Coupling and interactions cascading (Resilience Principle # 6)

In order to optimise resources and time, the FHA workshop should be organised jointly with HP experts. Thus, questions from the HP Issue Analysis are considered (see **Guidance L**).

G.2.2 Determination of the corresponding severity class

Once the operational hazards are identified, the next step is to assess their operational effects by determining the impact of each of them in the relevant AIM model. Potential causes of the assessed operational hazard affecting several barriers at the same time are to be taken into account for determining the operational consequence of that hazard.

The Severity Class (SC) for an operational hazard is then determined based on the last barrier negatively impacted by the corresponding hazard (taking into account potential common causes as mentioned above), i.e. stopping at the level of the precursor for which the subsequent non-impacted barrier will work nominally. The SC is to be determined as per the Severity Classification Scheme(s) from Guidance **G.3**.

If an operational hazard impacts several barriers or several accident models (such as MAC & CFIT for example) then safety objectives should be calculated as defined in Guidance **G.2.3** below and the most demanding objectives should be retained.

Using AIM supports consistency by choosing the consequences for an operational hazard and, consecutively, the associated severity class. However, despite the use of the models, this process still needs operational experts in the determination of effects and severity classes, as in the identification of operational hazards (see **G.2.1**). Operational experts are then to be involved in this assessment (preferably during the FHA/OHA workshop).

G.2.3 Quantitative definitions for the safety objectives

G.2.3.1 Presentation of the Method

Safety Objectives (according to the failure approach) limit the frequency of occurrence or probability on demand of the operational hazards such as to keep risks in line with the Safety Criteria (SAC).

Safety Objectives are calculated based on the severity of the impact of the operational hazard (as explained in Guidance **G.2.2**) and the corresponding maximum tolerable frequency of occurrence for this severity class as defined in the Risk Classification Schemes presented in Guidance **G.4**.

Before indicating how to calculate safety objectives, it is worth noting that:

1. The entire “risk budget” for operational hazards at a certain level has to be distributed amongst all the operational hazards that affect the barrier. It is therefore necessary to divide the overall risk budget by the number of operational hazards (N) affecting a barrier (i.e. belonging to the same severity class). This requires an estimate of the maximum number of operational hazards (these numbers are derived in **G.2.3.3** below).
2. The impact of an operational hazard can be a single conflict (e.g. Failure to prevent a planned conflict becoming a tactical conflict) or it can have an impact on several aircraft or even on all those in a sector or in an entire operation. Conversely, it can even affect one single aircraft (e.g. in case of CFIT). Ideally, the safety objective even takes this into account and therefore an Impact Modification factor (IM) is employed. Further information in defining the IM to fit special situations is further detailed in the paragraph **G.2.3.2** below.

The result of this is that safety objectives (SO) that are derived using this method are linked to a set of accident models representing the baseline operational risks. The SO directly represent contributions to barrier failures and are consistent with the approach used for Safety Criteria in the SRM.

The method to calculate SO for a given operational hazard is as follows:

$$SO = \frac{MTFoO_{relevant_severity_class}}{N \times IM}$$

where:

- $MTFoO_{relevant_severity_class}$ stands for the Maximum Tolerable Frequency of Occurrence being the maximum probability of the hazard's effect as defined in **Table 6** to **Table 9** in Guidance **G.4**.
- N is the overall number of operational hazards for a given severity class at a given barrier as obtained from **Table 5** below.
- IM is the Impact Modification factor to take account of additional information regarding the operational effect of the hazard, in particular related to the number of aircraft exposed to the operational hazard. See more detail here below.

G.2.3.2 On the Impact Modification Factor (IM)

The way the AIMs have been developed and the Severity Classes have been derived from them do not directly take into account the number of aircraft exposed to an operational hazard. In reality, one might wish to allocate a more stringent Safety Objective to a situation where multiple aircraft are affected, compared to the same situation concerning one or few aircraft. This is accounted for through the calculation of the Safety Objective, i.e. through the outcome frequency / probability on demand affected with a modification factor called Impact Modification factor (IM) related to the number of aircraft exposed to the operational hazard.

As a general rule, in case an operational hazard involves multiple (many aircraft) then an impact of one order of magnitude should be considered i.e. use $IM=10$ (instead of the reference value $IM = 1$ corresponding to the case of one or only few aircraft involved). However, the IM might be more finely estimated based on operational expert judgment.

The IM can also be used to account for cases where the last barrier negatively impacted by the corresponding operational hazard is not completely broken, but its efficiency is only reduced to some extent. A value $IM < 1$ needs to be applied in such cases (instead of the reference value $IM=1$ corresponding to the case where the barrier is completely lost). That value shall be carefully commensurate with the reduction in the efficiency of the safety barrier to be estimated based on operational expert judgment.

Another element that the IM can also account for is the exposure time before the operational hazard detection and subsequent mitigation; the longer the exposure time, the higher the risk is for which a greater IM may be more appropriate.

G.2.3.3 Estimation of the number of operational hazards (N) for each severity class

To generate the safety objectives it is necessary to make an estimation of the total number of contributing operational hazards for each severity class thereby appropriately managing the aggregate risk that is crucial in SESAR.

Currently, this estimation is based on operational judgment and previous experience in safety assessment. Within a given accident type, the number of operational hazards (N) for each severity class depends on the nature of the barriers and the induced events as input to the barriers. As an example, the potential number of operational hazards related to the STCA barrier (within MAC model) is not the same as the ones related to a barrier as Traffic Coordination and Synchronisation that encompasses several ATM system functions in it.

Table 5 provides the current values of N to be used in the calculation of Safety Objectives as per the process explained in section G.2.

	Values in Table 5 might be subject to further updates as the various safety assessments across the work programme are generating additional operational hazards.
---	---

Severity Class	Number of operational hazards per Severity Class per Accident Type				
	MAC (ER&TMA)	RWY Coll.	CFIT	TWY Coll.	WK-FA
SC1	1	1	5	1	1
SC2	n/a	n/a	10	n/a	n/a
SC2a	5	5	n/a	5	5
SC2b	10	10	n/a	10	5
SC3	25	20	n/a	20	n/a
SC3a	n/a	n/a	50	n/a	5
SC3b	n/a	n/a	50	n/a	5
SC4	n/a	30	n/a	30	5
SC4a	30	n/a	n/a	n/a	n/a
SC4b	100	n/a	n/a	n/a	n/a

Table 5: Maximum Operational Hazard Numbers per Severity Class

G.2.4 Examples of setting Safety Objectives

The examples provided in this section are based on the safety assessment done for two SESAR concepts. Note that as these assessments were performed using previous version of this guidance, they have been updated here taking into account the latest development of the SO setting process and of the Risks Classifications Schemes.

Example on “i4D + CTA” SESAR Concept

More information related to this example is available in [17].

Operational Hazard description

The following operational hazard was identified in the safety assessment done in the frame of SESAR for this concept:

OPERATIONAL HAZARD: Incorrect trajectory synchronization resulting in lateral deviation that induces tactical conflict in current sector

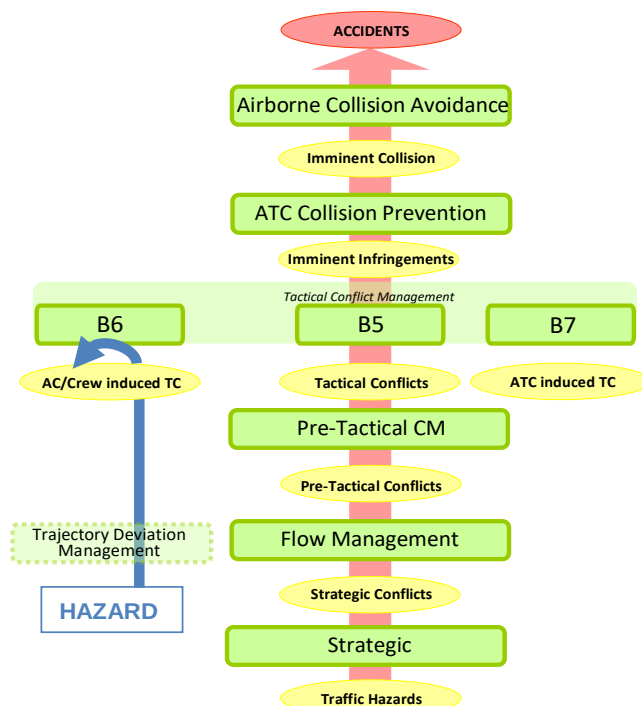
This operational hazard is caused by situations where airborne and ground trajectories are not or wrongly synchronized, not timely mitigated by a consistency check (via next Extended Projected Profile EPP downlink) or by a conformance monitoring tool alert, which involve an aircraft lateral deviation from the trajectory expected by the Executive Controller (ATCO_EXE) with other aircraft in potential conflict in the proximity.

Operational Hazard assessment – Mitigation Means

The assessment of this operational hazard was done using the simplified model of Mid-Air Collision (see section G.3.1 **Figure 8**). Once this operational hazard has occurred, it is expected to be mitigated by the ATCO_EXE detecting the conflict via radar monitoring and undertaking appropriate tactical conflict resolution (B6 barrier which is not impacted).

Operational Hazard within AIM

This operational hazard is the collection of a sub-set of scenarios leading to the pre-cursor MF6.1: Crew / Aircraft induced conflict”. The following scheme positions this operational hazard within the MAC-ER model:



Assigned Severity Class

The operational effect of this hazard is then a situation where an imminent infringement coming from a crew/aircraft induced conflict was prevented by the tactical conflict management.

Consequently the severity allocated is MAC-SC4a as per **Table 6**.

Allocated Safety Objective

The Safety Objective corresponding to this hazard, based on the assessment explained above is then:

SAFETY OBJECTIVE: The likelihood that incorrect trajectory synchronization induces tactical conflict by lateral deviation in current sector shall be no more than $2\text{e-}04$ per sector operational hour.

It has been calculated applying the formula from G.2.3, using the following values:

$\text{MTFoF}_{\text{MAC-SC4a}} = 1\text{E-}03$ [per fh] as per **Table 6**.

$N = 30$ as per **Table 5**

$\text{IM} = 1$ as no particular correction was required related to: (a) number of aircraft affected or (b) exposure time before detection or (c) alteration of probability of last barrier negatively impacted by the hazard.

With these values a SO of $3.3\text{E-}05$ [per fh] is obtained. It can be converted per sector operational hour using the assumption of 6 flight hours controlled per one sector operational hour:

$\text{SO} = 3.3\text{E-}05 * 6 = 2\text{E-}04$ [per sector operational hour]

Example on “Remote Tower” SESAR concept

More information related to this example is available in [SAR for Single Remote Tower – 00.01.01 March 2014].

Operational Hazard description

The following operational hazard was identified during the safety assessment of Remote Tower for a Single Aerodrome:

OPERATIONAL HAZARD: Remote ATC incorrectly manage runway crossing for a vehicle or an aircraft

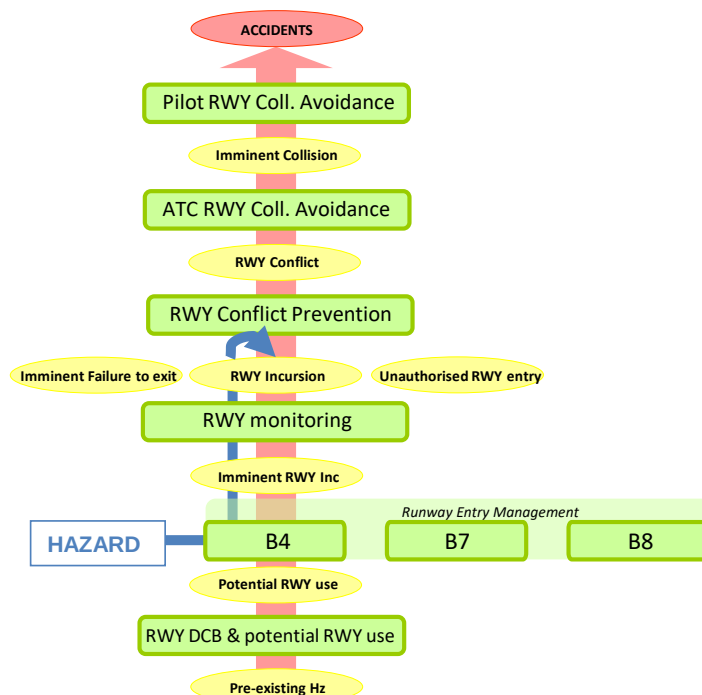
This operational hazard is related to a failure of the service “ATC runway entry management” (modelled by Barrier 4 in the Runway Collision model). It addresses the fact that ATC provides inappropriate instructions to a vehicle or an aircraft resulting in a potential runway incursion.

Operational Hazard assessment – Mitigation Means

The assessment of the operational hazard was done using the simplified model for Runway Collision (see section G.3.2). While B4 is the last barrier negatively impacted by the hazard, it was considered during the assessment workshop that the subsequent Runway Monitoring barrier was not efficient enough to prevent a potential runway incursion as a result of this specific operational hazard (since induced by ATC). As the runway could be already occupied / used for another operation when the hazard occurs, the failure of the Runway Monitoring barrier could then lead to a potential conflict on the runway. In that case, the “ATC collision prevention” barrier will most likely detect and solve the conflict.

Positioning the Operational Hazard within AIM

This operational hazard is the collection of a sub-set of scenarios leading to the pre-cursor RP3: Runway Incursion. The following scheme positions this operational hazard within the Runway Collision model:



Severity Class Assignment

The result of the assessment was that the operational hazard can lead to a situation where an encounter between a vehicle or an aircraft on the runway and another aircraft approaching occurs but ATC runway Collision avoidance prevents it to become an Imminent Runway Collision.

Thus the allocated severity class is RWY-SC3 (Runway Incursion) as per RCS in **Table 7**.

Allocated Safety Objective

The safety objective corresponding to this hazard, based on the assessment explained above is then:

SAFETY OBJECTIVE: The likelihood that Remote ATC incorrectly manage runway crossing for a vehicle or an aircraft shall be no more than $5e-7$ per movement.

It has been calculated applying the formula in G.2.3, using the following values:

$MTFoF_{RWY-SC3} = 1e-5$ as per **Table 7**

$N = 20$ as per **Table 5**

$IM = 1$ as no particular correction was required related to: (a) number of aircraft affected or (b) exposure time before detection or (c) alteration of probability of last barrier negatively impacted by the hazard).

G.3 Severity Classification Schemes

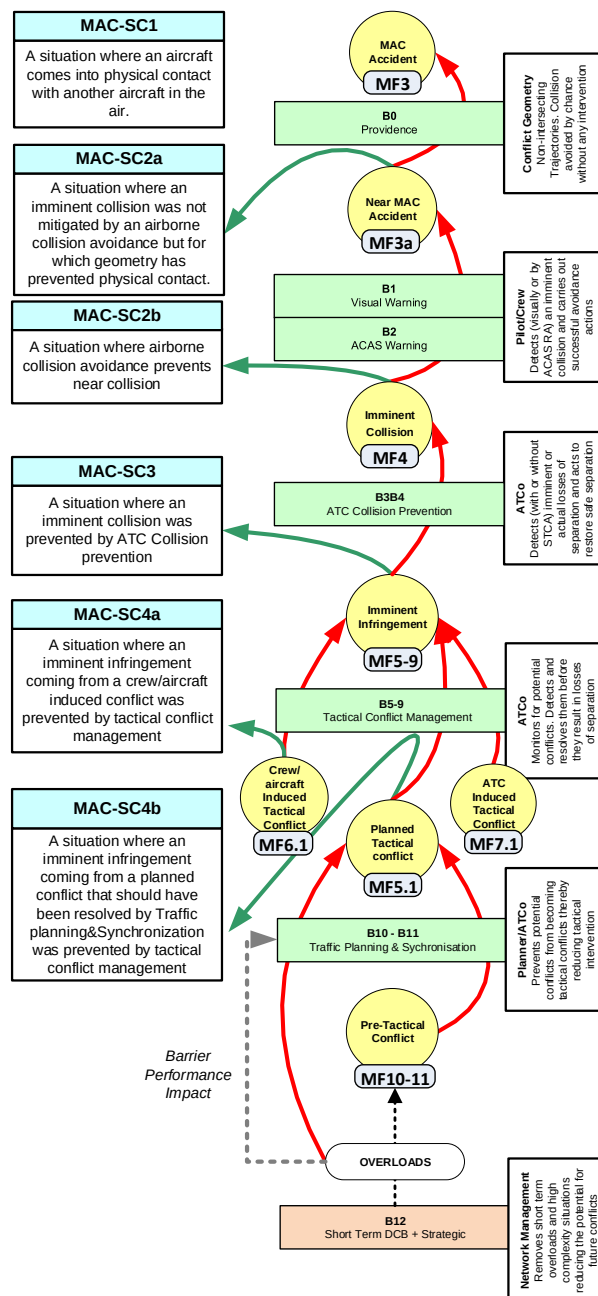
Diagrams in Guidance **G.3.1** to **G.3.6** show the Severity Classification Schemes (SCS) for the following accident types covered by the available AIM accident models:

- SCS for Models that are part of the AIM release 2017 **[2]** (as described in Guidance I):
 - MAC accident (version v1.0A) –for TMA and ER operations
 - Runway Collision (version v1.0)
 - Controlled Flight Into Terrain (version v1.0)
 - Taxiway Collision (version v1.0)
 - Wake Induced accident on final approach (version v2.0)

- SCS for models planned to be included in future AIM releases:
 - Runway Excursion (version v0.3) – only relating to landing operations

The above list might be enriched in case new AIM models will be developed (as an example, an AIM for Wake induced accident on initial departure and an AIM for MAC accident on final approach are close to finalization).

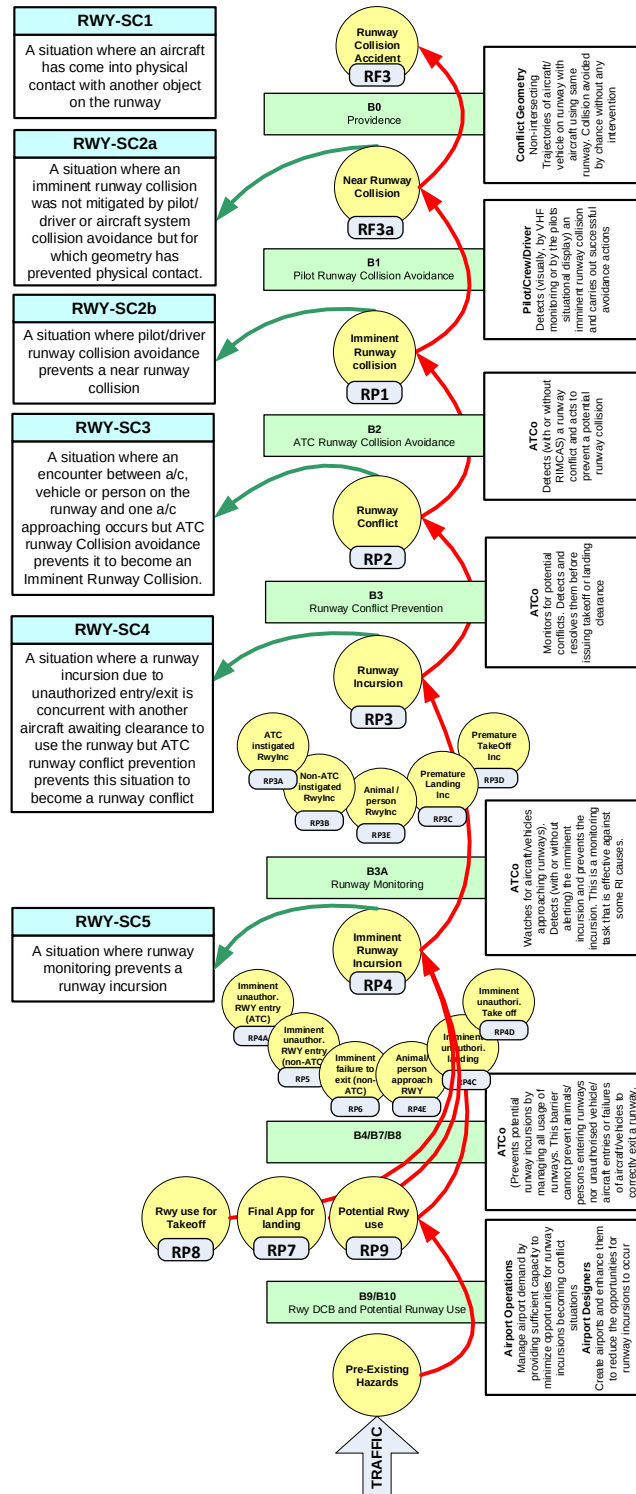
G.3.1 Severity Classification Scheme for MAC accident model



Severity Class Scheme for Mid-air Collision

Figure 8: Severity Classifications for the MAC model (ER and TMA)

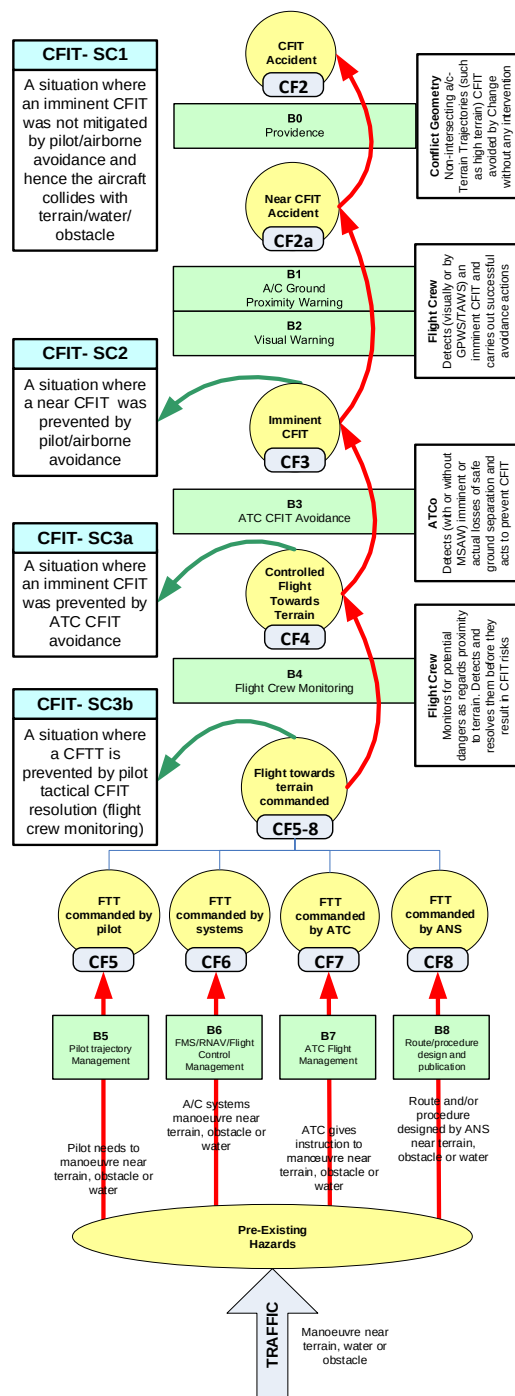
G.3.2 Severity Classification Scheme for Runway Collision model



Severity Class Scheme for Runway Collision
AIM-2017 RWY Col BARRIER MODEL v1.0

Figure 9: Severity Classifications for the RWY Collision accident model

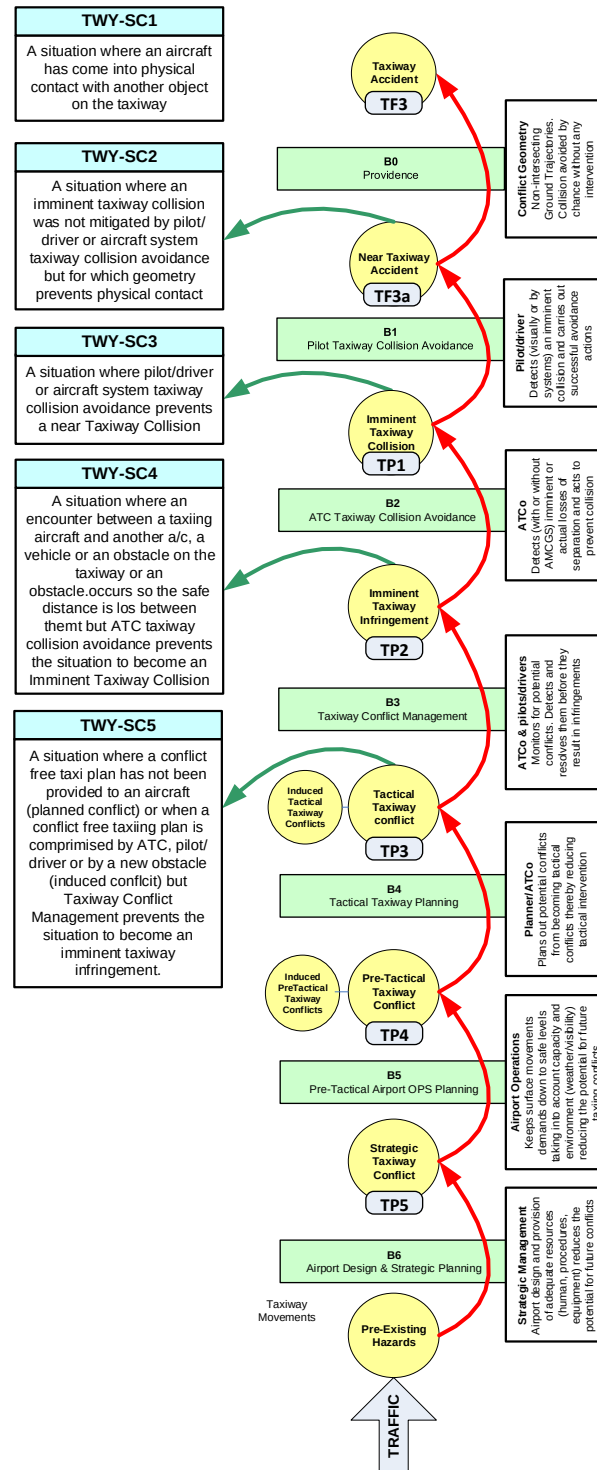
G.3.3 Severity Classification Scheme for CFIT accident model



Severity Class Scheme for CFIT
AIM-2017 CFIT BARRIER MODEL v1.0

Figure 10: Severity Classification Scheme for the CFIT accident model

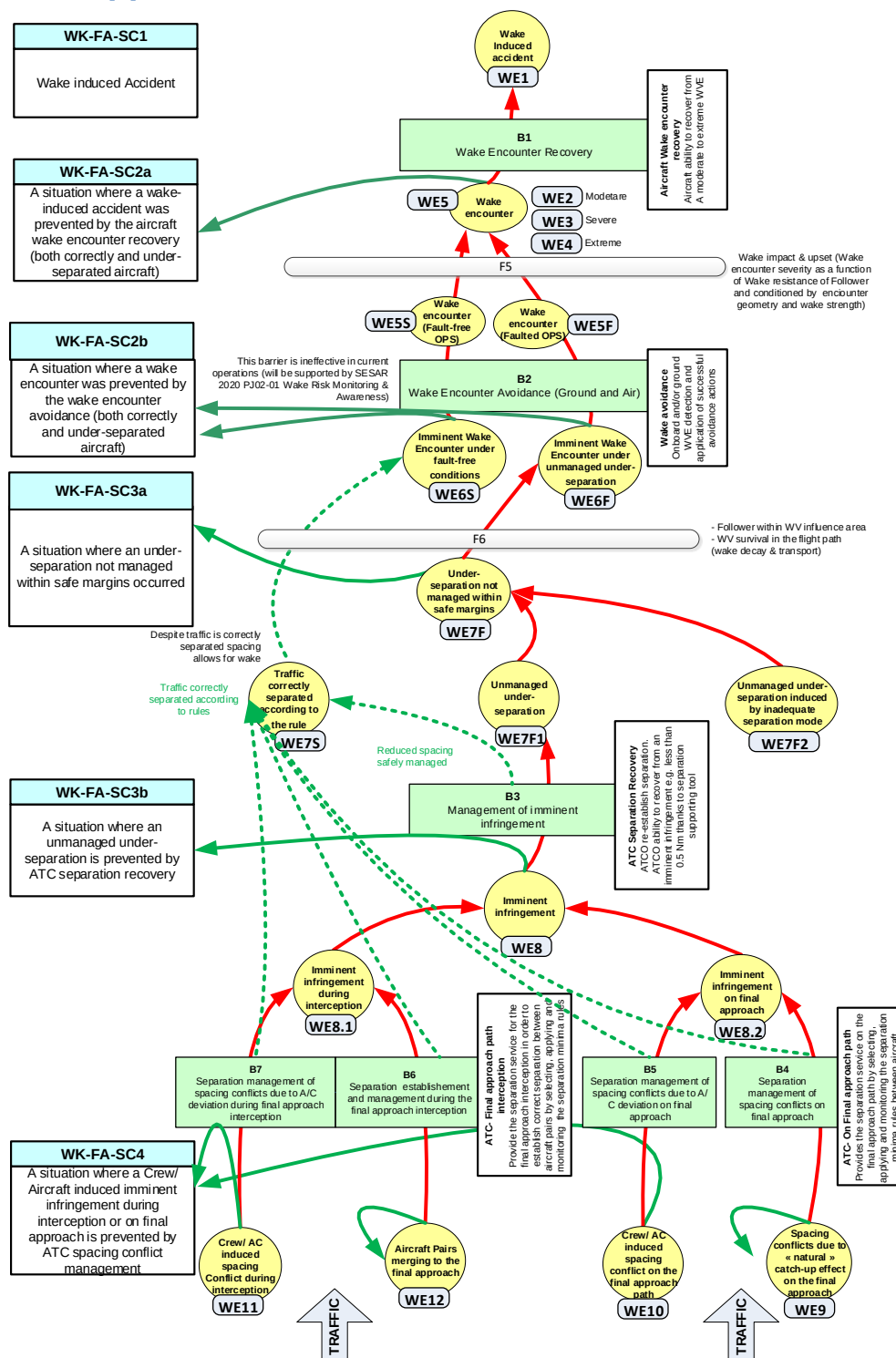
G.3.4 Severity Classification Scheme for Taxiway accident model



Severity Class Scheme for Taxiway Collision
AIM-2017 TWYCoI BARRIER MODEL v1.0

Figure 11: Severity Classifications for the Taxiway Collision accident model

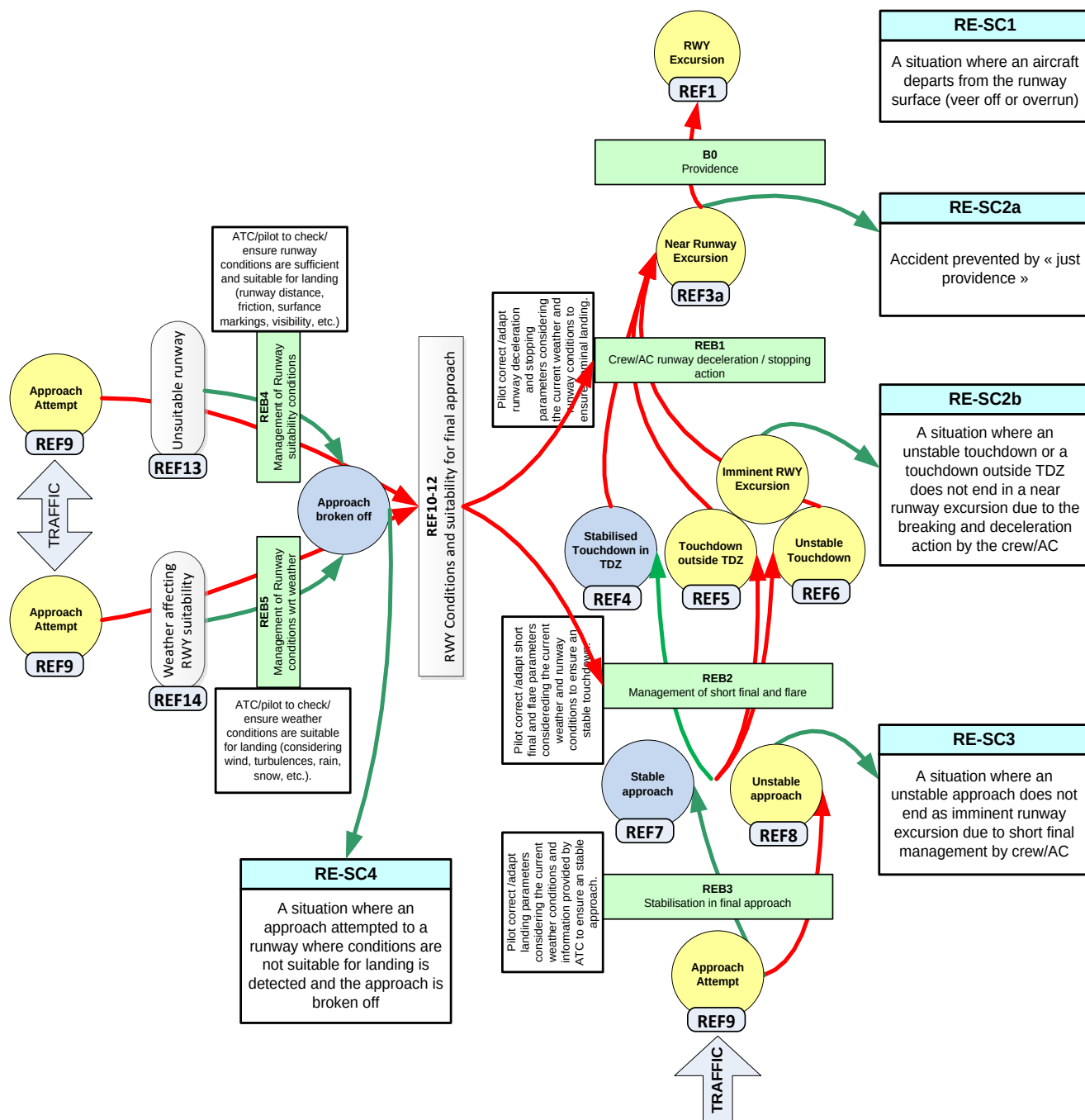
G.3.5 Severity Classification Scheme for Wake Induced accident on Final Approach model



Severity Class Scheme for final approach Wake Induced Accident
AIM WAKE BARRIER MODEL (Final Approach) v2.0

Figure 12: Severity Classifications for the Wake Induced accident on Final Approach model

G.3.6 Severity Classification Scheme for Runway Excursion model



Severity Class Scheme for Runway Excursion (related to landing only)
AIM RWY EXC BARRIER MODEL (Landing) v0.3

Figure 13: Severity Classifications for the Runway Excursion model

G.4 AIM-based Risk Classification Schemes

This section provides Risk Classification Schemes for the different accident types covered by the AIM accident models that are quantified. They provide a barrier based risk classification with a decreasing “risk distance” as we approach the accident. In these schemes, a Severity Class is associated with a tolerable frequency of occurrence (*i.e.* a maximum tolerable frequency of occurrence of ATM contributing to safety occurrences); the more severe the effect of the hazard the less frequent the hazard shall occur.

The definition of “ATM contribution” includes accidents with causes that either are part of the ATM system (whether ground-based, space-based or airborne) or that ATM could reasonably have been expected to mitigate. In the present study, this means that any accident in the modelled categories would inevitably include an ATM involvement. Tables presented in Guidance **G.4.1** to **G.4.5** below include definitions for the hazardous situations. Cross-references to accident precursors in **Figure 8** to **Figure 12** above are made in the column ‘Operational Effect’. The Maximum Tolerable Frequency of occurrence (MTFoO) is expressed per flight hour (fh) or per flight (flt) /movement (mov) depending on the type of accident. The numbers in the RCSs for the different models are related to quantitative values contained in the relevant AIM models at precursors, barrier efficiencies and criteria levels for which (in particular, but not limited to) the AIM Validation / Verification report [7] mentioned earlier provides full information.

	Compared to the AIM probabilistic values for precursors, the figures in Table 6 to Table 10 below have been rounded to 10^{-x} granularity in order to facilitate their usage in practical applications. The impact of this rounding on the derived Safety Objectives and subsequently on the allocated Safety Requirements is negligible. The rounding to 10^{-x} enables¹² to render transparent both the evolutions in traffic as per SESAR as well as the foreseen impacts of the various Solutions. As a consequence, the same RCS can be used unchanged for SESAR 1 and SESAR 2020, irrespective of the traffic increase (as per SESAR Target) and foreseen ATM system changes (Solutions).
	Values in G.4.1 to G.4.5 below could be refined as the result of ongoing activities related to the risk models to enrich the dataset used by AIM. This approach is currently being validated on a number of pilot projects. As a consequence, it may be subject to further refinements.

The Risk Classification Schemes provided in this guidance are related to the following accident types and models:

- Mid Air Collision in TMA and En-Route (version v1.0A)
- Controlled Flight Into Terrain (version v1.0)

¹² An estimation of the impact of these factors in the overall SESAR was performed in SESAR1 and the conclusion was that the resulting magnitude of the impact is commensurate with the magnitude involved by the rounding

- Runway collision (version v1.0)
- Taxiway Collision (version v1.0)
- Wake induced accident on Final Approach (version v2.0)

All these models are part of the AIM release 2017 [2].

The Risk Classification Schemes for other type of accidents will be provided once the corresponding AIM models will be more mature, in terms of quantification.

G.4.1 RCS for MAC in En-route & TMA operational environments

Table 6 shows the maximum tolerable frequency of occurrence for each severity class related to MAC accidents as defined in Guidance **G.3.1**.

Note that due to the rounding of values, the same RCS is to be used for En route and TMA operations.

<i>Severity Class</i>	<i>Hazardous situation</i>	<i>Operational Effect</i>	<i>MTFoO [per fh]</i>
MAC-SC1	A situation where an aircraft comes into physical contact with another aircraft in the air.	Accident - Mid air collision (MF3)	1e-9
MAC-SC2a	A situation where an imminent collision was not mitigated by an airborne collision avoidance but for which geometry has prevented physical contact.	Near Mid Air Collision (MF3a)	1e-6
MAC-SC2b	A situation where airborne collision avoidance prevents near collision	Imminent Collision (MF4)	1e-5
MAC-SC3	A situation where an imminent collision was prevented by ATC Collision prevention	Imminent Infringement (MF5-8)	1e-4
MAC-SC4a	A situation where an imminent infringement coming from a crew/aircraft induced conflict was prevented by tactical conflict management	Tactical Conflict (crew/aircraft induced) (MF6.1)	1e-3
MAC-SC4b	A situation where an imminent infringement coming from a planned conflict was prevented by tactical conflict management	Tactical Conflict (planned) (MF5.1)	1e-2

Table 6: Risk Classification Scheme for Mid Air Collision (TMA and En-Route)

G.4.2 RCS for Runway Collisions

Table 7 shows the maximum tolerable frequency of occurrence for each severity class related to Runway Collision accidents as defined in Guidance **G.3.2**

<i>Severity Class</i>	<i>Hazardous situation</i>	<i>Operational Effect</i>	<i>MTFoO [per movt.]</i>
RWY-SC1	A situation where an aircraft has come into physical contact with another object on the runway	Accident - Runway Collision (RF3)	1e-8
RWY-SC2a	A situation where an imminent runway collision was not mitigated by pilot/driver or aircraft system collision avoidance but for which geometry has prevented physical contact.	Near Runway Collision (RF3a)	1e-7
RWY-SC2b	A situation where pilot/driver runway collision avoidance prevents a near runway collision	Imminent runway collision (RP1)	1e-6
RWY-SC3	A situation where an encounter between a/c, vehicle or person on the runway and one a/c approaching occurs but ATC runway Collision avoidance prevents it to become an Imminent Runway Collision.	Runway Conflict (RP2)	1e-5
RWY-SC4	A situation where a runway incursion due to unauthorized entry/exit is concurrent with another aircraft awaiting clearance to use the runway but ATC runway conflict prevention prevents this situation to become a runway conflict	Runway incursion (RP3)	1e-4
RWY-SC5	A situation where runway monitoring prevents a runway incursion	Imminent Runway incursion (RP4)	1e-2*

Table 7: Risk Classification Scheme for Runway Collision related to Incursions

*Note that the MTFoO values for severity RWY-SC5 has been increased from 1e-4 to 1e-2. This is because the increased value makes more sense operationally in the context where the currently available data are not sufficiently statistically relevant.

G.4.3 RCS for Controlled Flight Into Terrain

Table 8 shows the maximum tolerable frequency of occurrence for each severity class related to Controlled Flight Into Terrain as defined in Guidance **G.3.3**.

<i>Severity Class</i>	<i>Hazardous situation</i>	<i>Operational Effect</i>	<i>MTFoO [per flgt]</i>
CFIT-SC1	A situation where an imminent CFIT is not mitigated by pilot/airborne avoidance and hence the aircraft collides with terrain/water/ obstacle [note 1 below]	CFIT Accident (CF2) Near CFIT (CF2a)	1e-8
CFIT-SC2	A situation where a near CFIT is prevented by pilot/airborne avoidance	Imminent CFIT (CF3)	1e-6
CFIT-SC3a	A situation where an imminent CFIT is prevented by ATC CFIT avoidance	Controlled flight towards terrain (CF4)	1e-5
CFIT-SC3b	A situation where a controlled flight towards terrain is prevented by pilot tactical CFIT resolution (flight crew monitoring)	Flight towards terrain commanded (CF5-8)	1e-5

Table 8: Risk Classification Scheme for CFIT

Note 1: In the CFIT model, a favourable aircraft trajectory geometry is not considered to be credible to prevent the collision with terrain/water/ obstacle following a near CFIT. Thus Near CFIT is classified together with the CFIT accident (severity class CFIT-SC1).

Note that the MTFoO values for severity CFIT-SC3a and CFIT-SC3b are the same. This is due to the relatively weak performance of the barrier between these two events, and the fact that figures from the AIM model have been rounded.

G.4.4 RCS for Taxiway Collisions

Table 9 shows the maximum tolerable frequency of occurrence for each severity class related to Taxiway Collision accidents as defined in Guidance **G.3.4**.

<i>Severity Class</i>	<i>Hazardous situation</i>	<i>Operational Effect</i>	<i>MTFoO [per movt.]</i>
TInc-SC1	A situation where an aircraft has come into physical contact with another object on the taxiway	Accident -Taxiway Collision (TF3)	1 e-7
TInc-SC2	A situation where an imminent taxiway collision was not mitigated by pilot/driver or aircraft system taxiway collision avoidance but for which geometry prevents physical contact.	Near Taxiway Collision TF3a	1 e-6
TInc-SC3	A situation where pilot/driver or aircraft system taxiway collision avoidance prevents a near Taxiway Collision	Imminent Taxiway Collision TP1	1 e-2
TInc-SC4	A situation where an encounter between a taxiing aircraft and another a/c, a vehicle or an obstacle on the taxiway or an obstacle occurs so the safe distance is lost between them but ATC taxiway collision avoidance prevents the situation to become an Imminent Taxiway Collision	Imminent Taxiway infringement TP2	1e-1
TInc-SC5	A situation where a conflict free taxi plan has not been provided to an aircraft (planned conflict) or when a conflict free taxiing plan is compromised by ATC, pilot/driver or by a new obstacle (induced conflict) but Taxiway Conflict Management prevents the situation to become an imminent taxiway infringement.	Tactical Taxiway conflict TP3	1

Table 9: Risk Classification Scheme for Taxiway Collision

G.4.5 RCS for Wake induced accident on Final Approach

Table 10 shows the maximum tolerable frequency of occurrence for each severity class related to Wake induced accident on Final Approach as defined in Guidance **G.3.5**

<i>Severity Class</i>	<i>Hazardous situation</i>	<i>Operational Effect</i>	<i>MTFoO (per approach)</i>
Wake-SC1	Aircraft accident following an encountered wake turbulence which led to a fatal structural failure, a collision with the ground or a collision with other aircraft in the air	Wake Induced Accident (WE1)	2E-08
WK-FA-SC2a	A situation where a wake-induced accident was prevented by the aircraft wake encounter recovery (both correctly and under-separated aircraft)	Wake Encounter (WE5 i.e. WE2/3/4)	1E-05
WK-FA-SC2b	A situation where a wake encounter was prevented by the wake encounter avoidance (both correctly and under-separated aircraft) ¹³	Imminent wake encounter (WE6S, WE6F)	1E-05
WK-FA-SC3a	A situation where an under-separation not managed within safe margins occurred	Under- separation not managed within safe margins (WE7F)	2E-04
WK-FA-SC3b	A situation where an unmanaged underseparation is prevented by ATC separation recovery	Imminent Infringement (WE 8)	1E-02
WK-FA-SC4	A situation where a Crew/aircraft induced imminent infringement during interception or on the Final Approach path was prevented by ATC spacing conflict management	Crew/Aircraft Induced spacing Conflict during Interception (WE11) or on Final Approach (WE10)	1,00E-01

Table 10. Risk Classification Scheme for Wake induced accident on Final Approach

¹³ This barrier is ineffective in current operations (will be supported by SESAR 2020 PJ02-01 Wake Risk Monitoring & Awareness)

Guidance H On deriving Safety Requirements (success approach)

H.1 Introduction

This guidance is about deriving Safety Requirements (success approach) which are intended to specify the Change involved by the Solution at the design level, in Normal and Abnormal conditions, such as to meet the Safety Objectives (note that the derivation of Safety Requirements for Faulted conditions i.e. the failures generated by the Solution functional system, is covered by SAM [15]).

The Safety Requirements are design characteristics/items of the functional system to ensure that the system operates as specified. Based on the verification/demonstration of these characteristics/items, it could be concluded that the safety objectives, and consequently the safety criteria, are met. Provided each element meets its safety requirements, the system will meet its safety criteria.

The Safety Requirements (success approach) specify formally the functional, performance and interfacing properties of the ATM/ANS functional system design elements that are affected by the Change and which have a safety implication i.e. they are in the category SAFETY (as per the requirement template used in Section 4 of SPR-INTEROP/OSED).

A requirement is designated in the category SAFETY according to the following criteria: in case the requirement were not satisfied, that would affect the efficiency of a safety barrier and/or directly contribute to an induced precursor in the relevant AIM model.

In order to ensure completeness and correctness, the safety requirements derivation process needs to be supported by Engineering Models that, ideally, should be jointly used by both the Project design experts and the Safety experts.

The EATMA formalism provides a powerful set of engineering models at the System and Service layers for supporting the functional system design and the requirements derivation.

Meanwhile, it might be that the Project/Solution design team progressed with the design sufficiently to set requirements in the SPR-INTEROP/OSED (and, function of the Solution maturity, in the TS/IRS), but has not (yet) developed such models at the time where the safety assessment needs to be performed for the initial or refined design. In that case, the Safety practitioners need to use alternative models to be developed by themselves with the support from the Project experts. Such alternative models might be also useful to complement, when necessary, the available EATMA System and Service layer models.

In terms of available EATMA System and Service layer models, the most useful in the Safety Requirements derivation in both V2 and V3 phases is the System Functionality and Flow model (NSV-4 diagram), outlined under sub-section I.3 below.

Note: In case the EATMA System and Service layer models are not yet available or mature, the EATMA Operational activity models (NOV-5, see sub-section I.2) might be also used to initiate the derivation of the Safety Requirements. This is possible because they formalize the Use Cases in terms of activities and entities (nodes) performing them, whilst textual OSED description (section New operating methods) might provide initial design information in terms of main functional system elements that are involved in those activities.

In terms of alternative models to be used to replace the missing EATMA models or to complement them, the current guidance proposes the following:

- Logical model – see sub-section I.4
- Thread Analysis model – see sub-section I.5.

H.2 Process for deriving Safety Requirements (success approach)

The derivation of Safety Requirements (success approach) is driven by the mapping of each Safety Objective (success approach i.e. Functionality and Performance) to the ATM/ANS functional system design elements (technical, human and procedural) whilst focusing on those design elements which are modified or new.

For a given Solution, the first step consists in the identification, for each Safety Objective (success approach), of the ATM/ANS functional system design elements that would concur to the fulfilment of the Safety Objective.

In a second step, Safety Requirements will be derived for the previously identified design elements, aiming at specifying the new or modified functionality or performance. The derived requirements are in the SAFETY category as they concur to the satisfaction of the Safety Objective at their origin.

As a general rule, a design element might be allocated to one or multiple Safety Requirements and a Safety Requirement should not address more than one design element (element as determined by the lowest available level of granularity of the design).

The level of granularity of the design is expected to evolve as the initial design progresses into the refined design, consequently the requirements derivation process will need to follow that refinement (i.e. certain Safety Requirements initially derived in the initial design will need to be further refined as appropriate in the refined design).

The safety requirements derivation process involves the joint participation of the Project design experts and Safety experts. The Project design experts have the necessary operational and technical expertise to allocate requirements to the functional system elements which are new or affected by the change, whilst the Safety experts bring the safety view, in terms of the elements contribution to the fulfilment of the Safety Objective and consequently of the Safety Criteria.

In order to ensure completeness and correctness, the safety requirements derivation process needs to be supported by Engineering Models, ideally to be jointly used by both the Project design experts and the Safety experts (see Guidance I).

H.3 Example of Application

This sub-section provides an example of derivation of safety requirements (success approach) under Normal conditions taken from the design of the Point Merge (PM) system operations. The example makes use of the Logical Model for the TMA ATC functional system instantiated to support PM operations design provided at I.4 complemented with more detailed information not included here (regarding the step by step description of the Point Merge operation (Use Case description) and the TMA ATCOs and Flight Crew tasks impacted by the Point Merge (PM) introduction).

The following Safety Objective (success), that has been allocated within the PM design at operational level, is considered:

SO#5 (Appropriately timed “Direct To” instruction): An aircraft shall not be turned off the Sequencing Leg towards the Merge Point until it is spaced behind the previous aircraft (in the final sequence) sufficiently to ensure that at least minimum longitudinal separation will be established well before vertical / lateral separation minima are infringed as a consequence of flow convergence.

The process starts by identifying which are the elements of the PM functional system that are involved in the realisation of this SO. These elements, highlighted with RED rectangles in the PM Logical model (shown at Figure 14) are:

- EXCs - Executive ATCOs (ITM and FIN DIR)
- SDP(G)- Surveillance Data Processing- ground (i.e. surveillance information displayed to ATCO)
- FDP - Flight plan Data Processing system (i.e. FPL information presented to ATCO)
- FCRW - Flight Crew
- FMS - Flight Management System

Logical Model
Task Analysis



Derive SR (success) by specifying data flow & interactions
to support each SO (success)

SO#5: Appropriately timed "Direct To" instruction i.e. An aircraft shall be turned off the Seq Leg towards the Merge Point only when it is spaced behind the previous aircraft (in the final sequence) sufficiently to ensure that at least minimum longitudinal separation will be established well before vertical / lateral separation minima are infringed as a consequence of flow convergence

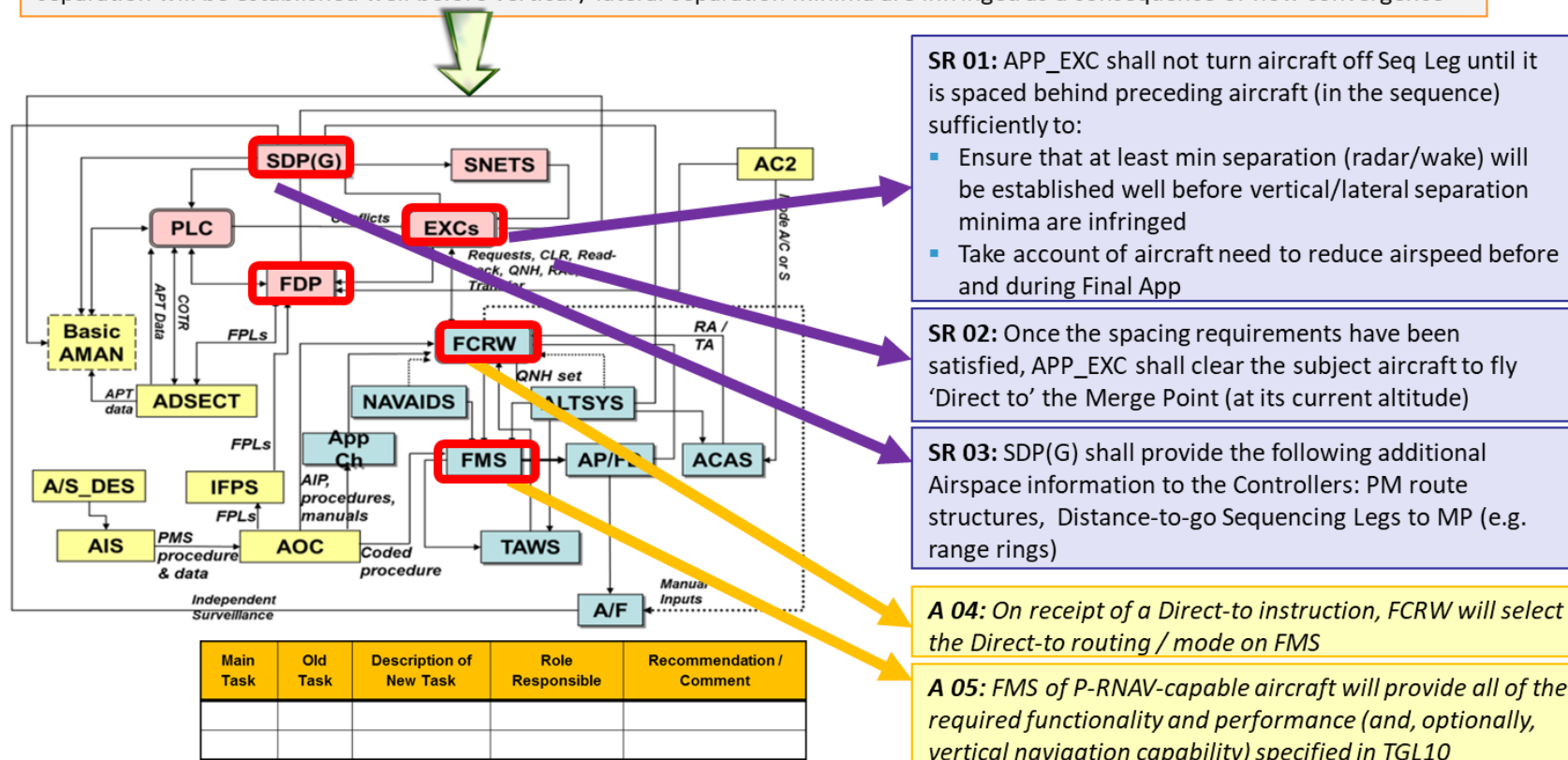


Figure 14. Illustration of Safety Requirements (success) derivation – extracted from Point Merge design

Founding Members



© – 2018 – EUROCONTROL 90

All rights reserved. Licensed to the SESAR Joint Undertaking under conditions.

Then the way each identified element contributes to the SO needs to be understood, making use of any design information made available by the Project team (complemented by information from the Task analysis performed by the HP assessment team, where available). Only the new aspects introduced by the change will make the object of the derivation of the following safety requirements (highlighted with MAGENTA arrows in Figure 14):

- SR 01: regarding spacing requirements for the aircraft to be turned off the Sequencing Leg direct to the Merge Point behind the preceding aircraft;
- SR 02: regarding the executive controller (EXC ATCO) clearance for Direct To Merge Point
- SR 03: regarding the additional airspace information to be presented to EXC ATCOs

The system elements contributions to the SO which are as per the Baseline (i.e. not affected by the change) are only recalled as Assumptions (highlighted with ORANGE arrows in Figure 14):

- A 04: regarding FCRW selection of Direct To routing on FMS
- A 05: regarding the aircraft adequate lateral navigation capability (P-RNAV).

Guidance I On system-engineering models

I.1 Accident Incident Model

The Accident Incident Model - AIM, as shown in Figure 15 below, is a set of accident risk barrier models for a set of accident types (listed below) based upon ECAC incident data and developed based on operational experts input (information related to the quantification of the models as well as the source of data is detailed in [7]).

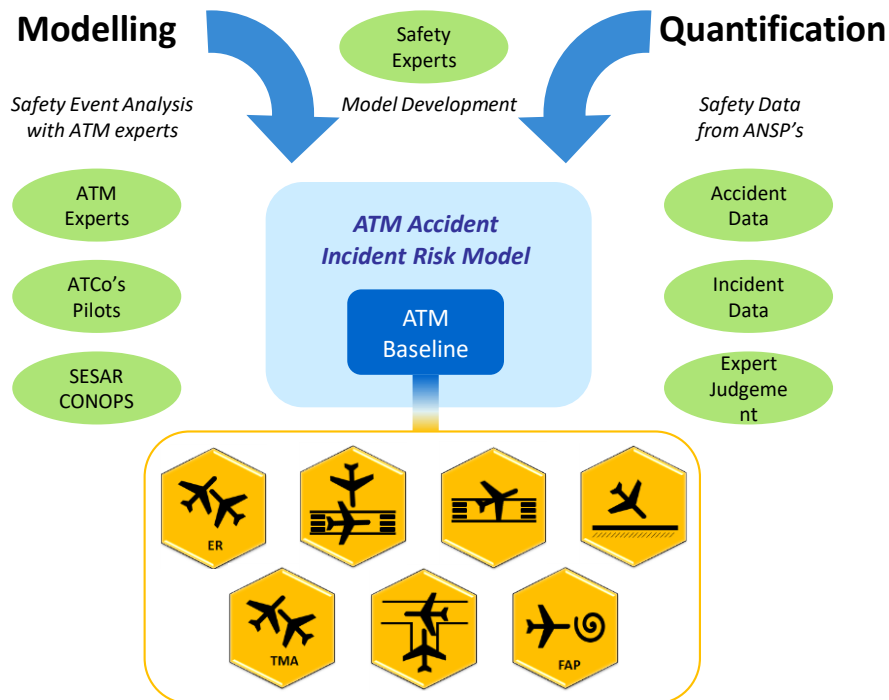


Figure 15: AIM, helicopter view

The latest release of AIM, AIM 2017 [2], includes the following models:

- Mid-Air Collision on en-route (version v1.0A) – MAC-ER
- Mid Air Collision on terminal area (version v1.0A) – MAC-TMA
- Runway Collision (version v1.0) – RWY Col
- Taxiway Collision (version v1.0) – TWY Col
- Controlled Flight Into Terrain (version v1.0) – CFIT
- Wake Induced Accidents on final approach (version v2.0) – WAKE FAP

Apart from the models included in the AIM release, other models are also available or close to finalization (only the qualitative version for the moment) addressing some other risks:

- Runway Excursion (version v0.3) – RWY EXC
- Wake Induced Accidents on Initial Departures (version v0.3) – WAKE ID
- Mid-Air Collision on final approach (version v0.2a) – MAC-FAP
- MAC in Oceanic environment (version v0.2) – MAC-OC

All those models, in their complete and simplified versions, as well as corresponding glossaries for some of them, are available on the SESAR platform STELLAR [3].

The AIM risk models are barrier based and their main elements are shown in next Figure:

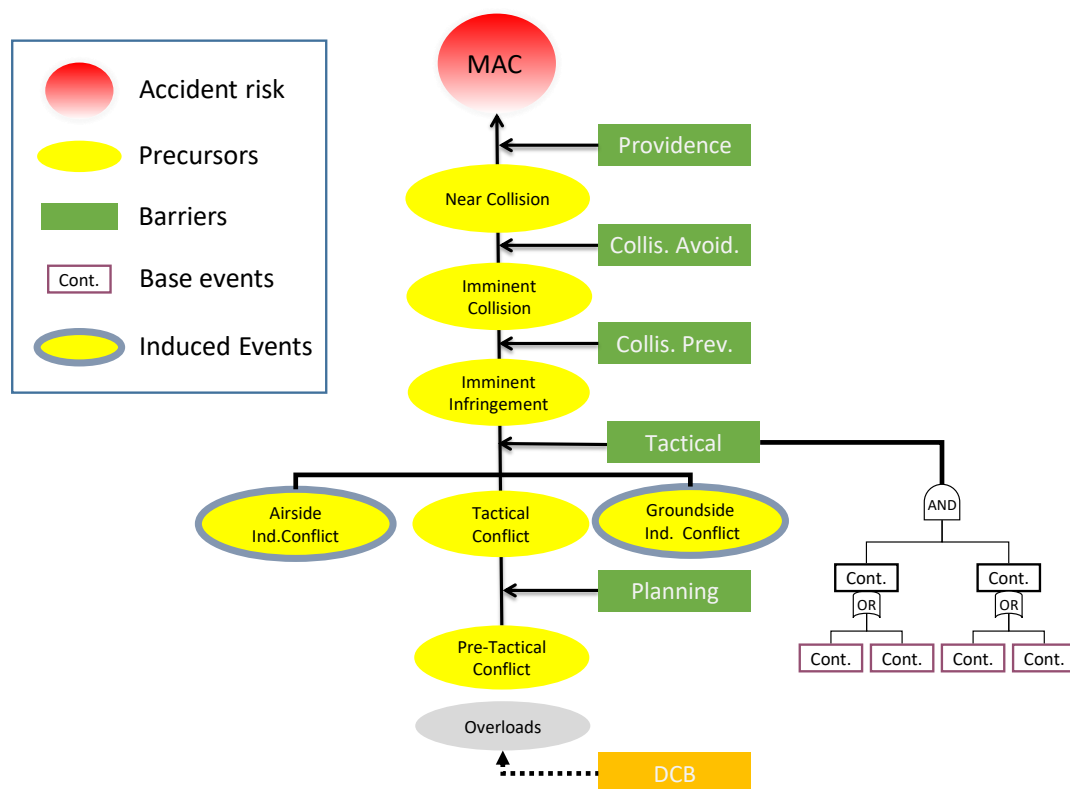


Figure 16: Main elements of the AIM barrier models illustrated with Mid-Air Collision

The models have been reviewed and refined by many ANSPs and represent a 2012 baseline that describes ATM risks to be used for SESAR 2020. The underlying structure of the AIM is also adapted to represent the SESAR ConOps, while ensuring that a similar structure can be used for both generic (the SESAR 2020 baseline is 2012) and predictive (setting of the SACs for SESAR 2020 solutions) modes.

The “Validation / Verification of the SESAR Accident Incident Model (AIM)” report summarizes the qualitative and quantitative validation / verification for the SESAR Accident Incident Model (AIM). The document is divided into two sections, the first describing the activities of qualitative validation and the second describing the quantitative validation [7].

USES of AIM within the SRM: As explained in Guidance D, the barrier model AIM – Accident Incident Model, is a mean to define the Safety Criteria for a Solution. AIM can also be used to support the identification of the Operational services related to a specific change as explained in Guidance E. AIM

has been used to set up the Severity Classification Schemes (SCS) and Risk Classification Schemes (RCS) as per G.2.

I.2 EATMA Operational Activity Model (diagram NOV 5)

The EATMA Operational activity models are process models used to describe operational scenarios/use cases (could be produced per phase of flight if practical). They are hosted by the EATMA Operational layer, which contains the elements needed to describe the operational concepts. This includes process models and descriptions of how ATM actors collaborate.

The EATMA Operational activity models are based on the BPMN formalism (Business Process Model Notation) which makes use of the following elements (illustrated at Figure 17):

- Node (EATMA pictogram: ) ,
- Activity (EATMA pictogram: ) ,
- Information Exchange (EATMA pictogram: ) ,
- Information Element (EATMA pictogram: ) .

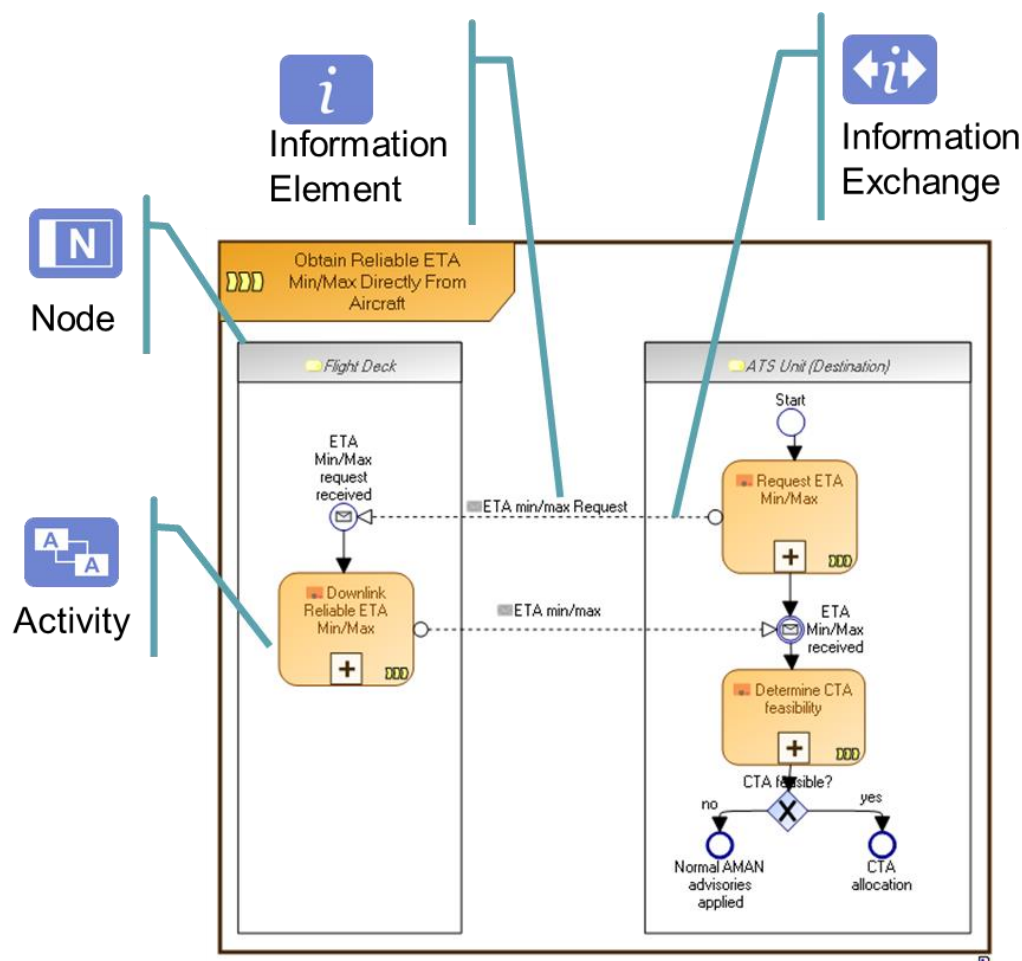


Figure 17: Elements of an EATMA Operational activity model (diagram NOV-5)

The EATMA Operational activity model is a high-level behavioural representation of the ATM/ANS functional system operation that describes what Activities are performed by each Node (entity involved in the operations), the process in which these Activities are involved (i.e. the logic of their interactions) and the data that is produced, used and exchanged by those Activities. It does not show who performs the Activities (the elements of the ATM/ANS functional system design – people, procedures, equipment).

Next Figure 18 illustrates the Operational activity model (NOV-5) produced by PJ07-03 for the Use Case “Mission Trajectory (MT) Management in Short Term Planning”. Note that the nodes are represented via horizontal rows (e.g. En Route/Approach ATS, Sub-regional/Local ATFCM, Regional ATFCM, WOC, MET provider).

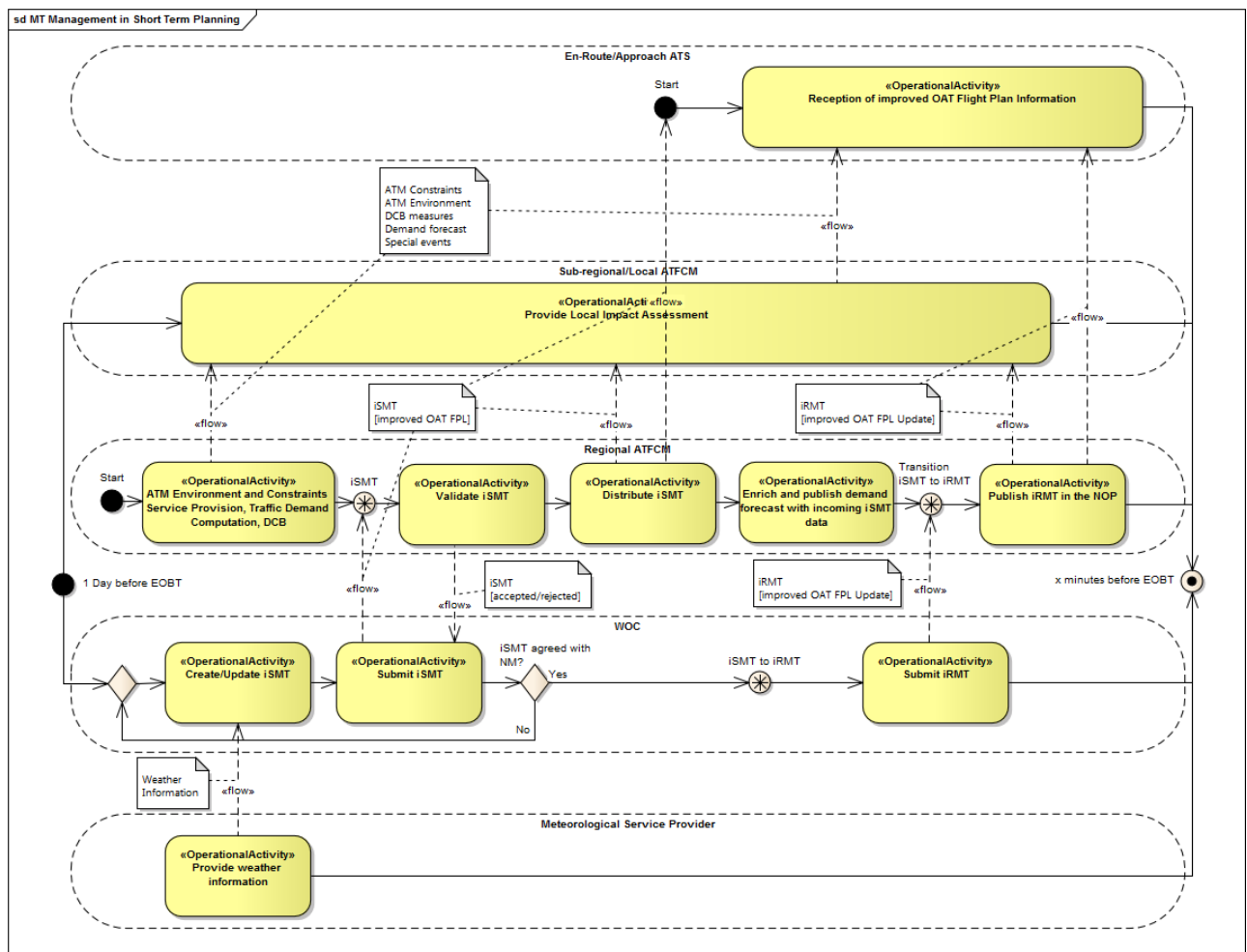


Figure 18: Operational activity model (NOV-5) for PJ07-03 Use Case “Mission Trajectory (MT) Management in Short Term Planning”

USES of EATMA Operational activity model within the SRM: As explained in Guidance F, the EATMA Operational activity Models (diagrams NOV 5), which reflect the OSED Use Cases and their representation as defined by the Project, are an important mean for supporting the definition of the Safety Objectives (success approach).

I.3 EATMA System Functionality and Flow model (NSV-4 diagram)

The EATMA System & Service layers are intended to support progressing of the definition and refinement of the description of the ATM Systems and Services that are part of each Solution and of the changes to those ATM Systems and Services by deriving them from the architectural work. Note that through EATMA the ATM Systems & Services are shared by all SESAR 2020 ATM and Enabling Solutions.

Based on the experience available at the date where this SRM guidance has been written, the EATMA NSV-4 model is currently identified as being the most useful model of the EATMA System & Service

layers for supporting the safety assessment in the initial and refined design phases and more specifically the Safety Requirements derivation within the success approach.

The EATMA System Functionality and Flow diagram NSV-4 (see Figure 19) can be created starting from the NOV-5 diagram (Operational activity model) which, as explained in the previous sub-section, describes the scenarios/use cases (Operational processes) defined for the Solution.

The System Functionality and Flow diagram supports the description of how the resources (human and technical) are contributing to the use case/operational process. The Activities of the operational process are achieved by Functions¹⁴, which are provided by a Capability Configuration, i.e. a combination of Human Roles and technical resources. The latter are represented as either Technical Systems or Functional Blocks. Functional Blocks are logical groupings of functions while Technical Systems represent more physical artefacts. A Technical System can be composed of Functional Blocks.

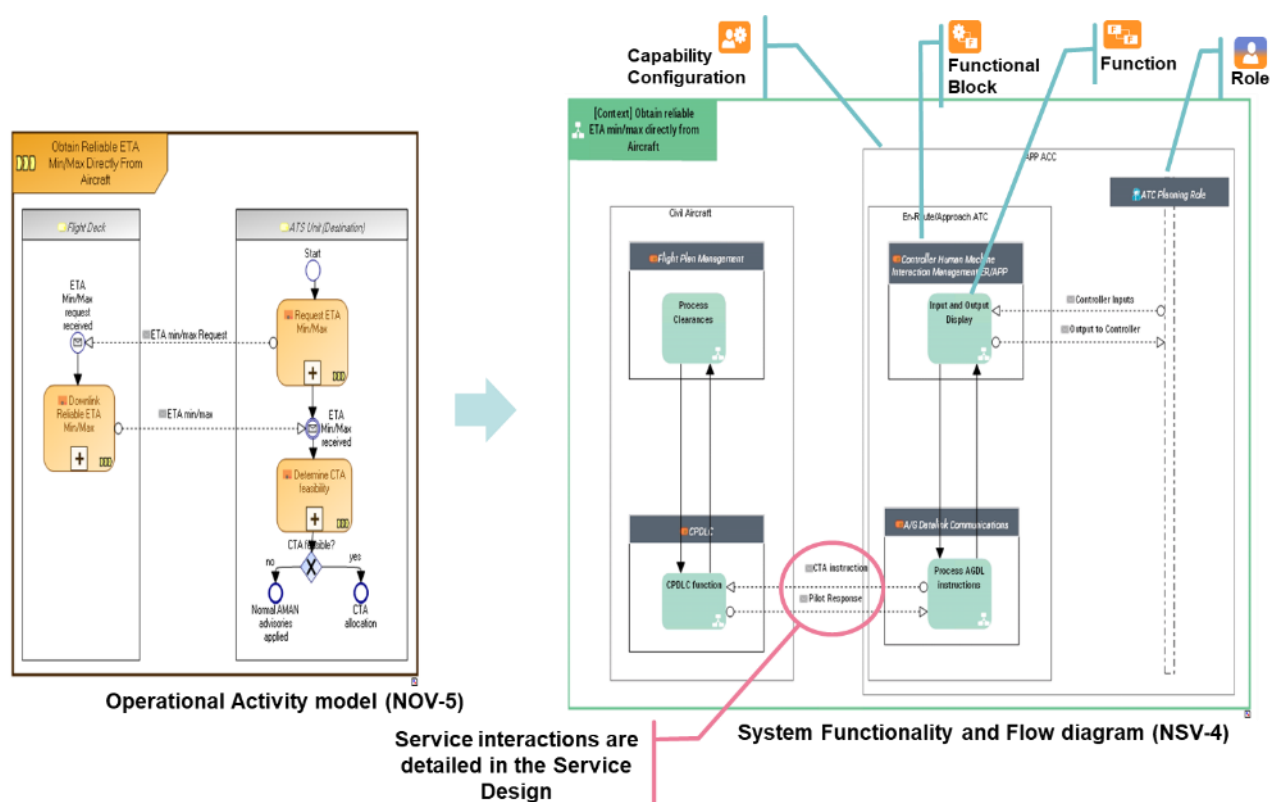


Figure 19: System Functionality and Flow diagram (NSV-4) created from an Operational activity model (NSV-4)

¹⁴ The term “Function” is used in EATMA modelling for this dedicated purpose. Meanwhile note that this term is quite generic and can be used in system engineering for many other purposes (e.g. high level functions at a very initial stage of the design of a new system, when the allocation of the resources to perform that function has not been decided).

One Function can support many operational activities and one activity may be supported by multiple functions as long as they are within the same node/capability configuration boundaries.

Capability Configurations are defined for specific purposes i.e. the same resources can be used in several Capability Configurations. A Capability Configuration provides and consumes Services and Resource Interactions. A Resource Interaction is used to describe existing interactions that are already standardised, whilst a Service is used for new interactions (e.g. SWIM Services). The Service enables loose coupling i.e. a System needs to consume or provide a service but the other end is not pre-defined.

USES of EATMA System Functionality and Flow model within the SRM: this is currently identified as being the most useful model of the EATMA System & Service layers for supporting the safety assessment in the initial and refined design phases and more specifically the Safety Requirements derivation within the success approach (as per Guidance H).

I.4 Logical Model

A Logical Model is a high-level, architectural representation of an ATM/ANS functional system design that leaves the door open to multiple alternatives for the eventual physical implementation of that design. It describes the main human roles or tasks, machine-based functions and airspace structures and explains what each of those “actors” provides in terms of functionality and performance. The Logical Model normally does not show elements of the physical design, such as specific hardware and software parts of technical systems, local implementation procedures or training, etc.

The Logical Model is a structural representation of the ATM/ANS functional system design, as it does not enable the description of the system behaviour (i.e. no mechanisms for modelling the sequence, parallelism, synchronisation or concurrency of actions/activities). Consequently, in order to enable the derivation of a correct and complete set of Safety Requirements, the Logical Model needs to be used in conjunction with the EATMA operational activity model (NOV-5 diagram) and/or a more detailed description of the human tasks and interactions with the technical systems which might be provided by the HP assessment in the form of a Task Analysis.

Figure 20 shows a typical graphical representation of the logical model for the TMA ATC functional system which has been instantiated to support the safety requirements derivation for the Point Merge system operations (PM).

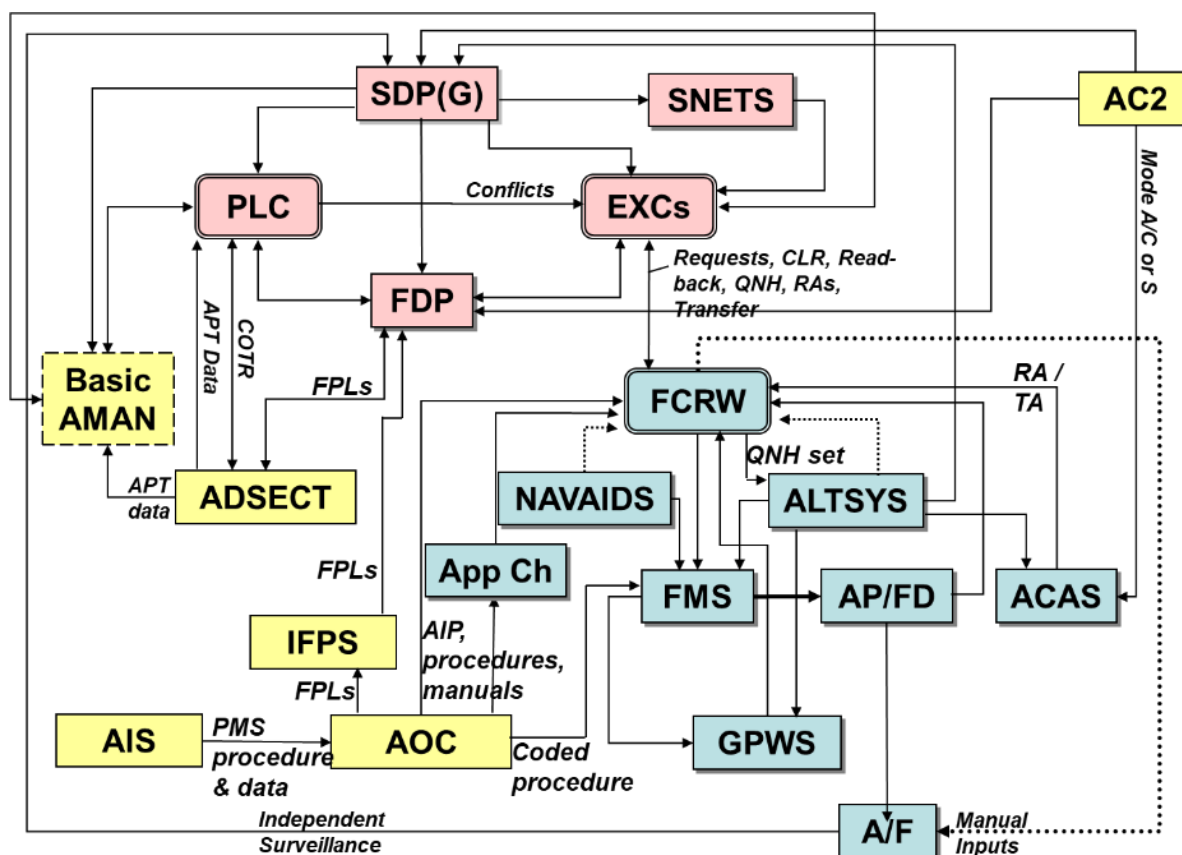


Figure 20: Typical Logical Model for the TMA ATC functional system instantiated to support PM operations design

The symbols&acronyms used in the model are the following (ground elements are in Pink, airborne elements in Blue and external entities in Yellow):

PLC	Planner ATCO (human roles are represented via a double line rectangles)
EXCs	Executive ATCOs (ITM and FIN DIR)
SDP(G)	Surveillance Data Processing- ground (technical systems or functions are represented via single line rectangles)
FDP	Flight plan Data Processing system
SNETS	Safety Nets- ground (STCA, APW)
FCRW	Flight Crew
NAVAIDS	Navigation system and supporting NAVAIDS
FMS	Flight Management System

ALTSYS	Altimeter system
App Ch	Approach chart
AP/FD	Auto Pilot/ Flight Director
GPWS	Ground Proximity Warning System
ACAS	Airborne Collision Avoidance System
A/F	Airframe
AC2	A second aircraft (external entity represented in Yellow)
ADSECT	Adjacent sector/ control unit (E-TMA or Airport TWR control)
Basic AMAN	Arrival MANager
IFPS	Initial Flight plan Processing System
AOC	Aircraft Operator Centre
AIS	Aeronautical Information System
	Main interactions & information flows

Human-machine interfaces (HMIs) are not represented explicitly in the Logical Model, but are implicit in each link between human and machine shown on the model.

The graphical representation of the Logical Model needs to be complemented by a textual description of the functionalities of each of its elements and of the content of each main interaction/information flow, whilst highlighting what is changed by the Solution compared to the Baseline (Reference).

USES of the Logical Model within the SRM: The Logical Model is a system representation that may support the Safety Requirements derivation in the initial and refined design (as per Guidance H), as an alternative to a missing EATMA System Functionality and Flow model or to complement it.

I.5 Thread Analysis model

Thread Analysis enables a behavioural representation of an ATM/ANS functional system (or sub-system) using a particular graphical presentation in which the actions of the individual elements of the Logical Model, and the interactions between those elements, are represented as a continuous ‘thread’, from initiation to completion.

The main equipment functions and human actions are described by reference to the related Safety Requirements (*functionality and performance properties* from the success approach) although some relatively minor functions / tasks may be represented only in the Threads themselves.

The Threads tell us more about the intended operation of the ATM/ANS functional system than could the Logical Model or Safety Requirements (success approach) on their own; therefore, they are regarded as an integral part of the design and of the corresponding set of Safety Requirements (*functionality and performance properties*).

An example of a Thread Analysis that has been used to complement the Logical Model for the TMA ATC functional system instantiated to support Point merge (PM) operations design is shown in **Figure 21**.

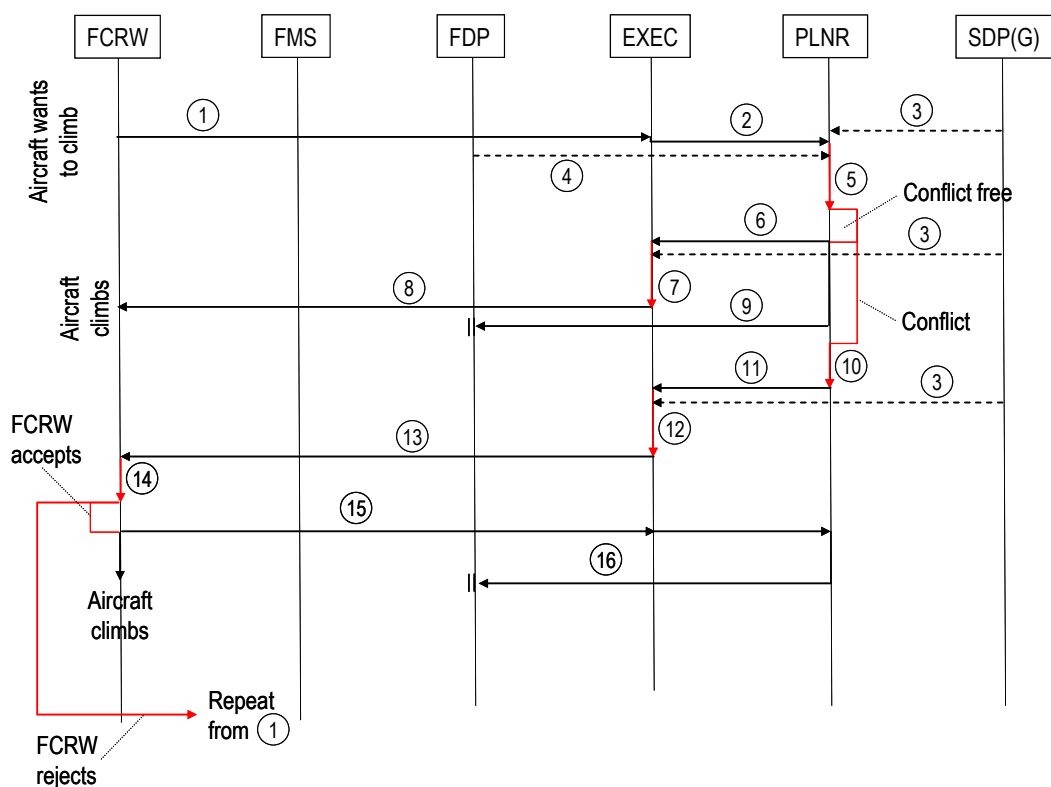
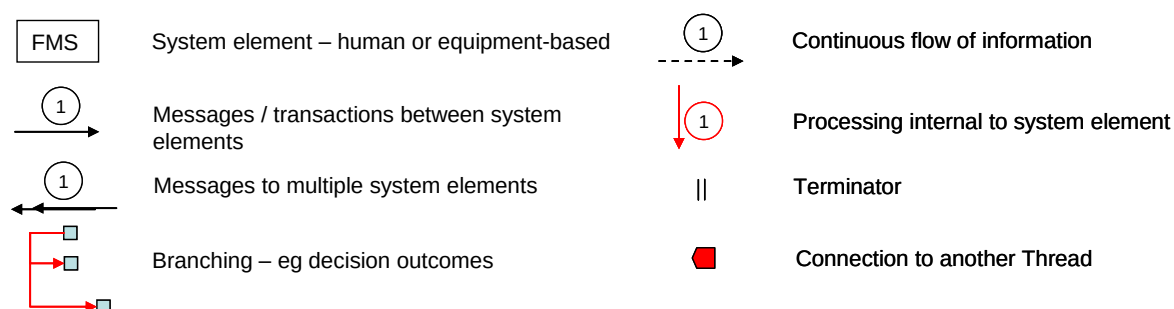


Figure 21: Example of a Thread Diagram (complementing the Logical Model for the TMA ATC functional system instantiated to support Pont Merge operations design)

Key:



Founding Members

Pre-condition

A flight needs to change its agreed trajectory – e.g. to avoid bad weather. The example shown is a requested climb.

Actions:

1. Flight Crew (FCRW) requests climb to a new flight level
2. Executive Controller (EXEC) asks Planner (PLNR) to coordinate with next Sector
3. Surveillance Data Processing (Ground) – SDP(G) – passes continuous ground surveillance data to EXEC and PLNR: Safety Requirement (success approach) [SG01]
4. Flight Data Processing (FDP) provides continuous Flight Plan information to PLNR [FD01]
5. PLNR coordinates change of FL with next Sector [If conflict-free go to (6) else go to (10)]
6. PLNR advises EXEC that the proposed FL is conflict-free (or at least acceptable to next sector)
7. EXEC decides (on basis of SDP(G)) whether / when the aircraft can start its climb [EX05]
8. EXEC clears aircraft to the requested new FL
9. PLNR updates the Flight Plan on the FDP [PL03]
10. PLNR chooses and coordinates alternative new FL with next sector [PL05]
11. PLNR advises EXEC of alternative new FL
12. EXEC decides (on basis of SDP(G)) whether / when the aircraft can start its climb [EX05]
13. EXEC clears aircraft to the alternative new FL
14. FCRW decides if the alternative new FL is acceptable operationally [If not acceptable, FCRW must request preferred alternative – i.e. go back to (1) – else go to (15)]
15. FCRW confirms climbing to << the alternative new FL>> [FC06]
16. PLNR updates the Flight Plan on the FDP [PL03]

The above depiction/notation might be replaced by a modified version of UML System Sequence Diagram (or equivalent) format, in line with current ATM and avionics industrial practices.

The use of the Thread Analysis is expected to bring the following benefits:

- it leads to an enhanced understanding of how the designed ATM/ANS functional system would work in practice – this should be of benefit to the rest of a Solution, not just to the safety assessment;
- it helps correct errors, inefficiencies and inconsistencies in the Logical Model or even in EATMA models; and

- it proves very effective in identifying missing or incorrect safety requirements (*functional and performance* from the success approach) for the Normal conditions.
- furthermore, by “breaking” Threads or inserting spurious Threads, it should be possible to get a better understanding of the behaviour under abnormal conditions (e.g. effects of external failures) or faulted conditions (failures generated by the ATM/ANS functional system itself), identify reversionary modes of operation and define contingency procedures associated to the degraded modes of operation. Thread Analysis is a very cost-effective way of proving the correctness of the initial and refined design under a wide range of normal and abnormal conditions.

USES of the Thread Analysis Model within the SRM: Thread Analysis is a system representation that may support, in the initial and refined design, the completeness and correctness check of the Safety Requirements that have been initially derived based on a Logical Model (as per Guidance H).

Guidance J On the usage of Resilience Engineering

J.1 Overview

The guidance describes the Resilience Engineering activities that provide a means to investigate everyday operations based on analysis of varying conditions, work-as-done and adaptive capacity to improve the resilience of ATM/ANS functional systems. The guidance recommends the usage of resilience engineering to complement the safety assurance activities performed in support of the SESAR Safety Reference Material, including the success approach. The relevant Resilience Engineering activities described in this guidance material have been used to feed the SRM safety assurance activities listed in Guidance A.

J.2 Introduction

While safety is traditionally viewed as the absence of unwanted outcomes, such as errors and accidents, recent trends in safety research insist on the necessity to understand and support how safety is actively produced. In the latter view, operators are not seen as the fallible elements of a system that otherwise functioned as designed, but as major sources of reliability necessary for successful operations. Indeed, even well-engineered systems cannot anticipate all potential variability they might face, and rely on operators' capacity to understand and adapt to changing, potentially surprising conditions to ensure safe operations. Ironically, because operators are successful in doing so, those adaptations remain unnoticed if they are not explicitly investigated.

In the context of the increased complexity of the ATM system, safety assessments may benefit from techniques based on system-oriented conceptual and methodological approaches. Especially in the context of innovative SESAR concepts that may transform the nature of operations, a safety assessment approach needs to adopt a view of the system as a whole and purposefully consider the different responsibilities and interactions between components (human and/or technical).

The Resilience Engineering activities described in this guidance provide the means to address these two fundamental issues, based on the philosophy and concepts of Resilience Engineering (RE). RE aims to investigate how work systems successfully handle varying conditions, whether expected or not, in order to improve their design. This aim involves understanding how those systems are capable of adjusting their behaviour to pursue essential goals in the face of changing conditions that can represent challenges, surprises or opportunities. RE is explicitly based on the study of the complex work system.

J.3 Core Principles

The Resilience Engineering activities are based upon a few core elements and principles from Resilience Engineering:

- **Varying conditions:** Variability and uncertainty are inherent in complex work such as ATM; the conditions and challenges that manifest themselves are many and various. These can take the form of changes experienced in the daily life of operational units everywhere; or surprises

that emerge from the interface of system elements that interact in unusual ways (e.g., hidden interactions); or challenges such as volcanic ash that defy any form of prediction. The RE activities aim to reveal the varying conditions the new design will need to handle.

- **Adaptive capacity:** Adaptive capacity is the potential for adjusting patterns of action to handle the varying conditions described above. It is useful to distinguish between two forms: a base adaptive capacity, which represents the ways the system handles varying conditions by design (e.g., procedures and experience for a specific unusual situation); and an extra adaptive capacity, which represents the system's capacity to handle situations that fall outside of the typical and planned for situations (e.g., operators solve a novel problem based on their expertise). Adaptive capacity, especially the latter form, is at the heart of the notion of resilience, and the RE activities aim at capturing, analysing and explaining how the new design impacts the system's adaptive capacity.
- **Work-as-done:** refers to work as it is actually performed in everyday operations; work-as-done (WAD) is understood in contrast with work-as-imagined (WAI), i.e., work as it is designed, how it occurs in principle or is planned to occur. Indeed, varying conditions cannot be fully specified, and adjustments are inevitable, leading to a difference between WAD and WAI. The RE activities are based on describing how systems work through exploring WAD. Consistent with user-centric methods, they rely on the inputs of the people who will work with the new design when it is implemented. This is achieved by letting operators and managers explain how they intend to use the new design and thereby explore the possibilities that will emerge. The RE activity aims to close the gap between the operational world and the people who are implementing the new design.

J.4 When to use Resilience Engineering in the SRM process

Assessments which use the RE guidance will have a broader scope and include activities which extends the SESAR Safety Assessment Process. Understanding changes between the current operation and new design can provide additional safety narratives that inform project decision making, support the derivation of new or modified requirements or validation objectives or can be included in safety cases.

The RE guidance provides qualitative support to the initial V1 stages of the concept development process. It supports the exploration of how safety is created in the current operation (by design or by innovative behaviour at different levels of the system). The RE activities also help developing an understanding of the purpose of the current system which informs the setting of goals for the future system.

As a concept becomes more mature, the RE activities support the investigation of the resilient properties of the current system and how these will be impacted in the future system. Scenarios for validation are enriched by an improved understanding of the likely varying conditions which may be encountered in operations. Recommendations for new or amended systems engineering requirements which capture the resilient properties required in the future system are generated. The

argument for the completeness of the safety assessment is supported because a comprehensive and structured analysis of these scenarios will have been generated.

This RE guidance provides an alternative and complementary perspective on system performance not just on safety. This additional perspective is particularly relevant for innovative designs that significantly impact operational working methods.

The relevant RE principles have been integrated into existing SRM activities. The RE processes should be conducted as a complete set of Steps 1-4 and iterated as required. For example, it may be beneficial to undertake an RE assessment early in the concept development e.g. to support the V2 OSED and explore concept ideas and set validation aims, and then repeat the exercise in the V2 initial design stage when the concept is more mature and validation results may be available to support requirements development.

The RE activities are intended to support the efficacy and rigour of the SRM requirements generation process.

J.5 Description of the RE Activities

The RE activities are organised in 5 steps, which follow **Figure 22** below.

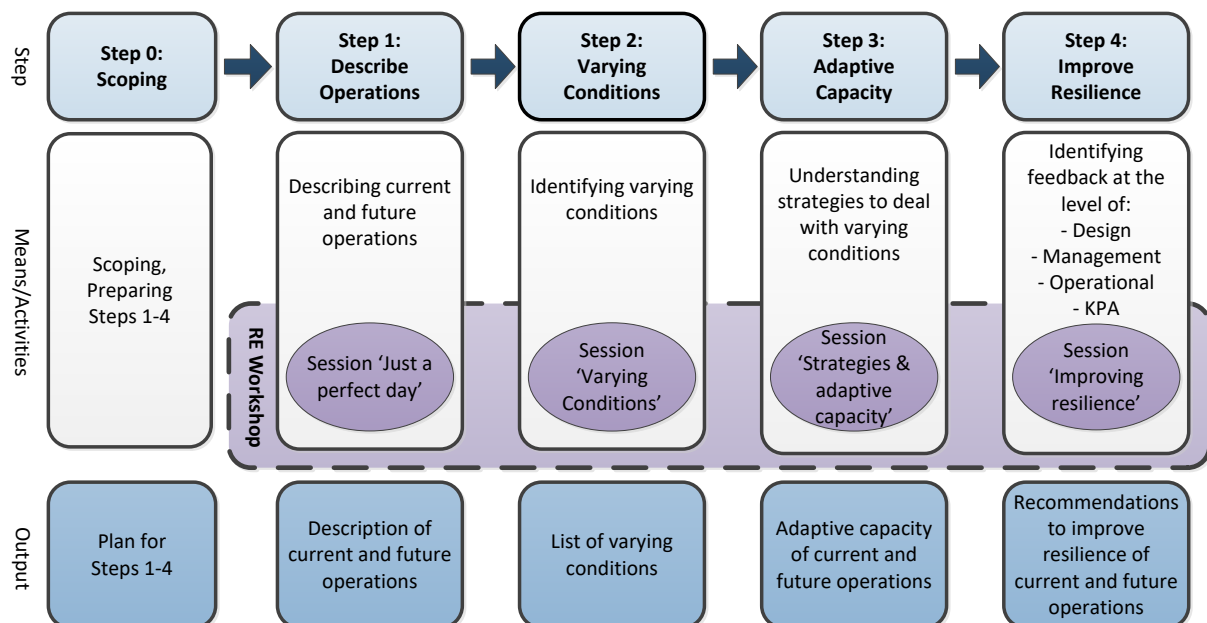


Figure 22: The RE activities are organised into 5 main steps

J.5.1 Step 0: Scoping

Objective - Scope and plan the work to be undertaken.

- Studying background information on RE, including documentation on the RE principles and on previous applications. Novice practitioners are recommended to take an RE training course.

- Developing a plan for the activities to be conducted in Steps 1-4. As part of the planning activities it should be decided whether these activities are to be conducted as a separate activity to inform the safety assessment, for example as RE workshop(s) (Figure 1 shows the recommended main sessions to be conducted as part of such RE workshop), or whether they should be integrated into other SRM activities to be conducted as part of the safety assessment. In the latter case the RE Steps should be reviewed and the safety plan should describe how the RE Steps will be integrated into other SRM activities. The next sections provide some guidance on the alignment with the stages of the SRM safety assessment, for the case when an integrated/augmented approach is to be followed.

Output - The Safety Plan integrates the RE steps with other activities conducted as part of the SRM safety assessment in accordance with **Guidance A**.

J.5.2 Step 1: Describe Operations

Objective - Build an initial understanding of the work-as-done in current ATM operations and of the way that future ATM operations are expected to be done.

Alignment to SRM - This activity can support the description of the Operational Environment before the proposed change and the development of the operational description as required by the SRM (Guidance A.1-A.2 and Guidance B).

Means - These include:

- Studying available documentation on current and future ATM operations e.g. OSED, validation plans, safety and human performance assessments reports, validation reports, procedure and rule sets, etc.
- Observations of current and future ATM operations to determine how operators (such as controllers, pilots, supervisors, engineers), act and interact with each other and with their human machine interface (HMI) and environment. For current ATM, actual operations can be observed. For future ATM operations, in later stages of the development lifecycle, real time simulations may be available for such observations.
- Interviewing the design experts of the future ATM operational concept regarding the context and details of the design that may not be available by the above means.
- Operational expert groups (controllers, pilots, supervisors, etc.) explain what a typical day of operations without considerable varying conditions ('just a perfect day') looks like for them in their current work. Next they are asked to express their expectations of what such a perfect day would look like in the future operation. This session serves to achieve a common understanding of the operations from various perspectives and to set the basis for identifying varying conditions and strategies in later sessions.

Output - An initial description of the work-as-done in current ATM operations and of the way that future ATM operations are expected to be done.

J.5.3 Step 2: Varying Conditions

Objective - Identify a list of expected and unexpected varying conditions that ATM operators and managers may have to deal with in the current and future ATM operation.

Alignment to SRM - The identification of varying conditions supports the development of the success case of the SRM and can be used to inform the capture of abnormal conditions which the proposed concept may be expected to encounter during its lifetime (Guidance A.2 & Guidance G). This Step, when combined with Step 3, identifies, and provides justification for, the design features necessary to support the future operation.

Means - These include a combination of the following:

- Using results of Step 1 such as validation reports or field observations to identify varying conditions.
- Using dedicated sessions with ATM operational experts, e.g. as part of an RE workshop or a FHA (Functional Hazard Assessment) workshop, to identify as many conditions as possible; rare conditions as well as normal conditions, and to consider situations both within as well outside of their control.

Output - The raw list of identified varying conditions can then be clustered into common areas and some which may be out of scope of the assessment can be removed. This list is used in Step 3.

J.5.4 Step 3: Adaptive Capacity

Objective - To obtain narrative descriptions of the strategies that operators use to deal with varying conditions in the current and the future ATM operation, and to analyse the adaptive capacity in the current and the future ATM operations.

Means - These include the following:

For each varying condition, the operational experts (controllers, pilots, supervisors) explain the strategy or strategies they use or envisage to use when dealing with this varying condition; first in current operations, and next in future operations. Some supporting questions are presented below:

- In what way and how often could the varying condition occur?
- Who or what would detect the varying condition, and how?
- What is the strategy to deal with the varying condition, i.e.: How would you act / adapt to the varying condition, with whom would you interact and coordinate, what resources are used?

- How is the strategy acquired, for instance is it part of basic training, is it learned by experience?
- What are the trade-offs and what are the effects of applying the strategy on ATM key performance areas such as safety, capacity, costs, and environment?

The raw data obtained is used as input to an adaptive capacity analysis. Many techniques are available to support this analysis and these aim at organising the raw data by identifying actors, interactions, dependencies, goal conflicts, patterns of behaviour, cascade effects, and sources of resilience. They are applied to the raw data for both the current and the future operation, thus supporting a comparative discussion. For the selection of a technique it is important to keep in mind that its application should provide effective input to Step 4.

Output - A narrative description of the strategies that are available when dealing with varying conditions, for the future ATM operation as well as for the current operation, and insight into the adaptive capacity of both the current and the future ATM operation.

J.5.5 Step 4: Improve Resilience

Objective - Derive recommendations for strengthening the resilience of current and future ATM operations.

Alignment to SRM - This step supports the SRM processes which develop systems engineering requirements for the future concept. This step supports the capture of user requirements and helps develop the rationale for design features (specifications, system behaviour, etc...). This step can help inform the development of Safety Criteria in the SRM. It can also support the rationale for such changes (or for why there are no changes) and capture operational safety effects and mitigations for possible failures (**Guidance A.2, A.3 and A.4**).

Means - These include a combination of the following:

Organisation of a session with operational experts to identify measures to improve the resilience of current and future ATM operations focussing on improvements at four levels:

- Design level, human factors, procedures, airspace structure, layout of the workplace, etc.
- Management level, including supervisors, managers and their procedures and processes for managing and controlling the organisation.
- Operational level, including training, organisational learning, team considerations, safety culture, etc.
- KPA (Key Performance Areas) level, including effects on safety, capacity, environment, cost-benefit.

Output - Depending on maturity of the concept, Step 4 can deliver new or amended design recommendations to support SRM activities such as Safety & Performance Requirements (SPR), Safety issues, Human performance issues / benefits, Human Performance (HP) Recommendations, Limitations, Assumptions, and Validation needs and scenario inputs. These outputs are recorded in the regular SESAR documentation.

Guidance K On the usage of Dynamic Risk Modelling

K.1 Forewords and introduction

Where performance variability of both people and equipment are combined, it may lead to varying levels of performance and deviation from normal practice. These in turn may ultimately lead to accidents or, alternatively, contribute to successful operations and greater System robustness.

Dynamic Risk Modelling (DRM) refers to the class of modelling techniques that explicitly models the dynamic performance of operation (people, equipment, procedures, and environment) and their time-dependent interactions.

The technique looks at a variety of possible combinations and permutations of events as they unfold through time. Where necessary (e.g. for the relevant sub-set of scenarios / use cases – see selection criteria below), DRM provides more accurate results that cannot be obtained through linear approaches.

As per **Guidance A** above, DRM can be used to verify that the Safety Requirements are complete, correct, and mutually consistent by reference to the Safety Objectives and SAC.

Various DRM approaches are available. They aim at providing augmented insights, with a sharper and more accurate assessment of safety risk (both success and failure). The approaches include (but are not limited to):

- ICAO Collision Risk Modelling (CRM): incl. the guidance available in A Unified Framework for Collision Risk Modelling in Support of the (Doc 9689), ICAO Doc 9274: Manual on the Use of the Collision Risk Model (CRM) for ILS Operations,
- Encounter-model: guidance can be found in, e.g., ICAO Annex 10 VOL 4 to calculate the effect of ACAS on the risk of collision
- Agent-based DRM for which extended method description as well as a case study are available on SESAR Platform.

Other methods and tools may be used however Transversal Activities in SESAR in agreement with the SJU focuses on the use of Agent-Based DRM, and for which:

1. Full Guidance has been developed in **[12]**.
2. A case study had been conducted as part of SESAR 1 – Conflicting ATC Clearances – that focused on a Landing versus Line-up use case. For the full report of the case study, see **[13]**.

As a result, and without being to the detriment of other techniques, this Guidance focuses on Agent-Based DRM only. It should evolve with the forthcoming annual releases of the Guidance Material with the inclusion of other approaches that can eventually be equally applicable.

As a result, it details the pre-requisites and the selection criteria and gives a summarized version of the description of the Agent-Based method. It is obvious that the deployment of the method will require far more insights and understanding. This will in particular require a thorough reading of the references **[12]** and **[13]** as well as appropriate operational, modelling and mathematical skills.

K.2 Pre-requisite and selection criteria

The deployment of Agent-Based DRM is an activity that requires the combination of a series of disciplines as well as time and resources. As a result:

- a) The PRE-REQUISITE is that a safety assessment based on ‘conventional’ (static) methods and tools has been conducted to a level of details that enables to make an informed decision on whether to go to a DRM-based study using the selection criteria below. This ‘conventional’ assessment has brought into play, in particular, but not limited to, the relevant safety assurance activities as per **Guidance A** above.
- b) INFORMATIVE SELECTION CRITERIA are needed. DRM is not ‘*for everything or everyone*’, and identification of when it should be applied is necessary. Those selection criteria are:

Criterion 1.: *Safety can be expressed as a function of physical parameters*: The Project requires that safety risk results are expressed as function of some physical parameters (e.g. separation distance between two parallel routes, descent/climb rate, distance between crossing point and runway threshold...) in order to derive specific requirements regarding the optimal value (from a safety perspective) of those parameters.

Criterion 2.: *System involving complex dynamic interactions*: The System being assessed involves complex dynamic interactions (encompassing human-equipment, equipment-equipment and human-human interactions) which might be characterised according to the following sub-criteria:

2a. *System behaviour (success & failure) depends on system status over time*: The system behaviour, when considering equipment functional variability and failures, human performance variability and errors, involves occurrences which cannot be considered in isolation, as they depend on whether other occurrences have already arisen (*i.e.* stochastic dependencies)

2b. *System behaviour (success & failure) depends on process variables*: The system behaviour when considering equipment functional variability and failures, human performance variability and errors, depends on process variables (e.g. the effect of an avoidance instruction following a short term conflict alert (STCA) depends on avoidance instruction being appropriate, the relative position and movement of involved aircraft, the pilot response and the flight parameters)

Criterion 3.: *Safety “importance” of the Change*: The safety importance of the change associated to the project shall be high. High is defined in terms of reducing or increasing safety risk in relation to the performance of AIM safety barriers. At Solution level, these are described in terms of Safety Criteria (SAC), or in terms of the severity of the operational hazards that are impacted or the new ones that emerge. Whether the safety importance is high enough to apply DRM is left to the appreciation of the Project. The Project must be supported by appropriate expert judgment and be aware of the resources that can be reasonably allocated to the safety assessment.

The following table provides support on decision-making by linking the above criteria to the DRM method that may be recommended. However, the ultimate decision on the selection should integrate the consideration of System thinking, constraints of operational effectiveness, time, and cost as well as required rigour attached to the evidence to be derived.

<i>Cr1: Safety expressed as f(physical parameter)</i>	<i>Cr2: System with complex dynamic interactions</i>	<i>Cr3: Safety importance of the Change is high</i>	<i>First advise</i>
YES	NO	YES	GO for ICAO CRM or Encounter model-based
NO	YES	YES	GO for Agent-based DRM
YES	YES	YES	GO for Agent-based DRM
Any remaining combination			NO GO for DRM

K.3 Description of the method

The following steps provide a high level view of the DRM method:

1. Preparatory activities to scope the application of DRM
2. Develop the dynamic risk model
3. Develop risk decomposition
4. Implement the dynamic risk model into software
5. Run Monte Carlo simulations
6. Assess bias and uncertainty
7. Develop safety risk results

Each of these steps is further explored below. A full description of each step can be found in [11][12][13].

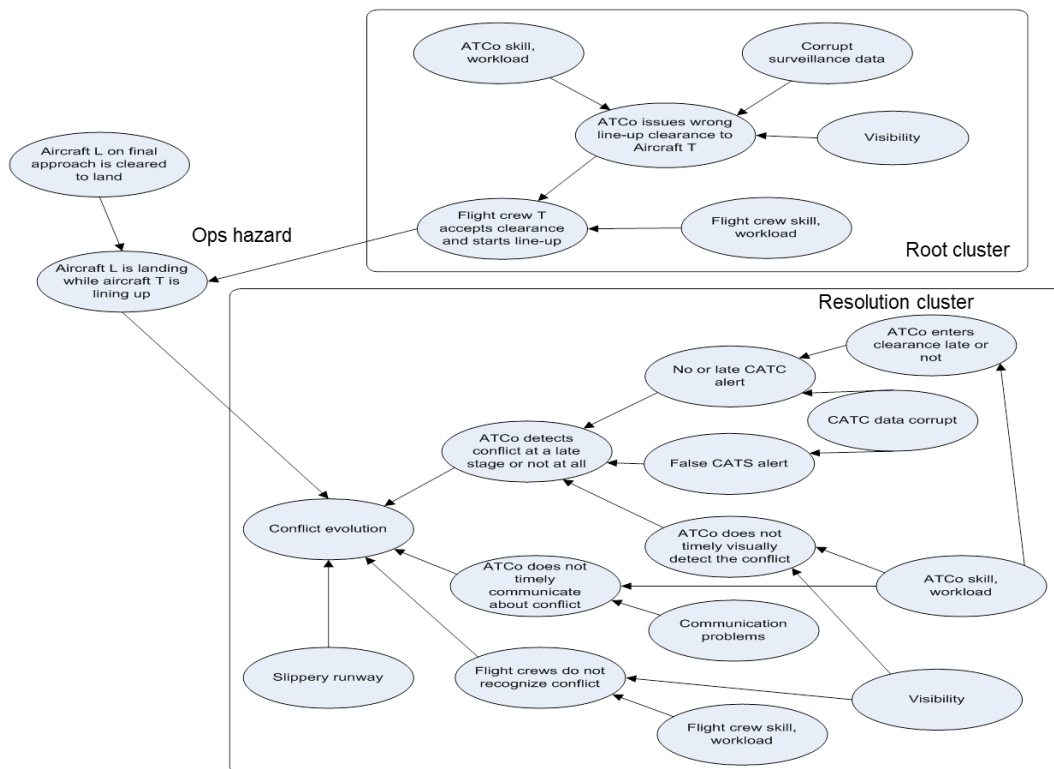
K.3.1 Preparatory activities

This includes:

- Scoping of the DRM assessment; this can be, for instance (but not limited to), the selection of a sub-set of uses cases as per the OSED or a specific aspect of a given use case
- The collection from the 'conventional' (static) safety assessment work already conducted of all relevant (as per the scope defined above) success- and failure-related safety information. This should encompass the definition of System operations in normal/abnormal conditions as well as list of operational hazards, with relevant causes, effects and mitigations.
- Clearly defining the objectives (i.e. type of evidence) of DRM (e.g. estimation of risk related to an undesired state)
- Developing operational hazard scenarios. Operational Hazard Scenarios are constructed with a view to preparing the agent-based DRM modelling. An Operational Hazard Scenario

describes the evolution of an operational hazard, under the influence of related operational conditions (such as flight phase and location, number of traffic, environmental conditions, etc.) and the related hazards (i.e. root hazards, resolution hazards, pre-existing hazards). Each such scenario aims to bring into play all the relevant ways that an operational hazard (e.g. an aircraft conflict) may develop and evolve, under the influence of the related operational conditions and hazards.

An illustration of an operational scenario is given below (see also [13]).



- Appropriate data mining techniques for those parameters making up the dynamic risk model (as per K.3.2 below) as well as the type of distributions to be used for the relevant parameters (normal Gaussian, triangular, etc.)

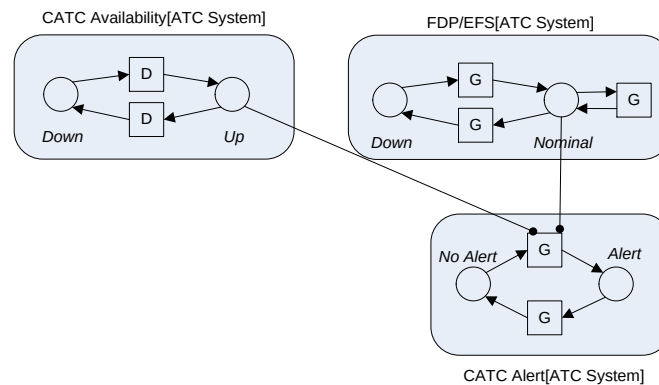
K.3.2 Develop the dynamic risk model

A multi-agent stochastic dynamic model is developed, which describes the stochastic dynamic evolution through time of one (or a selected set of) Operational Hazard Scenarios. Multi-agent refers to an operation or system that consists of multiple interacting agents. An agent is a distinctive element in the operation, which has its own states and situation awareness, operates relatively independently from other agents and interacts with other agents where applicable. The model uses the syntax of Stochastic Dynamically Coloured Petri Net (SDCPN) (for further details, see [12][13] as well as references in K.6). This is developed with the following six iterative steps that are:

1. Identify the relevant Agents
2. Identify the relevant entities per Agent
3. Specify a Local dynamically coloured Petri Net (LPN) per entity
4. Interconnect the LPNs within each Agent

5. Interconnect the Agent models
6. Check how the operation and each hazard has been modelled, and iterate

The syntax of the Dynamically Coloured Petri Net (DCPN) consists of Places (circles), Transitions (squares) and Arcs (arrows) that connect the Places with the Transitions is fully defined and explained in [12]. For illustration only, the figure below shows a LPN network for the Conflicting ATC Clearances detection system and interactions with the Flight Data Processing (FDP)/Electronic Flight Strips System (EFS).



K.3.3 Develop risk decomposition

Once the SDCPN-based model is completed, it can then be used as basis for a Monte Carlo (MC) simulation to determine the probability of occurrence of a safety event, e.g. an aircraft collision. In principle, the number of occurrences of the safety event are counted and divided by the number of runs (or by the number of associated flight hours or movements). The accurate assessment of such low collision probability values through brute force Monte Carlo simulation of a dynamic risk model might require high investment in terms of simulation times or computing resources. To overcome this resource demand and speed up MC simulations, risk decomposition is applied.

Risk decomposition involves identifying some conditions or states in which the system can enter or which it can leave as a result of events (normal evolution, reconfiguration, failure) occurring in a specific group of agents with no dependence on the status/evolution of the remaining agent entities. When such an appropriate set of conditions (*Condition_k*) has been identified, they would be pre-conditions of the occurrence of the Safety Event (e.g. collision), with the probability:

$$P(\text{Safety Event}) = \sum_k P(\text{Condition}_k) \cdot P(\text{Safety Event} \mid \text{Condition}_k)$$

(where (*Condition_k*) and (*Safety Event* | *Condition_k*) are independent

The probabilities on the right-hand side of the equation are determined as follows:

- The probabilities $P(\text{Condition}_k)$ can be determined analytically (given the way these conditions have been selected),
- The probabilities $P(\text{Safety Event} \mid \text{Condition}_k)$ are determined (“simulated”) separately for each k . The procedure is to make a conditional SDCPN model that starts in the situation of (*Condition_k*), and then to run MC simulations on the conditional SDCPN model to count occurrences of the Safety Event. This process determines $P(\text{Safety Event} \mid \text{Condition}_k)$.

K.3.4 Implement the dynamic risk model into software

In this step, when the specification of the DCPN-based model and the risk decomposition are fully defined, they are implemented in software language in order to be able to run Monte Carlo simulations. Many software languages are suitable for this, as long as they accept all SDCPN syntax principles. A major step in the software implementation is to test the code against all elements of the SDCPN-based model and Risk decomposition. For instance, for the study case described in [13], the model has been coded in Delphi using Embarcadero RAD Studio XE3.

K.3.5 Run Monte Carlo simulations

In this step, the software implementation of the DCPN-based model is used to perform Monte Carlo simulations and compute safety risk results. Any Safety Event that can be observed in such simulation can be counted, and the number of counts, divided by the number of runs or the number of associated flight hours or movements, provides an estimate for the probability of occurrence of the Safety Event (e.g. a collision).

In addition, several potentially representative parameters need to be varied (e.g. at least between a baseline, a low and a high value), in order to observe trends regarding impact on the safety event probability. These trends provide the most valuable indication on the validity of the model, i.e. whether it correctly represents the reality. In case errors are identified, the dynamic risk model needs to be corrected and the subsequent risk decomposition updated accordingly.

K.3.6 Assess bias and uncertainty

By definition, any model is not the exact image of reality. The purpose of a bias and uncertainty assessment is to identify how the differences would impact on the evaluation of the risk level in terms of bias and uncertainty:

- Bias: the model-based accident risk is systematically higher or lower than the risk of the real operation.
- Uncertainty: the model-based accident risk lies in a range of credible values for the risk of the real operation (e.g. a 95 % credibility interval).

This is done by assessing each parameter value in the dynamic risk model on uncertainty (represented by a credibility interval around the chosen value) and sensitivity (how much does the Safety Event probability change if the parameter value changes), and by assessing each model assumption (i.e. modelling choice with potential to create a difference between model and reality) on bias and direction. In line with the logic explained at the Risk decomposition step, these assessments might be performed analytically or might require dedicate MC simulations.

All results are combined to determine the bias and uncertainty around the Safety Event probability. Those parameters and assumptions with the highest bias and uncertainty contribution can be used to determine the most effective improvements in the model (either in improving its structure or in guiding additional data collection, where possible). In addition, the final safety risk results (as per next step) shall not be interpreted in isolation but combined with the bias and uncertainty results.

Last but not least, when modelling errors are discovered late in the process and are controllable, they can be fixed by affecting the results with the adequate bias.

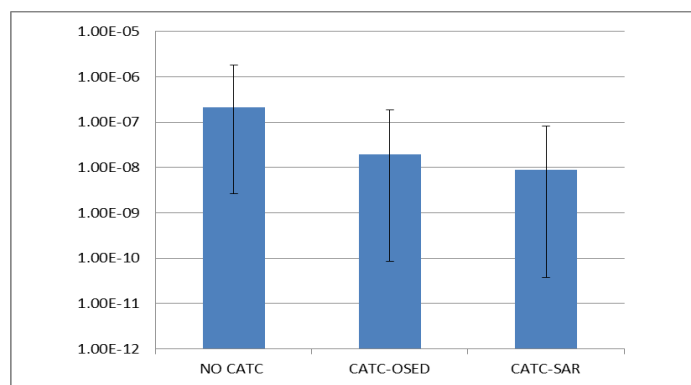
K.3.7 Develop safety risk results

The results of the previous steps provide point estimates and credibility intervals for the probabilities of safety events in various conditions. Checking these results against safety criteria (expressed in absolute or relative terms) provides insight in risk tolerability and risk margins.

Furthermore, the results of the sensitivity analysis for variation of particular parameter values (e.g. those conducted within the Bias & Uncertainty step) can be used to identify safety bottlenecks (aspects of the operation that contribute to unacceptable risk levels) and they provide a basis to determine any additional safety requirements and safety objectives.

Finally, remaining safety issues from the ‘conventional’ (static) safety assessment can be addressed taking advantage of the capability to account for the time-dependant behaviours and/or dynamic interactions (e.g. regarding effectiveness of a recovery procedure involving a combination of system data processing & information display, Controller detection & decision & instruction and Pilot implementation or concurrent action based on its own situation awareness).

For illustration only within this Guidance, the figure below shows the risk comparison for three different scenarios that have been analysed in the case study.



K.4 Required skills and competence

This section provides a description of the main skills and competence require to deploy a DRM capability appropriately.

1. **Resources & Skills** –DRM modelling is technically demanding work that requires significant resources and skills. The necessary DRM skills can be acquired through adequate training. The pre-requisites are: being familiar with (classical) safety assessment and having a strong mathematical background. Note that the amount of resources required, in terms of person hours and throughput time, depends highly on the complexity of the operation to be analysed, the previous experience of the DRM practitioner and the possibility in re-using previous related sub-models.
2. Currently, **SW implementation** of the model and subsequent modifications are cumbersome and create work. This is because there is no automatic coding of the DCPN into software. This coding of the DCPN into software would be unnecessary if graphical tools to implement the DCPN model were available. These tools would increase productivity significantly by supporting iterative model building, validation of input parameters and risk decomposition.
3. **Availability of data** – Similar to static approaches, it is often hard to give values to input parameters when data is not available. Many parameter values are therefore estimated by experts, but validation of these values is very difficult. This is partly mitigated through the Bias & Uncertainty (B&U) assessment; in case the safety results appear to be sensitive to a parameter

K.5 Conclusions

This chapter of the Guidance material for the application of the SRM has summarised the DRM approach developed for SESAR. It is acknowledged that Agent Based DRM is not the only method that is available and similarly is not the only method that may be deployed within SESAR. However, the research from SESAR 1 [11][12][13] in collaboration with the SJU determined that Agent based DRM was the approach to be further explored in SESAR.

The method requires careful consideration before application and this guidance contains criteria that support the choice of method and the choice of project upon which this powerful tool could be deployed.

DRM has the ability to provide insights to safety that static methods do not afford (in particular addressing dynamic interactions, variability of performance, coupling aspects, etc.).

K.6 Additional References

In addition to references made above [11][12][13] and ICAO documentations, the following can provide useful information for the deployment of Agent-based DRM:

- [Blom et al., 2006] H.A.P. Blom, S.H. Stroeve, H.H. De Jong, Safety risk assessment by Monte Carlo simulation of complex safety critical operations, Proc. 14th Safety-critical Systems Symposium, Bristol, UK, February 2006, Eds: F. Redmill and T. Anderson, Springer, London, 2006
- [Everdij, 2010] M.H.C. Everdij, Compositional modelling using Petri nets with the analysis power of stochastic hybrid processes, PhD Thesis, June 2010
- [Everdij et al, 2006] M.H.C. Everdij, H.A.P. Blom, S.H. Stroeve, Structured assessment of bias and uncertainty in Monte Carlo simulated accident risk, Proc. 8th Int. Conf. on Probabilistic Safety Assessment and Management (PSAM8), May 2006, New Orleans, USA.

Guidance L On Safety and Human Performance (HP)

L.1 Introduction

ATM will continue to depend upon the successful management and use of systems by “human operators”, which will relate directly (or indirectly) to the Safety of the Operational service. Hence, it is not sufficient to simply ensure that technical equipment delivers functionality reliably in order to guarantee Safety. The relationship between people, equipment and procedures must be assured such that where Safety depends upon the actions of the operator (controllers, engineers and all other related human roles) that those actions can be delivered reliably, with the desired outcomes within the required timeframes. This infers that in delivering safety, one must ensure Human Performance (HP). Thus, a close coordination between safety and human performance on performing the assessment of the corresponding concept in a Solution is essential.

An overview of the HP process is shown in L.2, together with a description on the tasks in which coordination is needed, providing proposals on how this coordination can be done.

One specific task that needs coordination between Safety and Human Performance relates to assess contribution of Human error, in conjunction with an equipment failure, to hazards occurrences. More detail on how address Human error and Human reliability aspects is presented in L.3.

L.2 Safety and HP assessment

Safety assessments need to be coherent, integrated and holistic so that there are clear links between the Safety analysis, design/engineering substantiation and demands made upon the operators. Therefore, the understanding and adequacy of Safety claims made on operators, procedures and other resources should be demonstrated.

For that, safety and human performance have to coordinate when performing their assessment. The analysis should demonstrate that claims being made on operators have been understood and can be delivered feasibly with evidence provided by a systematic analysis process. The Safety assessment will show how HP issues (relevant to Safety) have been assessed, supported and/or mitigated to ensure that reliance on operators and human.

L.2.1 HP assessment overview

The Human Performance assessment is performed in SESAR as per the HP Reference Material [8]. Only an overview is presented here, just in order for safety practitioners to have an insight of the HP process.

The main HP arguments addressed in the Human Performance assessment approach are (The full HP arguments is included in Appendix A of the HP Reference Material):

- **Arg1:** The role of human actors in the System is consistent with human capabilities and limitations

- **Arg2:** The contribution of the human within the system supports the expected System Performance
- **Arg3:** Team structures and team composition support the human actors in performing their tasks
- **Arg4:** Human Performance related transition factors are considered

Based on those arguments, the process applied by the HP for the several lifecycle steps is summarised here after:

- **Step 1 - Understand the ATM concept :** Review reference material and identify changes
- **Step 2 – Define assessment scope, activities and planning**
 - Identify relevant HP arguments & activities
 - Identify HP issues, benefits and impacts
 - Define validation objectives, HP activities & expected evidence
- **Step 3 - Improve and validate the concept**
 - Perform HP activities and analyse and document outcomes
 - Formulate requirements and recommendations
- **Step 4 - Collate findings and conclude on the transition to the next V-phase**
 - Conclude the transition to the next phase
 - Produce an Assessment Report

The HP assessment performed following the HPRM method presented above could be conducted in order to substantiate in the safety assessment (as examples):

- the feasibility of operator actions;
- that task design and organisation, and operator support for the task will result in optimised HP;
- that all significant HP variability has been identified and that it can be demonstrated that it is mitigated through the application of good System design.

It should be remembered that the HP assessment process is not limited to consideration of the user interface but also addresses communication, selection, training and impacts of automation.

As stated earlier however, the operator is central to delivering Safety within the ATM environment and it must be very clear that the Safety assessment makes no calls on the operator.

The HP assessment process is to be applied by a HP practitioner who coordinate activities with the safety practitioner in charge of the safety assessment. Some of the tasks on which this coordination needs to take place are listed in next section.

L.2.2 Coordinating HP and SAF assessments

It is not possible to prescribe how HP activities should be integrated into every project and or Safety assessment. The precise requirements and depth of detail and analysis that is required will be dependent on the size, complexity and Safety aspects identified within the project. It remains therefore the responsibility of the relevant safety assessment lead and HP lead to determine the required level of coordination.

The aim of this Section is to describe the approach that could be taken to coordinate HP and Safety assessment. Information in the remainder of this Section describes typical HP activities that could be performed within each phase of design stages and how it relates to the Safety deliverables.

Planning Phase

The following bullets summarise the tasks for HP & Safety coordination at the planning phase (usually at V1, but not exclusively). This related to safety assurance activities presented in **Guidance A.1**.

- Scoping

Agreement and alignment on the concept and the assumptions associated with the Solution. This mutual understanding is best derived through preparation meetings with between HP & Safety before the scoping and change assessment, followed by joint attendance at the scoping and change assessment meetings (additional information is provided in **Guidance C**).

- Safety Criteria setting

Safety should work with HP in determining the human impact of the proposed changes. HP inputs should be taken into account by Safety when defining the Safety Criteria, allowing to ensure a complete set of SAC defined using the AIM model (additional information is provided in **Guidance C**).

- Planning activities

Derive and produce a HP and Safety plan that describe specifically what areas need to be investigated jointly from a Safety and HP perspective. Ensure that the plans are cross references to show what HP activities will provide for the Safety assessment process and vice-versa (additional information is provided in **Guidance C**).

Execution Phase

The following bullets summarise the tasks for HP & Safety coordination at the execution phase, for the activities performed at operational level, at design level, and those related to validation aspects. They correspond to safety assurance activities in **Guidance A.2, A.3 and A.4**.

At operational level

- Scenarios and operational conditions

A common understanding between Safety and HP is needed with respect to defining normal and abnormal conditions (of the operational environment) to be considered in the assessment.

- Operational services and Hazards

It has to be ensured that operational services and processes description defined by Safety are in line with high level tasks in case a task analysis is done by HP. With respect to corresponding operational hazards, as human behaviours might be assumed or revealed during their identification, common HP

and Safety workshops should be organised to discuss these hazards. Outcomes from this workshop should feed both the operational hazards identification and assessment, for the safety part, and the HP issues log for the HP part. Assumption should be subsequently tested within a validation environment and ultimately expressed as design requirements.

At design level

- Common description of the detailed tasks of involved actors

HP should ensure that Safety is aware of the outcomes of the analysis relating to roles, responsibilities and allocated tasks in normal and abnormal condition. Most importantly HP should communicate to Safety, where information necessary to successfully perform operational tasks is required

The Safety expert should ensure that each requirement relevant to operator is communicated to the HP specialist assigned to the SESAR solution.

- Assessment of human actions/error

Causal analysis of operational hazards has to include technical elements but also human related ones. More detail on this task is presented in section L.3.

- Specification of requirements

Where a demand is made on an operator to fulfil a Safety function, the necessary substantiation activities can be delivered by the HP specialist. Thanks to Safety and HP coordination in performing their assessment, a complete and coherent set of requirements is ensured at the end of the process.

With respect to Validation activities

- Planning validation activities

Safety and HP expert have to coordinate in order to define the complete set of Validation objectives relevant for each specific validation activity, as well as their corresponding success criteria. Scenarios to be addressed during the validation exercises need to be defined and prioritized in order to ensure that normal, abnormal and failure conditions are properly addressed. Finally, data to be collected needs to be defined and when possible common means to collect it has to be identified.

- Generation of evidence

Where a Safety requirement makes a demand on operational staff, then the actions required by the operator should have been substantiated by HP analysis. Thus evidence exists that the requirement can be fulfilled by the operator. Safety support to a Solution should ensure that the required evidence from HP is available in the validation exercise report.

L.3 Causal analysis of Operational Hazards – Human Error

The final purpose of the causal analysis of operational hazard is to derive safety requirements to satisfy their corresponding safety objectives.

The related SRM safety assurance activities are:

P5P6	A05	a1	Identify all potential causes of each operational hazard derived under Assurance objectives P3P4_AO2_ above (deductive analysis)
P5P6	A05	a2	Specify Safety Requirements (<i>Integrity</i> property from the failure approach) and / or Assumptions for the causes of each operational hazard, such that the Safety Objectives (and/or SAfety Criteria) are satisfied, taking account of any internal mitigation means.
P5P6	A05	a3	Capture all internal mitigations as either functional, performance or safety requirements (<i>integrity property</i> from the failure approach) or Assumptions, as appropriate

The operational hazards are identified and for each hazard a severity class and a Safety Objective (SO) have been allocated in accordance with the SRM principle (see **Guidance G**). The conventional Fault Tree for each operational hazard is produced; and the basic causes leading to top event are identified.

The safety related human tasks that interface with technical element are also to be identified. This is to be done in coordination with HP experts, with respect to the identification but also for evaluating the human mitigation effectiveness or reliability. The HP data from field experience and HP process outcomes are to be used to provide evidence of the appropriateness of the design.

The quantification of the human error is not required by regulation. Nevertheless, the production of best estimate Human Error Probabilities - HPEs for errors identified by screening process as being contributors to system risk is possible. A range of different techniques are available for that:

- Absolute Probability Judgement (APJ)
- Controller Action Reliability Assessment (CARA)
- Technique for Human Error Rate Prediction (THERP)
- Human Error Assessment and Reduction Technique (HEART)

More information on them HP Repository: <https://ext.eurocontrol.int/ehp/?q=taxonomy/term/101>

Another alternative method to deal with Human Error without quantification is called Hybrid Fault Tree. This method is presented in next section.

L.3.1 Hybrid Fault Tree method

This section summarises the Hybrid Fault Tree Method as a means address human error within the fault tree (causal analysis) without quantifying it. The full description of the methodology can be found at [16]. The term *hybrid* as used throughout this guidance refers to the use of both qualitative and quantitative means within a fault tree to apportion / allocate the quantitative safety objective from the top to the several qualitative and quantitative safety requirements.

The main lines of the Qualitative / Quantitative Allocation Process are described below.

1. Process Overview

The process of allocating criticality for lower level events follows standard fault tree processes where no human mitigation is present. Where a gate exists that considers human mitigation in one of the events directly below it the hybrid fault tree processes are used to determine the cascade of criticality from the top event to the lower level events.

In the example below F represents a fault condition in hardware, and H represents a human failure event.

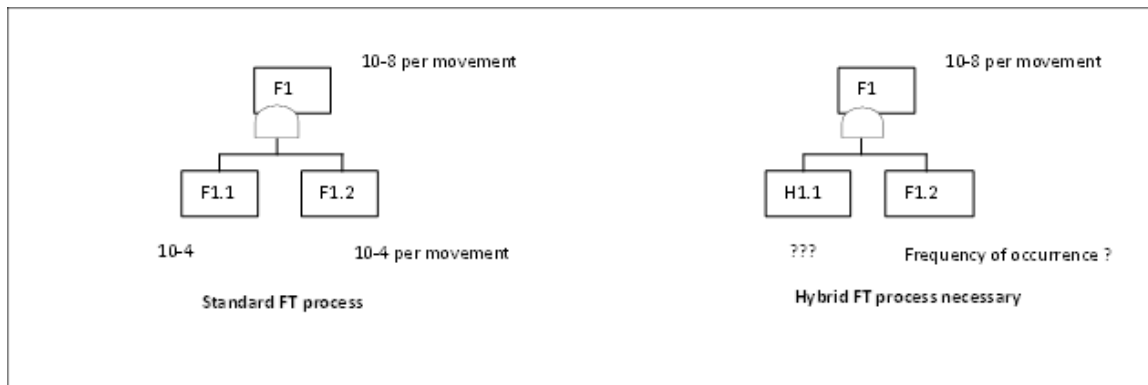


Figure 23: Example of a propagation of criticality for an AND gate

The relevance of the HP evidence and its quality drives the allocation.

The HF data from field experience that provides evidence that design of the functional system is efficient is to be used in evaluating the human mitigation effectiveness.

For new concepts, the HP assessment process is been carried out and the HP process outcomes are available for providing evidences of the appropriateness of the design.

Note that the evaluation of human mitigation effectiveness and the allocation of criticality in the fault tree based on this effectiveness is an iterative process that takes into account the evidences being providing all long the HP assessment process.

The main steps are:

- Step 1: Allocating criticality
- Step 2: Propagating criticality
- Step 3: Setting requirements for equipment elements
- Step 4: Setting requirements for Human tasks / procedures

2. Step 1: Allocating Criticality

The Level of Criticality is allocated based on the quantitative SO derived from the standard SO setting process in the SRM.

Level of Criticality		Frequency
Extreme Criticality	E1	$< 10^{-9}$ per movement
	E2	$< 10^{-8}$ per movement
High Criticality	H1	$< 10^{-7}$ per movement
	H2	$< 10^{-6}$ per movement
Medium	M1	$< 10^{-5}$ per movement
	M2	$< 10^{-4}$ per movement

Criticality		
Low Criticality	L1	$< 10^{-3}$ per movement

Table 11: Frequency & level of criticality

Conversion of the frequency of occurrence to different units is to be done as necessary depending on the different AIM metrics used to define the Safety Objective (per approach, per flight, per flight hour) and the needs of the project safety assessment.

3. Step 2: Propagating Criticality

Propagate the level of criticality of the top event in the Fault Tree down to the base events. The aim here is to determine a tolerable level of criticality for lower level event using a set of four principles.

The relevance of the HP evidence and its quality drives the allocation of one of four principles. Each of these principles provides an approach to allow consideration of a quantitative value for the technical part of a join human / equipment failure.

Rules

A set of rules are proposed in the hybrid FT method. They suggest an approach for preventing unsafe design and for “Downgrading” the Criticality level through the fault tree on the several elements based on the quality of evidence from the HP assessment.

Rule A – For an OR gate, the Level of Criticality of each “child” event shall be the same as the Level of Criticality of the “parent” event, except for OR Gate having 5 or more branches.

In this case, a higher Level of criticality is to be allocated to all the “children”.

Rule B – For an AND gate, the Level of Criticality of the “parent” event shall be propagated at child level provided the child events are independent and the human mitigation principles defined are applied with a possible downgrading of the level of criticality.

The mechanisms for this possible downgrading of the criticality are described in Principle 2, 3 and 4 applies

The approach can only be used to downgrade the criticality level to 1 class or 2 levels of criticality maximum.

Rule C – Rules above shall not prevent to propagate quantitative value when “quantitative” mitigations are duly justified.

A part from the rules presented above, a set of 4 Principles are also proposed in the hybrid FT method supporting the mentioned rules:

P1 – Preventing unsafe design

(P1a) No single human error should lead directly to an event defined as extremely critical

- (P1b). No flight crew / ATCO error combining with a maintenance staff error should lead directly to an event defined as extremely critical

Note related to P1b: the design of the maintenance procedures has to be included within the scope of the system design.

In this case P1 forms a design goal to minimise the contribution of human error to systems failure. It is not dependent upon evidence, it is a design goal, i.e. no evidence is required.

P2 – Evidence exists of the human contribution to safety

The human contributes positively to the safety objective; evidence is available and is of a high or medium quality.

P3 – No evidence for the human contribution to safety

The human may contribute positively to the safety objective, but no evidence is available or is of low quality

At the lowest level of the fault tree, if:

- A “Parent” event has a critically class which has been defined as extremely critical (E1) and that the “child” event for the Human element has been set with a HIGH level of evidence quality then the “child” event for the technical event will have to be defined as “HIGH (H1)” (e.g. criticality of the Equipment being two levels lower than the “parent” failure). Credit is taken for the human mitigation by two levels of criticality.
- A “Parent” event has a critically class which has been defined as extremely critical (E1) and that the “child” event for the Human element has been set with a MEDIUM level of evidence quality then the “child” event for the technical event will have to be defined as extremely critical (E2) (e.g. criticality of the Equipment being one level lower than the “parent” failure). Credit is taken for the human mitigation by one level of criticality
- A “Parent” event has a critically class which has been defined as extremely critical (E1) and that the “child” event for the Human element has been set with a LOW level of evidence quality then the “child” event for the technical event will have to be defined as extremely critical (E1) (e.g. criticality of the Equipment being at same level than the “parent” failure). No credit is taken of the human mitigation.

P4 – A change that affects behaviour, but is not a result of equipment

Human Mitigation principle (P4) is defined in order to consider a change in the operational concept that is based on existing equipment: .e. g. a new procedure to be followed by pilots or controllers which requires no technical system changes.

In this case, there is no requirement for new equipment, in the ground or in the air. Changes are likely to impact most heavily on procedures and training. In this case, the HP assessment is expected to provide detailed insight, not only into the requirements for training and changes to procedures, but also that the change has been:

- Analysed,
- Assessed; and
- Demonstrated to be effective in a real or simulated setting.

P4 provides the opportunity to complement the existing top down approach for with a bottom up approach. These two complementary approaches are considered in this Hybrid Fault Tree methodology. The top-down approach is for designing an ATM/ANS functional system which implements new technical design and the bottom-up approach is for designing an upgraded ATM/ANS functional system which uses existing technical design.

The P1 to P3 principles apply to the top-down approach while P4 applies to the bottom-up approach.

4. Step 3: setting requirements for technical elements

The quantitative requirement is established in terms of maximum probability of occurrence using the same unit of measurement for both the airborne and ground technical elements. When direct quantification is not possible, quantitative requirements are based on the allocated level of criticality. The qualitative requirement is established as per the current quality assurance practices for airborne and ground technical elements. E.g. for an extreme criticality – the quantitative requirement at E1 would be “< 10-9 per *AIM Metrics*”.

This step is further described in [16].

The qualitative requirement for the software (and development process for the airborne equipment) is established as per the current quality assurance practices for the airborne and the ground technical elements.

The same AIM metrics (units of per approach, movement, fight or flight hour) as determined in Step 1 for the top event operational hazard are used to express the quantitative requirements for the equipment / system failure; together with an agreed unit conversion formula to properly allocate the safety requirement of the ground equipment / system when supporting Air Traffic Services.

Depending on the Accident Type (AIM Model) the SESAR solution is associated with, the metrics used to set the MTFoO values are of different units. Conventionally, the unit used for En-Route & TMA is: per Flight Hour, for Surface it is: per movement but it may be in different ways using conversion factors between the metrics. The conversion factor is not fixed; it is normally adapted for each SESAR solution within its targeted environment.

Further detail on this process is described in [16].

5. Step 4: setting requirements for human tasks / procedures

This step allocates the qualitative requirements for human tasks/procedures to achieve the top level safety objectives. The process is driven by considering the availability and quality of evidence from the human performance assessment that has been conducted in support of the design project.

Evidence from the HP assessment should be directly relevant and sufficiently detailed to provide clarity on the failure being investigated in the fault tree. This provides a measure of Evidence Quality (EQ) of High (H) Medium (M) or Low (L). Where evidence is not considered relevant or of sufficiently high quality, i.e. it does not address all the areas of interest to safety, it should not prevent the safety expert requesting further information from the HP Assessment team.

The relevance of the HP evidence and its quality drives the allocation of one of four principles. Each of these principles provides an approach to allow consideration of a quantitative value for the technical part of a join human / equipment failure.

HP evidence is considered as follows:

- HP evidence should have arisen from a HP evaluation or observation.

- An EQ judgment is possible from an analysis of the HP assessment as judged by the safety specialists.
- An EQ judgment is possible and reflects the effectiveness of the assessed or observed mitigation by human actions. The EQ shall be judged high, medium or low in terms of quality of the evidence for the effectiveness to the proposed solution / design.
- High quality evidence from HP Assessments (well written, well analysed, complete etc.) that do not demonstrate the effectiveness of the proposed human mitigation actions shall not permit a down grading of criticality.
- On the airborne side, risk reduction results from observation containing commonly agreed quantification (e.g. figures from ICAO docs).
- On the ground side, risk reduction may result from formal methods, expert judgment or previously agreed values.

More detail on the derivation of the standard and source of Evidence is presented in [16].

Content of the HP Assessment	EQ	Guidance for HP Requirement
The assessment found evidence of a highly effective concept present in the design which specifically addresses the human component of the issue	High	Adequate System Design Procedures and training of the human operator in the specified task is sufficient to achieve the safety objective
The assessment found evidence of an effective design or a request for change in concept related to the issue.	Medium	Adequate training of the human operator in the specified task coupled with associated adequate mitigation means is sufficient to achieve the safety objective
The assessment found no evidence concerning design effectiveness relating to the issue. Open issues and /or Assumptions requiring further attention and validation are described in the HP report.	Low	Further validation is required to address Open Issues and Assumptions to achieve the safety objective.

Table 12: HP Assessment Evidence Quality considerations

6. Closing remarks

In identifying and assuring the human actions/factors required to deliver Safe operations, the assumption and inherent design constraints (requirements) can be captured within the Safety assessment process and the resulting Safety Case. It is necessary therefore for the Transversal Activities to identify areas of operation where Safety may be impacted by the “human” factors of the system. Similarly, where Safety identifies areas where Safety is delivered as a function of the operator, these functions need to be substantiated by the Transversal Activities. This guidance has explained how the Safety-related issues, from HP analyses, might be integrated into the Safety Lifecycle. In addition, this guidance has summarized the so-called Hybrid Fault Tree approach to dealing with human errors in fault tree when several elements will not be quantified.

Guidance M On gaining safety insights in real-time simulations

M.1 Introduction

Real-time human-in-the-loop simulations (RTS) are intensively used in SESAR to support the validation of the changes brought to the ATM/ANS functional system. Consequently, gaining safety insights from real-time simulations (RTS) is very important to support the collection of safety evidence that a designed Solution is fulfilling its Safety Criteria which will ultimately support the demonstration that the significant increase of safety (3-10 fold) could be achieved with SESAR 2020.

This Guidance should be used to determine specific safety validation objectives, success criteria and associated means for their demonstration (questionnaires, debriefings, observations and measurements where appropriate) relevant to a validation exercise based on a real-time human-in-the-loop simulation (RTS).

This Guidance provides support to determine the requirements for safety insights with the expectation that those requirements will be appropriately captured by Validation Plans and measured against during validation exercises based on RTS. This in particular addresses the expectations as per safety assurance activities:

P3P4	AO_C&C a1
P5P6	AO5 a4
P5P6	AO7 a1
P5P6	AO_C&C a1
P7	AO_C&C a1

as per Guidance **A.2**, **A.3** and **A.4**.

M.2 About the usage of real-time simulations in validation

Real-time simulations occur mid-way until late in the concept development life cycle (*i.e.* a detailed stage of design at which at least provisional controller procedures and working methods have been developed, and at least a preliminary working HMI exists).

Real time human-in-the-loop (HITL) simulations are a flexible approach, able to address airspace design, new automation tools and concepts, controller working methods and Human-Machine Interface (HMI) design for example. Real time simulations are also particularly useful in examining impacts on controller performance.

Real time simulations are less used for software and hardware evaluation, because firstly other methods are available and more efficient, and also simulation 'platforms' are themselves usually a simplified abstraction of the real system, so can only test hardware and software aspects in principle or functionally. Nevertheless, they are good overall tests of an ATM/ANS system, able to confirm benefits and/or find problems in the intended system architecture and implementation. For this reason often large-scale tests may be carried out on site, in a simulation facility at or adjacent to an air traffic control centre. If a system is tested in the centre itself, this constitutes either a 'shadow-mode trial' (controllers using the system are not in control but are 'following' live traffic), or else it can be an actual 'live trial' in which the new system is actively used to control/monitor traffic. In both of these cases, there must be an assessment of the safety of the trial itself, so that the trial cannot induce

Founding Members

actual incidents or reduce the real system's ability to respond to actual incidents during or after the trial (see more information under **Guidance N**).

M.3 Purpose of this Guidance

This Guidance describes a process to make measurements and derive safety insights during SESAR real-time human-in-the-loop (HITL) simulations. It is important to note that techniques/tools can be brought into play in order to collect relevant evidence about safety achievements (level of safety performance, requirements, etc.). The process involves both:

- The measurement of the controller safety-related performance when faced with specific safety-related events (e.g. hazards, abnormal conditions) in a simulation,
- General safety monitoring using less intrusive procedures to see if any safety-relevant information arises during a real time simulation, and
- The generation of evidence of safety performance arising from post-processing trajectory data (flight plans, plot data) from simulations and which relate to:
 - Analysis of the air traffic controllers' interventions and the impacts of supporting automations on separation management performance – with a focus on SESAR validation exercises related to Advanced Air Traffic Services in En-route and TMA and those related to Enhanced Runway Throughput (final approach & initial departure).
 - Potential Airspace management & configuration or network operations' impacts on safety – with a focus on SESAR validation exercises related to optimising the ATM Network Services (Dynamic Airspace Configuration, Optimized Airspace User Operations, Demand & Capacity Balancing, etc.)

M.4 Process Steps and measurements

The process steps and the proposed safety-related measurements are as follows:

Step 1: Determine whether there are specific safety validation objectives for a simulation – these may arise from:

- A hazard analysis (e.g. particular operational hazards that are of concern and may be seen during a simulation);
- Safety proxies, *i.e.* relevant safety performance indicators that can be used to demonstrate the achievement / achievability of the Safety Criteria (SAC);
- Safety Objectives (success approach) and/or Safety Requirements (functionality & performance), which must be measurable and can be demonstrated in validation exercises
- Other sources (e.g. review of operational incident data or controllers' opinion about pertinent safety issues).

Step 2: If there are specific safety-related events of interest for the simulation these must be related to the simulation environment and objectives, to see how they can be integrated into the overall simulation plan (VAL Plan for the relevant Solution) and its execution. This will lead to the definition of specific safety events or scenarios that must occur during the simulation in a planned and measurable fashion, less intrusive observations and/or post-processing of simulation data. Examples of safety events could be failure of or 'bad data' provided by a new controller supporting tool, or adverse weather events, or pilot error. If there are no specific safety events of interest, then a standard set of general safety-related measures can be applied to the simulation (see **Step 3** below).

Step 3: Measures must be chosen for the simulation that will allow safety conclusions or at least insights to be drawn. General measures include automatic monitoring of reductions in standard ATM-relevant safety proxies (e.g. losses of separation; runway incursions; safety nets activation, etc.) via automatic event logging systems. Such approaches may also be facilitated by controller self-report and simulation observer report. The means for such reporting are the standard debriefs and questionnaires after each exercise and at the end of the simulation, which should include general safety-related questions. For more safety-related-event oriented simulations (e.g. considering the potential impacts of a hazard on situation awareness, workload or teamwork, tools to support improvement of controller productivity, change of paradigm of ATC in Enroute and TMA) more specific measurements will be used.

For all measures, it must be decided in the VAL Plan how the measure will be administered, the expected direction of the effect, and how to analyse the measure, and the safety criterion (qualitative or quantitative) from which to judge the extent of the impact. In a number of cases this may include the need for a classification of the severity (e.g. for losses of separation), for counting specific controllers' interventions, etc. In other cases the measures may be more subjective or interpretative by the simulation 'experimenters' e.g. interpretations of workload or situation awareness impacts on safety.

Step 4: The simulation is then run. For general safety measurements, there may be a need for debrief and clarification sessions with the controller subjects. For more focused measures these debriefing sessions (with single controllers or multiple controllers) may be expected to be more intensive. In other cases, post-processing of data from simulations might generate evidence of safety performance. Some measures (e.g. situation awareness or physiological measures) may be more 'intrusive' in that they may actually require a short temporary interruption of the simulation itself whilst key questions or measurements are taken. In the case of psycho-physiological measurements (e.g. heart rate, eye movement tracking, electro-dermal activity, etc.) the measures may not actually interrupt the simulation but the controller will be required to wear monitoring equipment. In all such cases the impacts of the measurement methods themselves on behaviour must be assessed to determine how they affect the validity of the safety-related results.

Step 5: Analysis and determination of safety insights then occurs. This should usually lead to a conclusion that safety as evidenced in the simulation and/or from post-processing of simulation data, was:

- either enhanced, degraded, no change occurred,
- or the measure/simulation/scenario was insufficiently sensitive to the intended safety aspect being investigated,
- or finally that the observed change was an artefact from the measure itself (and therefore may not appear in a real situation).

Such safety insights or evidence require careful interpretation as well as operational support in analysing the outcomes from data processing. In particular, for hazards that are 'fed into' the simulation the controller reactions may differ from reality, as these events will often have a far higher occurrence rate in the simulation than in reality and the controller reaction would involve less stress than in reality.

Secondly, in terms of errors or events that 'arise' during a simulation (i.e. they were not pre-planned into the simulation), it must be remembered that these safety-related events may sometimes occur more easily in simulations than in reality, due to lack of familiarity of controllers with the simulation and scenarios (e.g. HMI, new concept and airspace unfamiliarity), and also simply because it is 'just a

simulation’ and so controllers may act less safely than when handling real traffic in the controllers’ normal working environment. This does not mean that observed events (e.g. controller errors) are artificial, but rather the ‘rate’ may be significantly higher than in normal activities. As an important counterpoint to this potential ‘bias’ however, if an event predicted as possible (e.g. a human error) does not appear during a simulation, it does not mean it will never appear in reality.

Whilst a typical simulation is always a substantial test of a system, allowing to provide relevant evidence with respect to the operational safety (e.g. capability of ATCOs to deal safely with a certain amount of traffic whilst operating as per the new Solution), it will not allow reliable safety measurements in relation to rare events (e.g. less than one in a thousand in terms of anticipated likelihood). Care is therefore needed in drawing conclusions from simulations to inform the Solution safety assessments and eventually the safety case conclusions. Real time simulations can provide important insights for safety cases, but will not always be definitive. This is why this Guidance deals only with ‘Safety insights in simulations’ – because a simulation can rarely be exhaustive due to practical limitations (simulation costs and availability of controllers), and so it is insufficient as a means to judge safety conclusively when considering rare events. Nevertheless, the controller reactions and experiences associated with such simulations and/or post-processing of simulation data can lead to important insights about safety of the concept being simulated, the achieved safety performance and associated errors and failure-recovery paths. These experiences can still inform the safety of the Solution, and can lead to the derivation of additional safety requirements (e.g. training and procedural improvements).

Step 6: Safety insights are fed into the safety documentation for the involved Solution. This covers the VAL Report and the Safety Assessment Report. Moreover, any new or modified safety requirement as a result of a validation exercise outcome will be included in the SPR-INTEROP/OSED and/or TS documents.

Guidance N Safety Management of VLD: an ANSP and Network Manager perspective

N.1 Objectives

When used in conjunction with the existing Final Guidance Material to Execute Proof of Concept [14], this guidance provides, as a recommendation, a clear, complete, coherent and integrated approach to the safety assessment of Very Large Demonstrations (VLD) to the participating providers of air navigation services (Network Manager and Air Navigation Service Providers (ANSPs)).

It has been produced in response to providers of air traffic services' requests for a guidance supporting a formalised, explicit and proactive approach to the systematic safety management of VLD thereby meeting their safety responsibilities within the provision of their services

It seeks neither to replace nor replicate [14], which main focus is on the collaboration and mutual linking between national authorities, providers of air navigation, manufacturers and airspace users involved in the VLD with the aim to support a co-ordinated certification / approval process. Rather it is intended to provide a theoretical and practical guide to safety assessment and assurance to the participant air traffic service providers who have to discharge their safety responsibilities properly and also provide an adequate level of safety assurance to obtain the necessary regulatory approval for the conduct of a VLD from their Competent Authorities (NSA and/or EASA).

The material is intended to apply to the full range of VLDs in SESAR 2020. Having said that, it is not intended to be prescriptive – rather it may be adopted and adapted for particular VLD applications as appropriate and necessary; in particular the guidance includes in **N.5** some criteria to assess the significance of the VLD and, as a result, enables a proportionate approach to the safety assurance of the VLD.

N.2 Introduction

The Very Large Scale Demonstrations cover the final part of SESAR 2020 Research and Innovation (R&I) Pipeline, as from TRL 6 to TRL7, as shown in Figure 24 below:

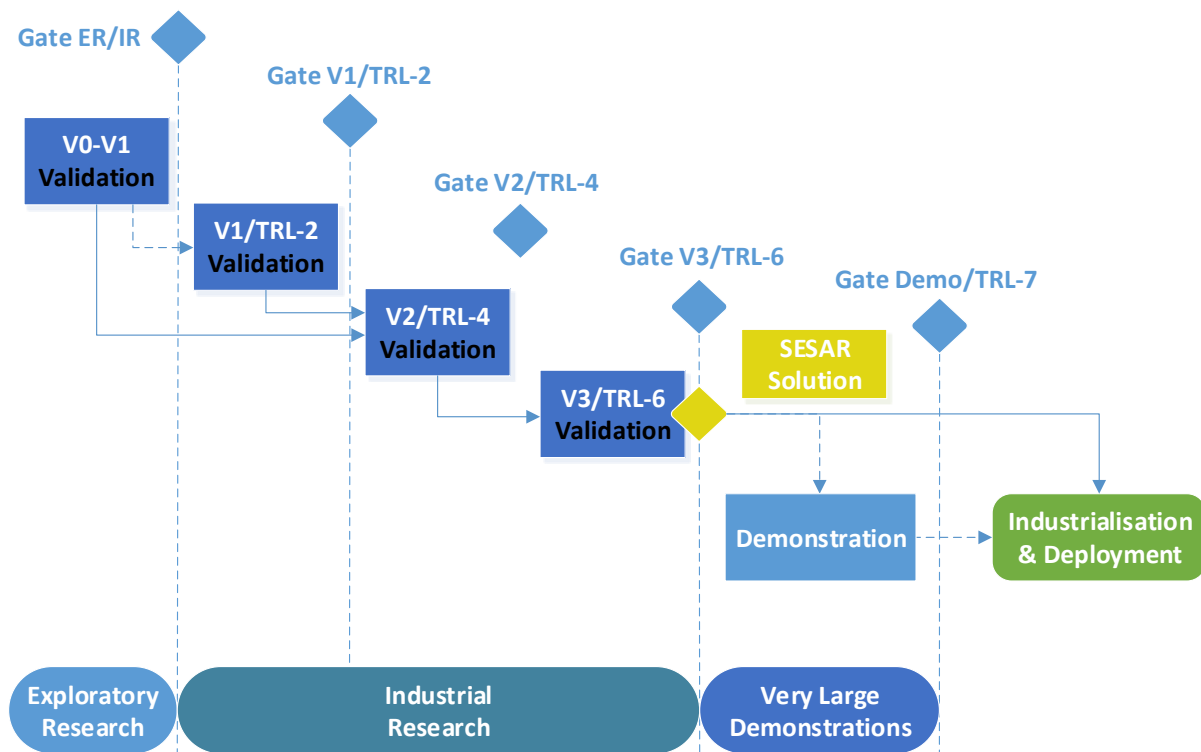


Figure 24: Gates and phases of SESAR Solution development life cycle

The Very Large Scale Demonstrations (VLD) are designed to help to fill the gap between the development and deployment phases.

The Proof of Concept (PoC) to be conducted under a VLD is a confidence building exercise that comes in addition to the traditional validation required prior to certification and implementation of new concepts or new technologies. This has to be distinguished from operational live trials since it brings a new dimension of the validation, that is, early operations with a significant scale environment.

The PoC consists of an early operation of a SESAR solution making use of pre-operational or operational products (airborne and ground) in a real operational environment. This includes the preparation and platform availability (ground and onboard) to support the demonstration in the targeted operational environment involving target audience end-users.

Notwithstanding the fact that a VLD is effectively a ‘technology’ demonstration, it still implies that ‘not fully tested’ ‘technology’ will be instantiated into operational – ground based and airside – Systems. The VLD must, therefore, be managed with safety as the primary concern. This includes both that the VLD delivers the required evidence to support the ongoing implementation of the concept being trialled and that the demonstration itself is conducted safely. Consequently local safety assurance activities which need to be conducted to support the VLD are an essential part of the VLD safety demonstration. Both the local safety assurance and approval process are not necessarily within the remit of the SRM but material generated by the SRM process and the SRM per se provide practical guidelines to assist.

N.3 VLD safety assurance

The main objective of the safety demonstration is to show that ATS operations during the VLD which might include participating and non-participating flights are acceptably safe. The definition of what is acceptably safe must be defined for each VLD but it generally means that the already defined Safety Criteria relative to the SESAR Solution under VLD should be satisfied and that safety level of current ATS operations in the relevant airspace/airport is at least maintained when VLD are conducted.

To support this objective, the VLD safety assurance activities are twofold:

- i. Suitability of the SESAR Solution for the deployment:
 - ✓ The Solution under VLD delivers the foreseen safety performance for the required application/operation; and
- ii. Safety Impact of the VLD on current operations:
 - ✓ The VLD does not degrade to an unacceptable level the safety of the operations (e.g. with other surrounding operations and/or components of the ATM/ANS System)

As a result, the specific activities that must be considered are:

1. Solution readiness for VLD by documenting the current safety assurance status in order to make a decision on approval to move a SESAR solution from a pre-industrialization stage to a 'ready for VLD' status. This includes ensuring that the findings of the safety assessment at V3 are fully accounted for and any safety issues not adequately addressed in the Solution System design are managed and adequately mitigated in the design of operational procedures, equipment and training before the VLD takes place.
2. Enabling the use of VLDs as a new dimension in the validation approach and providing further evidence as a support to standardization. This includes, but is not limited to, (i) building and evaluating the physical Solution System against the final system design in V3; (ii) the setting of appropriate safety validation objectives; and (iii) as a result preparation and availability of the VLD validation platform (ground and onboard) to support the demonstration of the achievement / achievability of the safety validation objectives and safety requirements;
3. Enabling significant levels of engagement and co-ordination of both the end-users (e.g. ANSPs, Network Manager, airports; airspace users, etc.) and appropriate Competent Authorities (National Authorities (NAAs; NSAs) and/or EASA) as fully detailed in [14].
4. Determining and documenting in a VLD safety Plan (Appendix of the VLD DEMO Plan) the safety assurance to be conducted for the VLD encompassing the suitability of the SESAR Solution for the deployment and the safety impact of the VLD on current operations; and finally;
5. Documenting the VLD Safety Case within the VLD DEMO Report. The VLD Safety Case is here a means of structuring and documenting a summary of the results of a VLD Safety Assessment addressing the suitability of the SESAR Solution for the deployment and the safety impact of the VLD on current operations.

N.4 The VLD Safety Plan

The VLD Safety Plan (Appendix of the VLD DEMO Plan) specifies, inter alia, the safety assurance activities that are to be carried out in order to create necessary and sufficient Evidence for the production of the VLD Safety Case. The Safety Plan should:

- a) Determine the SESAR solution readiness for VLD

- b) Determine the scope and boundaries of the VLD safety assessment / safety case
- c) Develop the specific Safety Argument from the generic example herein (**N.5**)
- d) Develop the associated Safety Assurance activities based of the VLD safety argument
- e) Assess the resources and skills needed to execute the Safety Plan
- f) Determine the safety organisation for the VLD project, and the roles and responsibilities of the personnel, departments and organisations involved in the execution of the Safety Plan
- g) Schedule the Safety Assurance Activities in line with the resource requirements / availability and any dependencies
- h) Determine the safety-regulatory arrangements for the project on the basis of [14].

N.5 Structuring the VLD Safety Case – generic guidance for ANSPs / NM

This section provides guidance on the development of Safety Cases as a means of structuring and documenting the demonstration of the safety of a VLD. It provides a generic example of a structured Safety Arguments for a VLD. The argument should be structured as follows:

1. It must start with a top-level statement (Claim) about what the VLD Safety Case is trying to demonstrate in relation to the safety of the relevant SESAR Solution(s). The Claim must be supported by:
 - a. The safety target, which define ‘what is *safe*’ in the context of the VLD. This safety target should include the relevant Safety Criteria (SAC) for the Solution plus any specific criteria relative to the safety impact of the VLD on current operations (e.g. safety level of current ATS operations in the relevant airspace/airport is at least maintained when VLD are conducted).
 - b. The Justification for introducing the changes brought by the VLD to the service or system concerned
 - c. Operational Context for the Claim
 - d. any fundamental Assumptions on which the Claim relies
2. The decomposition of the Claim into the following lower-level:
 - a. The suitability of the SESAR Solution for the deployment. This includes:
 - i. Showing that the Solution(s) technical system, procedures (for controllers, pilots, operational engineers and maintenance staff) and training (for the same four groups) satisfy their respective safety requirements (from V3) and that all three components are shown to operate correctly. This includes evidence:
 - That the SESAR Solution(s) design has reached V3 maturity level and any finding affecting safety have been addressed

- Of the tailoring of the V3 Safety Assessment Report (SAR) to the VLD local 'implementation' incl. the Operational Environment (OE) and the completeness of the definition of normal / abnormal conditions
 - That the implemented design of the technical system under VLD (*i.e.* equipment) satisfies the safety requirements that were derived at V3 level and any emerging properties of the implemented design have been analysed
 - That the operational procedures to be used for the VLD (ATC, Flight Crew, technical staff) satisfies the safety requirements that were derived at V3 level, are addressing the specificities of the implemented design for the VLD and have been promulgated
 - That the training/briefing of the different operational (ATC, Flight Crew) and technical staff (e.g. maintenance) satisfies the safety requirements that were derived at V3 level, are addressing the specificities of the implemented design for the VLD and have been delivered
 - That the installation and commissioning / evaluation of the complete Solution(s) System have been carried out; then it can be argued that the SESAR Solution design for the VLD has been implemented completely and correctly
- ii. Defining appropriate safety validation objectives to show that the safety target (incl. SAC and/or proxies) are met; validation objectives have to be commensurate to the time exposure and scale of the VLD (duration of the VLD, number of aircraft involved,...);
 - iii. Defining and implementing appropriate means to measure those indicators; this includes the preparation and the VLD platform availability (ground and onboard) to support the demonstration in the targeted operational environment involving target audience end-users measure and analysis. This is addressed in sections 8.2 and 8.3 of **[14]**.
 - iv. The appropriate definition of start / stop criteria/procedures with respect to the VLD incl. requirements (means: equipment, staffing, etc.) and procedures for reversion. In addition to START/STOP criteria, following aspects should be considered:
 - Need for temporary AIP and/or NOTAM
 - Special approvals that are required (wrt targeted airspace users)
 - LoA between involved ANSPs including but not limited to any airspace or traffic limitations that may need to be implemented while running a VLD in an operational environment

- b. The safety impact of the VLD on current operations. This includes:
 - i. Showing that VLD will not degrade to an unacceptable level the safety of the ATS operations in participating locations and for participating and non-participating flights and
 - ii. Showing, if relevant, that VLD will not degrade to an unacceptable level the safety of the ATS operations in non-participating locations.

N.6 End-users & Regulatory Authorities: engagement & co-ordination

This is fully described in [14] and consequently not replicated here.

Guidance O Technological Solutions

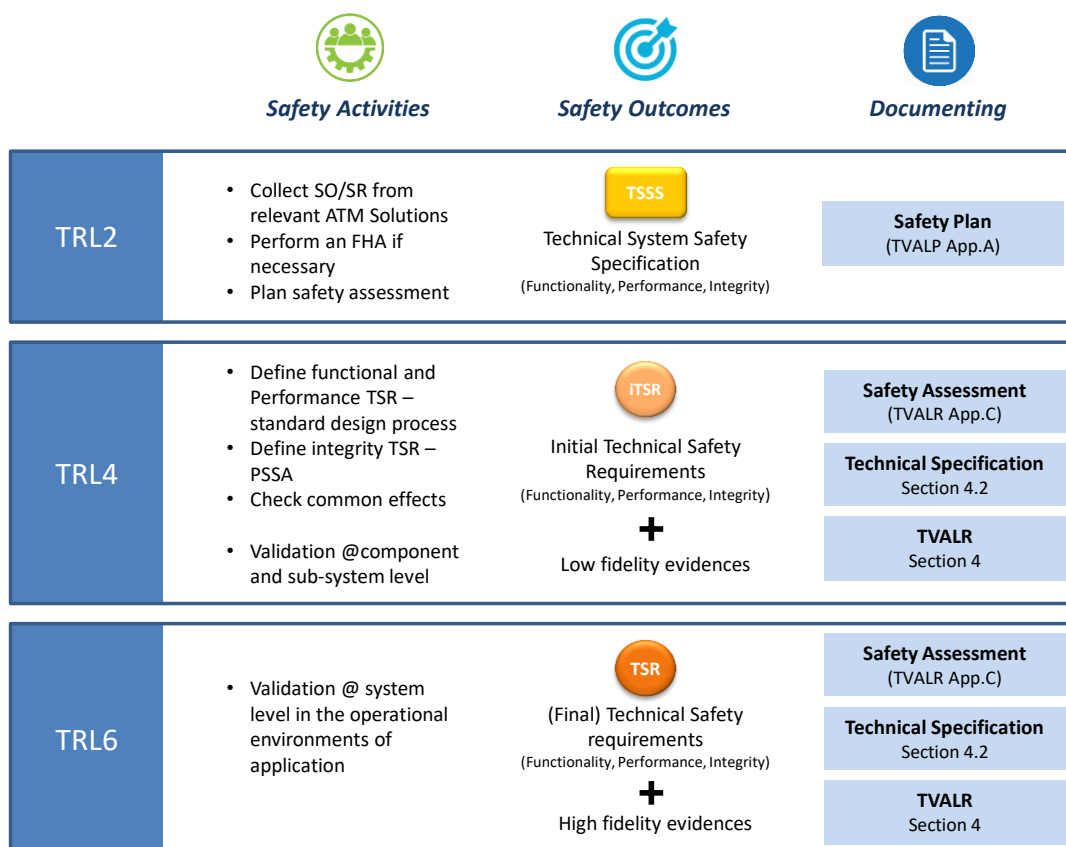
O.1 Why Technological Solutions need a dedicated Safety process

The SESAR Safety References Material – SRM describes the safety approach to be applied in SESAR in order to ensure that safety is integrated in the design of the several SESAR concepts and to perform the corresponding safety assessment. Despite the approach in the SRM covers all the Solutions in SESAR 2020, the SESAR SRM Guidance A mainly provides guidance for the safety assessment to be performed by ATM Operational Solutions, as they are the ones having direct operational consequences with safety implication (i.e. accidents and operational incidents seen by the airspace users). The safety process to be applied by the Technological Solutions is then an extension of the one applied by the Operational ones, in which the outcomes from the ATM Operational Solutions will define the System Safety Specification for the Technological Solutions, i.e. the starting point for their safety assessment defining how safe the technical system needs to be with respect to its operational use.

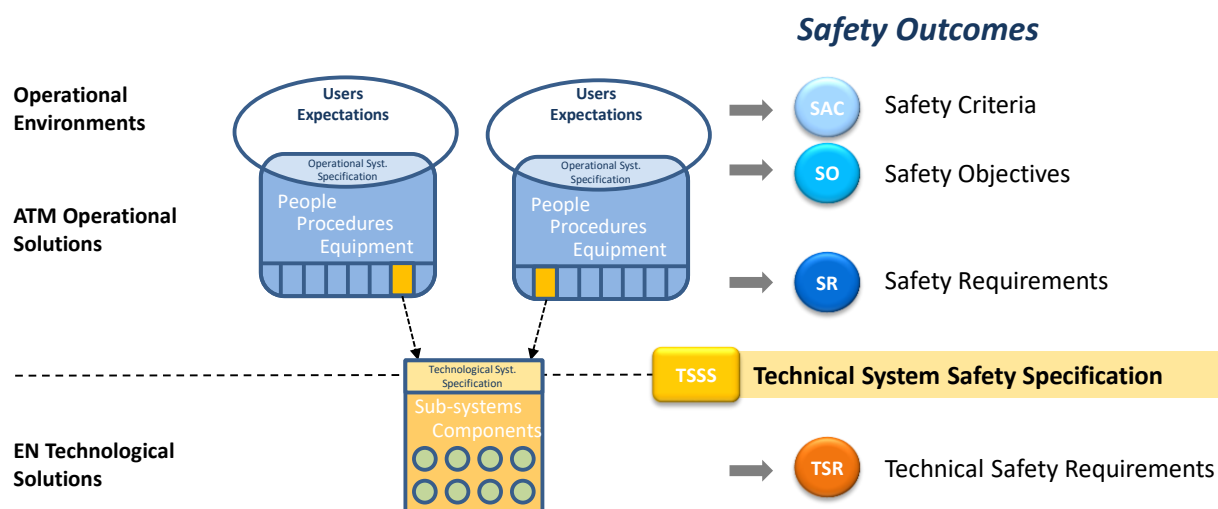
This guidance describes then the safety process to be applied by the Technological Solutions as well as the link with the activities described in the SRM for the operational concepts.

O.2 Overview of the process and link with SRM activities/outcomes

The following figure shows an overview of the safety process to be applied for the Enablers Technological Solutions. The detail of this process is provided in section **O.3** of this guidance.



The relationship between the safety process shown above and the safety assessment performed by the ATM Operational Solutions is illustrated in the figure below:



In most cases, technological systems provide data services to ATM systems and / or, in some cases, directly to Airspace Users. Therefore, the *Specification* can be expressed in terms of the data provided according to its required properties such as (note that this list is not exhaustive) :

- type
- scope / applicability
- format
- interface protocols
- accuracy
- resolution
- latency / refresh rate
- integrity
- etc.

These properties are to be defined by the service users (i.e. the corresponding ATM Solutions), through their corresponding Safety Requirements or Safety Objectives (as relevant). Then they can be considered to be the **Technological System Safety Specification – TSSS** without further modelling or analysis being required.

Additionally, maximum use should be made of existing standards (including ICAO Annexes) in developing these safety properties as relevant.

O.3 Description of the safety activities to be done per TRL and the corresponding expected outcomes

O.3.1 TRL2 - Technological concept and/or application formulated

Once basic physical principles are observed and translated into applied research and development, then at the next level of maturation, practical applications of those characteristics can be 'invented' or identified. At this level, the application is still speculative: there is not experimental proof or detailed analysis to support the conjecture.

TRL2-SAFETY ACTIVITIES

OUTCOMES - DOCUMENTING

2.1. Understand the basic principles of the technological concept, including its safety implications, and define the scope of the safety assessment <i>Note: This activity is related to safety activity P1-AO1-a1 in Guidance A.1. Additional guidance is provided in Guidance C.1.</i>	Description of the technological concept and its safety impact
2.2. Identification of the practical operational applications for the technological concept <i>Note: This activity is related to safety activity P1-AO2-3-a1 in Guidance A.1. Additional guidance is provided in Guidance C.1.</i>	
a. Identify the relevant ATM operational Solutions in which the technological concept is to be applied	List of operational applications
b. Additionally or in case no ATM operational Solution (or outcomes) is available, define the application of the technological concept based on Subject Matter Expert - SME	(Additional) List of operational applications
2.3. Definition of the Technical system safety specification <i>Note: This activity is related to safety activity P2-a1 in Guidance A.1. Additional guidance is provided in Guidance C.1.</i>	
a. From the identified ATM operational Solutions, select the relevant Safety Requirements - SR related to the Technological concept (in some cases Safety Objectives - SO might be more relevant). In case of different requirements concerning the same function and characteristic are collected, a reconciliation process is to be applied in order to ensure that the most critical one is retained. This set of Safety Requirements becomes the system safety specification for the design of the technological solution.	Technical System Safety Specification (including functional, performance and integrity characteristics)

b. Concerning the additional operational applications not (appropriately) covered by an ATM operational Solution: • Based on the identified operational usage of the intended functions (using operational expertise), define the intended functions for those cases (what the technological solution has to provide in terms of functions) • Based on SME or existing standards, define the corresponding performance required for each intended function • Perform a Functional Hazard Assessment - FHA for those intended functions in order to define the corresponding integrity required for each intended function. This is to be done following the same process as the Operational Hazard assessment described in the SRM, i.e. using the Risk Classification Schemes proposed in Guidance G. Note: this FHA should be performed then with the support of SME familiar with each operational application considered; due to the fact that the assessment will be limited, all the assumptions made during the assessment need to be documented and validated (specifying the integrity characteristic at which the intended functions have to be provided, plus any additional safety function requested to mitigate identified risks based on the FHA). Note: depending on extend of this task, this activity can be performed in TRL4 delivering at that stage the Complemented TSSS. But in this case this activity (and the corresponding tasks and resources to perform it) needs to be described, planned and documented in the Safety Plan (as per safety activity 4 and 5 below).	(Complemented) Technical System Safety Specification (including functional, performance and integrity characteristics) Note: the Complemented TSSS can be delivered in TRL4, but only in case an initial TSSS is already delivered in TRL2.
2.4. Plan the safety activities to be performed at the technological/enabler level and identify the required safety resources to perform the safety assessment Note: in case safety activity 2.3.b needs to be performed, corresponding activities for this task also need to be identified, described and planned. <i>Note: This activity is related to safety activity P2-a2 in Guidance A.1. Additional guidance is provided in Guidance C.1.</i>	List of activities to be performed for the safety assessment and people involved (with corresponding responsibilities)

2.5. Document the outcomes from previous actions in the safety plan	Safety Plan for Enabler Solution in TVALP Appendix A
---	--

O.3.2 TRL4 - Component and/or breadboard validation in laboratory environment

At this step in the maturation process, active research and development (R&D) is initiated. This must include both analytical studies to set the technology into an appropriate context and laboratory-based studies to physically validate that the analytical predictions are correct. These studies and experiments should constitute "proof-of-concept" validation of the applications/concepts formulated at TRL 2. Following successful "proof-of-concept" work, basic technological elements must be integrated to establish that the "pieces" will work together to achieve concept-enabling levels of performance for a component and/or breadboard. This validation must be devised to support the concept that was formulated earlier, and should also be consistent with the requirements of potential system applications. The validation is "low-fidelity" compared to the eventual system: it could be composed of ad hoc discrete components in a laboratory.

TRL4-SAFETY ACTIVITIES

OUTCOMES - DOCUMENTING

1. Ensure that the sub-systems and components of the technological system defined by the Technological Solution and the interactions/links between them – (following standard system design process) is complete in order to capture any safety aspect related to the technological concept.	Technical system Functional architecture in the Technical Specification document – Section 4.1.
2. For each functionality or performance requirement of the Technical System Safety Specification (from TRL2-activity3), define at the level of each component what it is required to fulfil in terms of functionality and performance (following standard system design process).	Initial set of Technical (Safety) Requirements @ component / sub-system level (success approach part)
3. For each requirement of the Technical System Safety Specification related to integrity, perform a Preliminary System Safety Assessment – PSSA in order to define at the level of each component what it is required to fulfil in terms of integrity and additional functionalities (note that any requirement related to integrity addresses a feared event which causes need to be analysed and the related risk needs to be assessed and mitigated through the PSSA).	Initial set of Technical (Safety) Requirements @ component / sub-system level (failure approach part)
4. Any potential for common cause in terms of a component failure that could invalidate multiple Technical System Safety Specification (the most critical case being the one where an affected requirement at operational level represents a risk mitigation for a second affected requirement).	Validated Technical System Safety Specification with respect to common effects from the technological system.

5. Document process and outcomes from activities 2, 3 and 4 in the Safety Assessment Report	TVALR Appendix C – Safety Assessment Report
6. Planning Validation activities:	
a. Define relevant safety Validation Objectives with respect to laboratory based studies performed to provide evidences on the validity of the Technical (Safety) Requirements @ component level (they can be achieved and physically implemented)	TVALP Section 4.3 and 5.1.3
b. Define relevant safety Validation Objectives with respect to initial validation activities performed to ensure that the several components together / sub-systems will provide the corresponding intended function and performance expected for the Technological system	TVALP Section 4.3 and 5.1.3
7. Based on validation activities outcomes:	
a. Analyse and document the outcomes of the validation activities and evaluate if the corresponding safety validation objectives are satisfied	TVALR Section 4
b. Update the list of Technical (Safety) Requirements as necessary and document the corresponding evidence on their validity	Updated set of Technical (Safety) Requirements to be included : - In the safety assessment report (TVALR App.C) - In the EN Technical Specification section 4.2
c. Document the low fidelity set of evidences showing Technical System Safety Specification is satisfied (potential update if necessary)	TVALR Appendix C - Safety Assessment Report

O.3.3 TRL6 - System/subsystem model or prototype demonstration in a relevant environment

At this level, the fidelity of the component and/or breadboard being tested has to increase significantly. The basic technological elements must be integrated with reasonably realistic supporting elements so that the total applications (component-level, sub-system level, or system-level) can be tested. A representative model or prototype system or system - which would go well beyond ad hoc, 'patch-cord' or discrete component level bread-boarding - would be tested in a relevant environment. At this level, if the only 'relevant environment' is the environment of space, then the model/prototype must be demonstrated in space.

TRL6-SAFETY ACTIVITIES

OUTCOMES - DOCUMENTING

1. Planning Validation activities:	
a. Define relevant safety Validation Objectives with respect to validation activities to ensure that the several components together / sub-systems / system will provide the corresponding intended function and performance expected for the Technological system for each application and in the corresponding environment – Note: validation activities should be done in coordination with the corresponding ATM Operational Solutions.	TVALP Section 4.3 and 5.1.3
2. Based on Validation activities outcomes:	
a. Analyse and document the outcomes of the validation activities and evaluate if the corresponding safety validation objectives are satisfied	TVALR Section 4
b. Update the list of Technical (Safety) Requirements as necessary and document the corresponding evidence on their validity	Final set of Technical (Safety) Requirements to be included : - In the safety assessment report (TVALR App.C) - In the EN Technical Specification section 4.2
c. Document the high fidelity set of evidences showing Technical System Safety Specification is satisfied (potential update if necessary)	TVALR Appendix C - Safety Assessment Report

References

- [1] SESAR Safety Reference Material, Ed04.01, available at Stellar SJU Extranet
- [2] Accident Incident Models in MS Visio – AIM2017, available at Stellar SJU Extranet
- [3] AIM Glossaries, available at Stellar SJU Extranet
- [4] Community of Practice (CoP) available at Stellar SJU Extranet
- [5] SESAR 2020 Templates, available at Stellar SJU Extranet
- [6] European ATM Architecture (EATMA): <https://www.atmmasterplan.eu/architecture/views/>
- [7] P16.01.01, Validation / Verification of the SESAR Accident Incident Model (AIM), Edition 00.01.00, May 2014
- [8] Human Performance Assessment process V1 to V3 including VLD Ed 00.02.00, April 2018, available at Stellar SJU Extranet
- [9] Final Resilience Guidance Material for Safety Assessment (SRM) and Design, Edition 00.01.00, available at Stellar SJU Extranet
- [10] ICAO Collision Risk Modelling incl. the guidance available in A Unified Framework for Collision Risk Modelling in Support of the (Doc 9689)
- [11] P16.01.03, D02, Identification of Dynamic Risk Modelling for SESAR needs, Ed00.00.03, October 2011
- [12] P16.01.03, D11, Final guidelines for Dynamic Risk Modelling (DRM) application, Ed00.01.01 August 2014
- [13] P16.01.03 D09, Dynamic Risk Modelling (DRM) test case application and lessons learned, Ed00.01.03, September 2014
- [14] SESAR P16.01.04, Final Guidance Material to Execute Proof of Concept, Ed00.04.00, available at Stellar SJU Extranet
- [15] EUROCONTROL, 2007, Air Navigation System Safety Assessment Methodology (SAM), SAF.ET1.ST03.1000-MAN-01, Edition 2.1
- [16] SESAR 1 P16.06.01, Hybrid Fault Tree Methodology, Ed00.01.00
- [17] SESAR 1 i4D&CTA (OFA04.01.05) Safety Assessment Report (SAR) Ed 00.02.00

Acronyms

ADD	:	Architecture Definition Document
AIM	:	Accident Incident Model
APP	:	Approach
ARES	:	Airspace reservation/restrictions
ASM	:	Airspace Management
ATC	:	Air Traffic Control
ATCO	:	Air Traffic Controller
ATFCM	:	Air Traffic Flow and Capacity Management
ATM/ANS	:	Air Traffic Management/ Air Navigation Services
ATS	:	Air Traffic Service
BM	:	Barrier Model
CCF	:	Common Cause Failure
CFIT	:	Controlled Flight Into terrain
CoP	:	Community of Practice
COTS	:	Commercial Off-The-Shelf
CRM	:	Collision Risk Model
DCB	:	Demand Capacity Balancing
DOD	:	Detailed Operational Description
DOORS	:	Data Object Oriented Repository System
DRM	:	Dynamic Risk Model
EASA	:	European Aviation Safety Agency
EATMA	:	European ATM Architecture
ENR	:	Enroute
ETA	:	Event Tree Analysis
EXC	:	Excursion
EXC ATCO or EXEC ATCO	:	Executive Air Traffic Controller
FOD	:	Foreign Object Debris
FCRW	:	Flight Crew
FHA	:	Functional Hazard Assessment
FIN DIR	:	Final Director
FMEA	:	Failure Modes & Effects Analysis

FTA	: Fault Tree Analysis
FTS	: Fast-time Simulation
FMS	: Flight Management System
FPL	: Flight Plan
HAZID	: HAZard IDentification session
HFIA	: HP Issue Analysis
HMI	: Human-Machine Interface
HP	: Human Performance
HRA	: Human Reliability Assessment
IAF	: Initial Approach Fix
ID	: Identification
IFR	: Instrument Flight Rule
iRMT	: Initial Reference Mission Trajectory
iSMT	: Initial Shared Mission Trajectory
ITM	: Intermediate
LoS	: Loss of Separation
MAC	: Mid Air Collision
MT	: Mission trajectory
MTFoO	: Maximum Tolerable Frequency of Occurrence
NAA	: National Aviation Authority
NSA	: National Supervisory Authority
OAT	: Operational Air Traffic
OCVM	: Operational Concept Validation Methodology
OE	: Operational Environment
OHA	: Operations Hazard Analysis
OI	: Operational Improvement
OSD	: Operational Service & Environment Description
PAGAR	: Performance Assessment And Gap Analysis Report
PAR	: Performance Assessment Report
PM	: Point Merge
PRNAV	: Precision RNAV
PSSA	: Preliminary System Safety Assessment
RE	: Resilience Engineering

RCS	: Risk Classification Scheme
RTS	: Real-Time Simulation
RWY	: Runway
SAC	: Safety Criteria
SAM	: Safety Assessment Methodology
SAR	: Safety Assessment Report
SE	: System Engineering
SES	: Single European Sky
SESAR	: Single European Sky ATM Research programme
SID	: Standard Instrument Departure
SJU	: SESAR JU
SME	: Subject Matter Expert
SO	: Safety Objective
SPR	: Safety & Performance Requirements
SR	: Safety Requirement
SRM	: Safety Reference Material
SSA	: System Safety Assessment
STAM	: Short Term ATFCM Measures
STAR	: Safety Target Achievement Roadmap
SVT	: Safety Validation Target
SWIM	: System Wide Information Management
TA	: Transversal Area
TAD	: Technical Architecture Document
TC	: Tactical Conflict
TLS	: Target Level of Safety
TMA	: Terminal Area
TRL	: Test Readiness Level
TS	: Technical Specification
TSR	: Technical Safety Requirement
TSSS	: Technical System Safety Specification
TVALP	: Technical Validation Plan
TVALR	: Technical Validation Report
TWY	: Taxiway



UC	:	Use Case
UML	:	Unified Modelling Language
VALP	:	Validation Plan
VALR	:	Validation Report
VFR	:	Visual Flight rule
VLD	:	Very Large Demonstration
WOC	:	Wing Operation Centre
WVE	:	Wake Vortex Encounter
WX	:	Weather

For Further Reading – Safety Assurance in SESAR

1 Introduction

Although the safety assurance process follows a typical safety lifecycle, the safety assurance activities that constitute the process are driven entirely by the need for the activities to generate evidence with the right rigour to show that the subject of the safety assessment is (will be) tolerably safe, as defined by the Safety Criteria. The rigorous logic applied by this document is as follows:

- *principles* which are the essential foundations for capturing and demonstrating satisfaction of a complete and correct set of safety requirements for a SESAR Solution before bringing it into service and maintaining it throughout its operational life
- *safety assurance objectives*, which state what has to be achieved in order to satisfy the related *principles*; and
- *safety assurance activities* which state how the safety assurance objectives will be satisfied – including the tools and techniques to be used

The definition of the *principles* was done by starting with a top-level statement (claim) about what a safety assessment / case is trying to demonstrate in SESAR in relation to the safety of the service or System. The decomposition of the claim into lower-level arguments into *safety assurance objectives* and *safety assurance activities* then provided the essential links between the Claim and the wealth of Evidence needed to show that the Claim is valid. Rather than using a standard Goal Structured Notation (GSN) as proposed in, e.g. the EUROCONTROL Safety Case Development Manual (SCDM), the required generic safety assurance objectives and activities to generate the required evidence are presented in a tabular format in **Guidance A.1** to **A.4**. Then obviously, in order to develop specimen safety assessments for specific concepts, **Guidance C** provides the means to define the tailored set of goals for the Safety Plan to address and associated assurance activities.

Thus the safety assurance objectives are determined solely and entirely by the need to satisfy the higher-level principles. The output of the safety assurance activities is then the evidence that is needed to show in turn that each safety assurance objective has been achieved and eventually, therefore, that the principles are satisfied.

This is illustrated in **Figure 25** below:

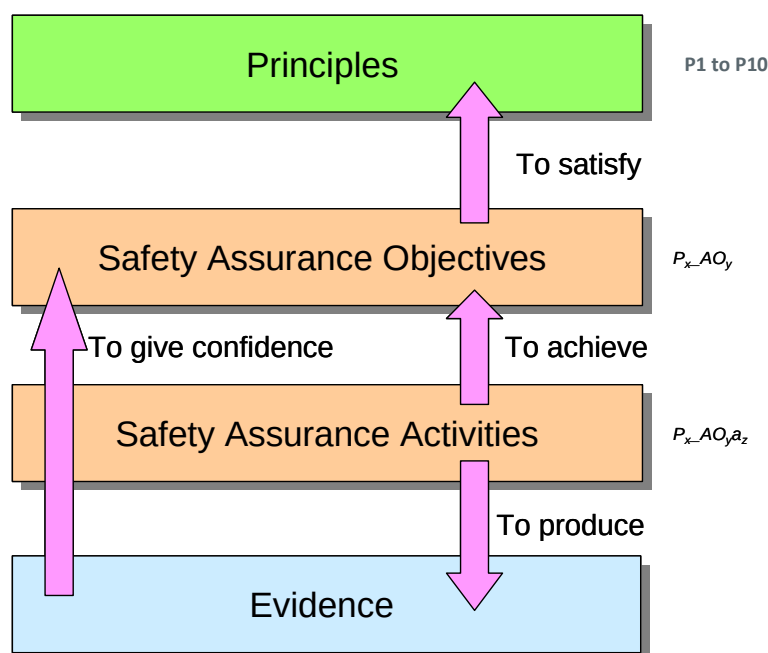


Figure 25: Safety Assurance Structure

Note: Safety Objectives and Safety Requirements developed to satisfy the Safety Criteria (with forward and backward traceability) are part of the evidence as outputs of the Safety Assurance activities.

2 Generic Principles – fundamental aspects

For any changes to ATM/ANS functional systems, operational and system experts within a specific Solution shall collectively¹⁵ conduct a risk assessment and mitigation in order to:

- P1. Define the scope, boundaries and interfaces of the functional system being considered, or other affected parts of the remainder air navigation services and underlying functional systems, its intended functions as well as the environment(s) of operations in which the change is intended to operate.
- P2. Derive Safety Criteria specific for the change that are consistent with the overall criterion in terms of safety for SESAR and operational environment(s).
- P3. As appropriate¹⁶, specify safety objectives at operational level for the change which seek to maximise the positive contribution of the air navigation services to aviation safety and minimize their contribution to the risk of an accident
- P4. Show that if the safety objectives are achieved, then the Safety Criteria will be satisfied.
- P5. As appropriate (see footnote 16), derive initial safety requirements for the design induced by the change in order to achieve the safety objectives.

¹⁵ What collectively means in terms of roles and responsibilities is expanded in sections 3.1 to 3.4 below and **Guidance A.1 to A.4.**

¹⁶ What is 'appropriate' is given by the execution of the change assessment as part of the Safety Scoping and Change assessment process described in **Guidance C.**

- P6. Show that, if the initial safety requirements are satisfied, then the safety objectives will be achieved.
- P7. Show that the refined safety requirements for the pre-industrialisation & integration phase are complete, correct and consistent.
- P8. Show that safety requirements for the implementation are complete, correct and consistent
- P9. Show that the change can be safely transitioned into operation.
- P10. Propose how the safety performance related to the change could be demonstrated and maintained during its operational lifecycle.

Note: P8, P9 and P10 principles are not addressed by the SESAR SRM because outside of the Industrial Research & Validation phase.

3 Generic Safety Assurance Objectives (about the satisfaction of principles)

3.1 Safety Planning

Operational and system experts within a specific Solution shall collectively provide assurance that:

- P1_AO1. the scope of the safety assessment properties of the particular operational environment(s) have been captured to ensure that they are a true representation of the environment to which the change to ATM/ANS functional systems will be exposed;
- P1_AO2. the change brought by the Solution to, the ATM/ANS functional systems in terms of what is removed, added, modified or affected at the operational level, at the high-level design and/or final design has been identified;
- P1_AO3. other affected parts of the ATM/ANS operations have been identified.

For Principle P2, no assurance objectives are specified¹⁷. Rather a detailed set of assurance activities is given in **Guidance A.1**.

3.2 Safety Assessment at operational level

The Solution shall, as appropriate (see footnote 16), provide assurance that:

- P3P4_AO1. the safety objectives resulting from the success approach define functional and performance safety properties to ensure adequate positive contribution to aviation safety, in accordance with the Safety Criteria for the change;
- P3P4_AO2. the safety objectives resulting from the failure approach define integrity safety properties to limit the negative contribution to the risk of accident/incident (and additional functional and performance properties to provide mitigation of the consequences of the operational hazards), in accordance with the Safety Criteria for the change;

¹⁷ In any type of argument, in case of full equivalence between the argument and the sub-argument, nothing prevents you to move straight to the evidence (in this case safety assurance activities to generate the evidence).

- P3P4_AO3. all assumptions upon which safety objectives are dependent shall be captured;
- P3P4_AO4. the safety objectives apply to known configuration(s)^{note} of the operational level system description and its operational environment(s).
- P3P4_AO5. the evidence for the safety properties of the Operational Environment(s), the Safety Criteria and the safety objectives is trustworthy.

Note: It is essential to show that all evidence in support of the safety arguments applies to a known system configuration and one which is consistent for all phases the development lifecycle. Since projects are liable to changes being introduced at various stages of system development, this requires careful change management and configuration control of the various representations of the system throughout the lifecycle, and iterations back through previous phases whenever a change invalidates (to some degree or extent) evidence that was collected prior to that change.

3.3 Safety Assessment of SESAR Solution's initial design

The Solution shall, as appropriate (see footnote 16), collectively provide assurance that at the initial design:

- P5P6_AO1. the initial safety requirements resulting from the success approach define functional and performance safety properties to achieve the corresponding operational level safety objectives
- P5P6_AO2. these functional and performance safety properties will be delivered under all normal conditions¹⁸ of the operation environment that the ATM/ANS functional system is expected to encounter in day-to-day operations;
- P5P6_AO3. the degree and extent to which the elements of the high-level architecture can continue to deliver the functional and performance safety properties under any external abnormal conditions¹⁹ that the ATM/ANS functional system may exceptionally encounter shall be assessed
- P5P6_AO4. additional initial safety requirements are defined so that the risk during the period of the degraded state is shown to be within the Safety Criteria
- P5P6_AO5. the initial safety requirements resulting from the failure approach define the necessary safety-integrity attributes to achieve the corresponding operational level safety objectives (and additional functional and performance properties for internal mitigation of failures);
- P5P6_AO6. any non-safety functionality in the initial design cannot adversely affect the safety of the initial design;
- P5P6_AO7. any adverse emergent properties have been eliminated or mitigated sufficiently, in the initial design;
- P5P6_AO8. any safety functionality in the initial design cannot adversely affect the operation of related ground-based and airborne safety nets

¹⁸ For those conditions, the ATM/ANS functional system is expected to deliver full functionality and performance.

¹⁹ For those conditions, the ATM/ANS functional system design is expected to be Robust against (*i.e.* work through), or at least Resilient to (*i.e.* recover easily from).

Founding Members

- P5P6_AO9. all assurance for the initial safety requirements applies to a known configuration(s) of the ATM/ANS functional system and its operational environment(s);
- P5P6_AO10. the evidence for the initial safety requirements is trustworthy.

3.4 Safety Assessment of SESAR Solution's refined system design

Given that the scoping of SESAR is limited to the pre-industrialization phase, the Solution shall, as appropriate (see footnote **16**) collectively provide assurance that:

- P7_AO1. Refined safety requirements resulting from the success approach for the refined system design level of the SESAR solution satisfy the corresponding safety requirements derived for the initial system architecture;
- P7_AO2. these functional and performance safety properties will be delivered under all normal conditions²⁰ of the operation environment that the ATM/ANS functional system is expected to encounter in day-to-day operations;
- P7_AO3. the degree and extent to which the elements of the refined design architecture can continue to deliver the functional and performance safety properties under any external abnormal conditions that the ATM/ANS functional system may exceptionally encounter shall be assessed
- P7_AO4. additional refined safety requirements are defined so that the risk during the period of the degraded state is shown to be within the Safety Criteria
- P7_AO5. Refined Safety requirements resulting from the failure approach for the refined system design level of the SESAR solution satisfy the corresponding safety requirements derived for the initial system architecture;
- P7_AO6. any non-safety functionality in the refined design cannot adversely affect the safety of the refined design;
- P7_AO7. Additional refined safety requirements are defined to ensure that any adverse emergent properties have been eliminated or mitigated sufficiently, in the refined system design.
- P7_AO8. any safety functionality in the refined design cannot adversely affect the operation of related ground-based and airborne safety nets
- P7_AO9. all refined safety requirements are achievable in a typical implementation;
- P7_AO10. all assurance for the refined system safety requirements applies to a known configuration(s) of the ATM/ANS functional system and its operational environment(s);
- P7_AO11. the evidence for the refined safety requirements is trustworthy.

²⁰ For those conditions, the ATM/ANS functional system is expected to deliver full functionality and performance.



-END OF DOCUMENT-

