SESAR Solution 02.05 SPR-INTEROP/OSED V3 - Part II - Safety Assessment Report

Deliverable ID:	**D4.1.012-2**
Dissemination Level:	**PU**
Project Acronym:	**EARTH**
Grant:	**731781**
Call:	**H2020-SESAR-2015-2**
Topic:	**SESAR.IR-VLD.Wave1-04-2015**
Consortium Coordinator:	**EUROCONTROL**
Edition Date:	**11 November 2019**
Edition:	**00.01.01**
Template Edition:	**02.00.01**

Authoring & Approval

Authors of the document

Name/Beneficiary	Position/Title	Date
Marco Paino / ENAV	Solution SAF Expert	16/11/2018

Reviewers internal to the project

Name/Beneficiary	Position/Title	Date
Fabio MANGIARACINA / ENAV	Solution 02-05 Manager	17/07/2019
Stefano Ghilardi / ENAV	Operational Project Leader /TMA	25/07/2019
Matteo Ergotti / ENAV	Validation Ops Lead / APT	25/07/2019
Carotenuto Salvatore / ENAV	Airspace Designer Dept.	25/07/2019
Giovanni NEGRO / LEONARDO	Solution Member	25/07/2019
Davide Ferraro / LEONARDO	Solution Member	25/07/2019
Marco Cappella / NAIS	Solution Member	25/07/2019
Luigi Perrotta / NAIS	Solution Member	25/07/2019
Francesca Parrotta / NAIS	Solution Member	25/07/2019
Luna Babusci/ENAV	SESAR Operational Expert	25/07/2019

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

Name/Beneficiary	Position/Title	Date
Fabio MANGIARACINA / ENAV	Solution 02-05 Manager	31/07/2019
Giovanni NEGRO / LEONARDO	Solution Member	31/07/2019

Rejected By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date

Document History

Edition	Date	Status	Author	Justification
00.00.01	16/11/2018	Draft	Marco Paino	First draft
00.00.02	25/03/2019	Draft 1	Marco Paino	2nd draft
00.00.03	18/07/2019	Draft 2	Marco Paino	3rd draft
00.00.04	19/07/2019	Final Draft	Marco Paino	Final Draft before delivery

00.01.00	30/07/2019	Final for delivery	Marco Paino	Final for SJU quality check
00.01.01	30/10/2019	Final Update	Marco Paino	Final version with PJ19 guidelines

Copyright Statement

© – 2017,2018,2019 – ENAV, LEONARDO.
All rights reserved. Licensed to the SESAR Joint Undertaking under conditions

EARTH

ENHANCED RUNWAY THROUGHPUTENHANCED RUNWAY THROUGHPUT

This Safety Assessment Report is part of a project that has received funding from the SESAR Joint Undertaking under grant agreement No 731781 under European Union’s Horizon 2020 research and innovation programme.

Abstract

The part II of the SESAR Solution 02-05 SPR-INTEROP/OSED describes the expected environment, the operational concept, the New SESAR Operating Method options and associated use cases, to address Operational Improvement AO-0316. This document is used as basis for assessing and establishing operational, safety recommendations and requirements to deliver the related Operational Improvements:

AO-0316 - Increased Airport Performance through Independent (parallel or convergent) IFR Rotorcraft Operations.

Table of Contents

Abstract 4
1 *Executive Summary* 8
2 *Introduction* 9
2.1 Background 9
2.2 General Approach to Safety Assessment 9
2.3 Scope of the Safety Assessment 9
2.4 Layout of the Document 9
3 *Safety specifications at the OSED Level* 11
3.1 Scope 11
3.2 Solution Operational Environment and Key Properties 11
3.3 Airspace Users Requirements 11
3.4 Relevant Pre-existing Hazards 12
3.5 SAfety Criteria 13
3.6 Mitigation of the Pre-existing Risks – Normal Operations 18
3.7 PJ02.05 Solution Operations under Abnormal Conditions 20
3.8 Mitigation of System-generated Risks (failure approach) 21
3.9 Achievability of the Safety Criteria 24
3.10 . Validation & Verification of the Safety Specification 24
4 *Safe Design at SPR Level* 25
4.1 Scope 25
4.2 The [TBD] Solution Functional Model 25
4.3 The PJ02.05 Solution SPR-level Model 25
4.4 Analysis of the SPR-level Model – Normal Operational Conditions 33
4.5 Analysis of the SPR-level Model – Abnormal Operational Conditions 34
4.6 Design Analysis – Case of Internal System Failures 35
4.7 Achievability of the SAfety Criteria 38
4.8 Realism of the SPR-level Design 38
4.9 Validation & Verification of the Safe Design at SPR Level 38
5 *Detailed Safe Design at Physical Level* 40
6 *Acronyms and Terminology* 41
7 *References* 47

Appendix A Safety Objectives ... 48

A.1 Safety Objectives (Functionality and Performance) ... 48

A.2 Safety Objectives (Integrity) ... 48

Appendix B Consolidated List of Safety Requirements ... 49

B.1 Safety Requirements (Functionality and Performance) ... 49

B.2 Safety Requirements (Integrity) ... 49

Appendix C Assumptions, Safety Issues & Limitations ... 50

C.1 Assumptions log ... 50

C.2 Safety Issues log ... 50

C.3 Operational Limitations log ... 51

Appendix D RCS for MAC in En-route & TMA operational environments and for Controlled Flight Into Terrain ... 52

List of Tables

Table 1: Pre-existing Hazards ... 13

Table 2: SAfety Criteria (SAC) ... 14

Table 3: Precursor "ATC induced tactical conflict" ... 16

Table 4: Precursor "ATC induced pre-tactical conflict" ... 16

Table 5: Precursor "Crew/aircraft induced tactical conflict" ... 17

Table 6: Precursor "Tactical Conflict Management" / Precursor "Imminent Infringement" ... 17

Table 7: ATM and Pre-existing Hazards ... 18

Table 8: PJ02.05 Solution Operational Services & Safety Objectives (success approach) ... 19

Table 9: List of Safety Objectives (success approach) for Normal Operations ... 20

Table 10: Additional Safety Objectives (success approach) for Abnormal Conditions ... 21

Table 11: List of Safety Objectives (success approach) for Abnormal Operations ... 21

Table 12: System-Generated Hazards and Analysis ... 23

Table 13: Additional Safety Objectives (functionality and performance) in the case of internal failures ... 23

Table 14: Safety Objectives (integrity/reliability) ... 24

Table 15: Mapping of Safety Objectives to SPR-level Model Elements ... 30

Table 16: Derivation of Safety Requirements (functionality and performance) from Safety Objectives 32

Table 17: Assumptions made in deriving the above Safety Requirements........ 32

Table 18: Operational Scenarios – Normal Conditions 33

Table 19: Additional SR from Thread Analysis – Normal Operational Conditions 34

Table 20: Operational Scenarios – Abnormal Conditions 34

Table 21: Safety Requirements or Assumptions to mitigate abnormal conditions 35

Table 22: Additional Safety Requirements from Thread Analysis – Abnormal Operational Conditions 35

Table 23: Acronyms and terminology 46

Table 24: Assumptions log 50

Table 25: Safety Issues log........ 51

Table 26: Operational Limitations log 51

Table 27: Risk Classification Scheme for Mid Air Collision (TMA and En-Route) 52

Table 28: Risk Classification Scheme for CFIT 53

List of Figures

Figure 1: Mid Air Collision Barrier Model........ 15

Figure 2: APV (-ADV) SPR level model 27

1 Executive Summary

Solution PJ.02-05 – Enhanced Runway Throughput – addresses concepts and systems which allow the implementation of the operational concept of the ***Simultaneous-non-Interfering (SNI)*** Operations for rotorcraft aimed to increase the Airport Performance through the use of independent IFR rotorcraft procedures to/from a FATO (Standard/Advanced Point In Space procedures). Furthermore, the Solution 02-05 addresses *additionally* the applicability of **PinS *designing criteria*** to specific rotorcraft operations GBAS technologies based.

The Solution evaluated also the use of a combined SBAS (CAT I) procedures with Radius to Fix legs (RF) and Synthetic Vision System (SVS) for evaluating the possibility to reduce the approach minima value of the procedure, increasing pilot situational awareness and safety meanwhile reducing ATCOs' and Pilot's workload.

The SAR (Safety Assessment Report) draws upon the detailed descriptions of the Operating Environment and Use Cases documented in the PJ02-05 SPR-INTEROP/OSED document in order to define a list of achievable Safety Criteria (SC) that are required to be fulfilled to satisfy the safety benefits, and to satisfy any appropriate regulatory requirements.

2 Introduction

2.1 Background

The Operational Service and Environment Definition (OSED) describes the operational concept, the operational services, their environment, use cases and is used as the basis for assessing and establishing operational, safety, performance and interoperability requirements for the related systems detailed in the Safety and Performance Requirements (SPR) and INTEROP sections of this document. The OSED identifies the operational services supported by several entities within the ATM community and includes the operational expectations of the related systems.

2.2 General Approach to Safety Assessment

The assurance of validation and verification of the safety assessment requirements is an on-going activity. A qualitative safety assessment has been performed from airborne side on the basis of the Use Cases, Solution Scenarios VS Reference Scenario and Operating Method described in the OSED and validated through the exercises described in the VALP and recorded in the synthesis of validation results VALR for IT1 and IT2. An on-going activity (questionnaires, pilot and flight crew feedback, post analysis and de-briefing activities) is being performed to map the safety objectives and requirements generated here to the validation objectives and results, to ensure that all requirements have been assessed. For that reasons some safety requirements are evaluated together, and the outcomes has been complementary

2.3 Scope of the Safety Assessment

This SPR-INTEROP/OSED identifies the operating method options that were analysed in the V3 phase to address Operational Improvement AO-0316. It should also be noted that PJ.02-05 work might also contribute to mature the OI AOM-0104-B, which is led by PJ.01-06.

This document focuses mainly on the success approach to assess how much the identified pre-existing hazards already in aviation are expected to be reduced by the definition of the Simultaneous-non-Interfering (SNI) Operations for rotorcraft aimed to increase the Airport Performance.

Based on the information detailed in the Solution PJ02-05 SPR-INTEROP/OSED document, the SAR describes, through the definition of safety objectives (from the failure approach), how they could mitigate pre-existing hazards.

Beneficially the part II SPR-INTEROP/OSED contains the Specimen Safety Assessment for an application of the PinS Solution in SNI operations. The report presents even the assurance that the Safety Requirements for the V3 phase are complete, correct and realistic, thereby it provides all material to adequately inform the PJ02-05 Solution OSED/SPR/INTEROP.

2.4 Layout of the Document

Section 1 presents the executive summary of the document.

Section 2 provides background information regarding the definition, design and validation of the Concepts Solutions, the principles for safety assessment in SESAR Programme and the scope of this safety assessment.

Section 3 addresses the safety specification at OSED level, through the definition of Safety Criteria (SAC), the determination of Safety Objectives (SO) and link to validation objectives.

Section 4 addresses the safe design at SPR level, through the derivation of Safety Requirements (SR) and link to validation results.

Section 5 addresses the safe design at physical level through the derivation of safety requirements (functionality and performance) for the physical design that satisfy the SPR level safety requirements

Appendix A presents the consolidated list of Safety Objectives

Appendix B presents the consolidated list of Safety Requirements with traceability to the Safety Objectives and to SESAR 1 OFA SPR requirements.

Appendix C presents the list of Assumptions, Issues, Recommendations and Assessment Limitations

Appendix D presents the Risk Classification Schemes for the relevant accident-incident types

Appendix E outlines the Accident Incident Models (AIM) relevant for SESASR Solution 02-05.

3 Safety specifications at the OSED Level

3.1 Scope

The aim is to provide right evidence that the subject of the safety assessment is acceptably safe, as defined by the SAfety Criteria [see section 3.5].

This document addresses the following activities:

- Description of the key properties of the Operational Environment that are relevant to the safety assessment
- Identification of the pre-existing hazards that affect Simultaneous-non-Interfering (SNI) for rotorcraft operations in relevant environment and the risks of which operational services provided by ATS System may reasonably be expected to mitigate to some degree and extent
- Setting of the Safety Criteria
- Comprehensive determination of the operational services that are provided by the OFA to address the relevant pre-existing hazards and derivation of Safety Objectives (success approach) in order to mitigate the pre-existing risks under normal operational conditions
- Assessment of the adequacy of the operational services provided by the Solution under abnormal conditions of the Operational Environment
- Assessment of the adequacy of the operational services provided by the OFA in the case of internal failures and mitigation of the system-generated hazards (derivation of Safety Objectives (failure approach))
- Achievability of the SAfety Criteria
- Validation & verification of the safety specification

3.2 Solution Operational Environment and Key Properties

Please refer to PJ.02-05 SPR-INTEROP /OSED V3 Part I [7].

3.2.1 Airspace Structure and Boundaries

The controlled airspace (e.g. TMA\Class “A” and CTR\Class “D”) has been the operational environment in which all operations have been considered.

Nevertheless, no particular constrain to preclude the development of this kind of routes/procedures (e.g. RNP1) in a class “G” airspace has been identified, provided the concerned CAA allows IFR in Class G airspace (e.g. today, still forbidden in Switzerland). This is also valid for RNP 0.3.

3.3 Airspace Users Requirements

The SAFETY AUs' Requirements addressed within the validations are the following ones:

REQ-02.05-SAFE-PSNI.0320
REQ-02.05-SAFE-PSNI.0330
REQ-02.05-SAFE-PSNI.0350
REQ-02.05-SAFE-PSNI.0360
REQ-02.05-SAFE-PSNI.0370
REQ-02.05-SAFE-PSNI.0380
REQ-02.05-SAFE-PSNI.0390
REQ-02.05-SAFE-PSNI.0400
REQ-02.05-SAFE-PSNI.0410
REQ-02.05-SAFE-PSNI.0420
REQ-02.05-SAFE-PSNI.0430
REQ-02.05-SAFE-PSNI.0440
REQ-02.05-SAFE-PSNI.0450
REQ-02.05-SAFE-PSNI.0460
REQ-02.05-SAFE-PSNI.0470
REQ-02.05-SAFE-PSNI.0510

Anyhow, for further info please refer to the Section §4 in PJ.02-05 SPR-INTEROP /OSED V3 Part I .[7].

3.4 Relevant Pre-existing Hazards

The pre-existing hazards relevant to the solution PJ.02-05 have been identified from the list provided in the guidance for applying SRM (Guidance F.2.2 Identifying Pre-existing Hazards). By definition, the pre-existing hazards are 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 tolerable level.

The SRM Guidance (D and E) provides even a set of Accident Incident Models (AIM - one per each type of accident) which represent an integrated risk picture with respect to ATM contribution to aviation accidents.
The pre-existing hazards relevant to the PJ.02-05, together with the corresponding ATM-related accident types and AIM models, are presented in the table below:

Hazard ID	Hazard	Reasoning
Hp#1	A situation in which the intended trajectories of aircrafts and rotorcraft are in conflict (MAC)	Mid-Air Collision (MAC) on the Final Approach. The use of the procedure may bring rotorcraft into a situation where this hazard might occur
Hp#2	A situation where the intended trajectory of an aircraft is in conflict with terrain or an obstacle (CFIT)	Controlled Flight into Terrain (CFIT) on the Final Approach path
Hp#3	Penetration of restricted airspace (This category is quite distinct from MAC for military danger areas where	Any possible infringement and/or penetration of restricted airspace

	the end effect could be being shot down.)	
Hp#4	Encounters with adverse weather	Any possible rotorcraft into an area of adverse weather unknown to ATC

Table 1: Pre-existing Hazards

3.5 SAfety Criteria

SAfety Criteria (SAC) means explicit and verifiable (qualitative or quantitative) criteria, the satisfaction of which results in tolerable safety following the change.
SACs are derived during V1 through safety assessment of the AIM and as the Solution progresses to V2 and the concept is further refined till fully V3 level, the safety assessment at the OSED level establishs the safety objectives to deliver the SAC and the SPR level safety requirements to satisfy the safety objectives.

SAC Ref	Suggested SAC	Associated Hazard Ref	Associated Hazard
SAC#1	Re-routing shall not be used when PinS procedure has started to be implemented unless it is necessary for safety reasons (the sequence will be influenced and changes will have to be made with resulting increased work-load).	**Hp#1**	a situation in which the intended trajectories of two or more aircraft are in conflict (MAC)
SAC#2	Any re-routings shall not introduce conflicts between fixed-wing and rotorcraft SNI PinS procedures for arrival [1]planned routes.	**Hp#1**	a situation in which the intended trajectories of two or more aircraft are in conflict (MAC)
SAC#3	Any re-routings shall ensure that the rotorcraft arrival procedures (simultaneously and non-interfering) can be safely carried out when the re-routings will be performed.	**Hp#1**	a situation in which the intended trajectories of two or more aircraft are in conflict (MAC)

[1] The SAC#2 could be referred to the rotorcraft SNI PinS procedures for departure, further to the arrival procedures, but for the scope of this solution just approaching operations have been analyzed.

SAC#4	The SNI criteria adopted for the designing of the rotorcraft PinS procedures shall ensure that the pilot is informed -through procedure maps- about all the relevant obstacles in the manoeuvring area.	**Hp#2**	a situation where the intended trajectory of an aircraft is in conflict with terrain or an obstacle (CFIT)
SAC#5	The rotorcraft PinS SNI procedures designing criteria (SOIR ICAO DOC9643, PASNOPS 8168, Annex 14) will enable rotorcraft operations not interfering with the existing standard approach procedures conceived for fixed-wing aircraft.	**Hp#3**	a situation in which the intended trajectories of two or more aircraft are in conflict (MAC)
SAC#6	Local real-time weather details shall be available and taken into account during the operations.	**Hp#4**	encounters with adverse weather

Table 2: SAfety Criteria (SAC)

3.5.1 Identification of the accident type impacted by the change

Different types of accidents can occur in ATM domain: Mid Air Collision, Runway Collision, Controlled Flight Into Terrain or Taxiway Accident. The whole ATM system acts as a set of barriers preventing these accidents from happening. Barriers models have been defined for each kind of accident representing all the ATM elements (equipment, procedures and people) that work together in order to stop the precursors before they become accidents.

Considering the pre-existing hazards that are impacted by Simultaneous-non-Interfering (SNI) for rotorcraft operations concept, the relevant accident type for this Solution is the **Mid-Air Collision**.

The simplified version of the Accident Incident Models that have been identified as being relevant for the PJ02 Solution 5 is presented in the next figure:

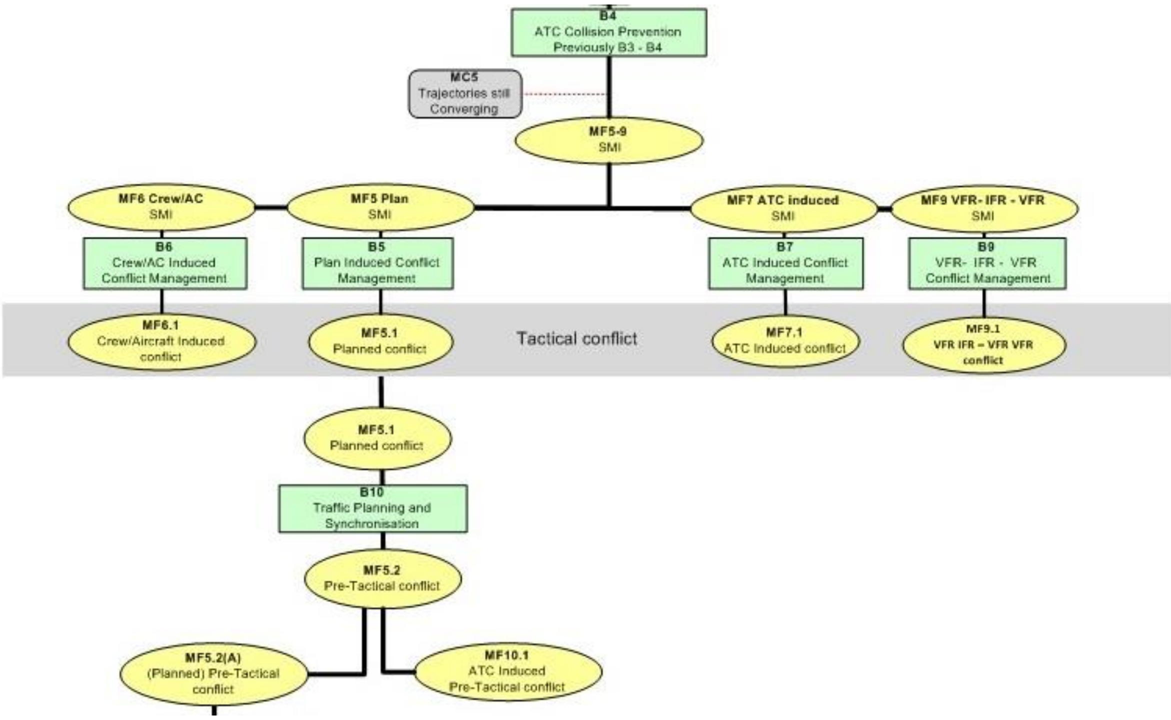


Figure 1: Mid Air Collision Barrier Model

The "**Tactical conflict resolution barrier**: **tactical conflict management**" consists in managing the tactical conflicts and consequently maintaining the separation between aircrafts/rotorcrafts or with restricted areas. This barrier includes:

- Management of planned conflict (conflict detected by the ATC),
- Management of ATC induced conflict (conflict induced by the ATCO when solving another conflict or when dealing with a situation of bad weather / restricted area activation),
- Management of crew/aircraft induced conflict (conflict induced by a failure of the pilot or the aircraft)

This barrier is implemented by the tactical controller (for detection and resolution of the conflict) and the crew (for execution of the clearance) and, the simplified version of the related AIM makes reference to the following items:

- B5 Plan Induced Conflict Management,
- B6 Crew-R/C Induced Conflict Management,
- B7 ATC Induced Conflict Management,
- B9 VFR – IFR Conflict Management,
- B10 Traffic Planning and Synchronization.

The main precursors (conditions, events, and sequences that precede and lead up to the mid-air collision) of this model are

- Imminent Infringement
- Pilot induced tactical conflict: manoeuver performed by the aircraft or the pilot leading to a deviation and potentially to a conflict
- ATC induced tactical conflict: conflict induced by the tactical controller within the frame of its activities.
- ATC induced pre-tactical conflict: conflict induced by the planner controller within the frame of its activities.
- Planned Tactical conflict
- Pre-tactical conflict
- Strategic conflict

All these precursors contribute to "Mid Air Collision".

Precursor "ATC induced tactical conflict" (MF 7.1)	
Positive impact	**Negative impact**
On the precursor: Less ATCO intervention to provide more efficient trajectories to aircraft across their airspace (pilot requests), because rotorcraft are flying their preferred route, leading to less ATC induced conflicts. It is a positive impact, but very small in quantitative terms.	increase in knock-on conflicts due to a possible impact on SA. increase in conflicts by trajectory management instructions due to a possible impact on SA
	No disregarded negative impact:
Positive and negative impacts balanced: no increase in ATC induced conflicts	

Table 3: Precursor "ATC induced tactical conflict"

Precursor "ATC induced pre-tactical conflict" (MF 9.1)	
Positive impact	**Negative impact**
On the precursor: number of planning actions (pre-tactical instructions). Less ATCO intervention.	No negative impact
No negative impact. Conservative SAC: maintain ATC induced pre-tactical conflicts	

Table 4: Precursor "ATC induced pre-tactical conflict"

<table>
<tr><td colspan="2">Precursor “Crew/aircraft induced tactical conflict” (MF 6.1)</td></tr>
<tr><th>Positive impact</th><th>Negative impact</th></tr>
<tr><td>On the precursor: Rotorcraft are flying their preferred route in approaching operations, leading to less requests (both from pilots and ATCOs) for trajectory revision and then to fewer pilot induced deviations.</td><td>No disregarded negative impact:</td></tr>
<tr><td colspan="2">No negative impact. Conservative SAC: maintain crew induced tactical conflicts</td></tr>
</table>

Table 5: Precursor “Crew/aircraft induced tactical conflict”

<table>
<tr><td colspan="2">Barrier “Tactical Conflict Management” (B5 & B6 & B7) / Precursor “Imminent Infringement” (M5-9)</td></tr>
<tr><th>Positive impact</th><th>Negative impact</th></tr>
<tr><td rowspan="4">On the barrier: Easier conflict detection due to better aircraft trajectory predictability (less unexpected trajectories)</td><td>On the barrier on conflict detection:

Difficult to monitor conformance to the approaches route for IFR rotorcraft operations, consequently, difficult to detect rotorcraft deviations (potential pilot/aircraft induced conflict).</td></tr>
<tr><td>On the barrier on conflict resolution:

Some conflict situations can be more workload demanding for ATCOs (for instance two converging trajectories with a low converging angle between the trajectories, or conflicts close to sector boundaries). Detection not impacted, only resolution.</td></tr>
<tr><td>Disregarded negative impacts:

.</td></tr>
<tr><td></td></tr>
<tr><td colspan="2">More negative impact than positive impact, but mitigation should maintain barrier efficiency.</td></tr>
</table>

Table 6: Precursor “Tactical Conflict Management” / Precursor “Imminent Infringement”

3.6 Mitigation of the Pre-existing Risks – Normal Operations

3.6.1 Operational Services to Address the Pre-existing Hazards

ID	Service Objective	Pre-existing Hazards [Hp xx]
SP3	Create and maintain spacing/separation between aircraft in converging arrival flows of the landing sequence	Hp#1
AFA	Facilitate acquisition of the Final approach path	Hp#1
SPO	Separate arrivals from departures, transit flights, overflights and other arrivals (i.e. to other airports)	Hp#1
SPT	Separate arrivals from terrain/obstacles	Hp#2
PAW	Prevent adverse weather encounters	Hp#4

Table 7: ATM and Pre-existing Hazards

3.6.2 Derivation of Safety Objectives (Functionality & Performance – success approach) for Normal Operations

The safety requirements and assumptions developed in this paragraph and evaluated during the solution timeframe are directly compatible with those in the previous phase and are therefore achievable for the same reasons (stated below). In particular it is noted that the level of performance strictly connected with safety is stated in line with existing standards.

- It is under light that safety requirements have been determined/derived and evaluated only for elements under the managerial control of airborne side (Flight crew, Pilots and flying platform) and from ANSP regarding Airspace Design, in conjunctions with specific PinS APCH procedures.
- Regarding ANSP safety requirements are capable of being satisfied in an already identified typical implementation because they are relying on either existing standards (e.g ICAO Documents) either on similar requirements already locally implemented in different States. Assumptions are easily implemented because they are relying mainly on the EASA AMC 20-28 (which is the airworthiness and ops approval guidance material for example regarding LPV approach).

Some safety requirements should be easily satisfied because they are not different from those applicable to the "solution scenario" existing standards which are well known by the aeronautical community (e.g. GNSS/SBAS, LNAV/LPV..etc).

The assurance of validation and verification of the safety assessment requirements is an on-going activity. A qualitative safety assessment has been performed from airborne side on the basis of the Use Cases, Solution Scenarios VS Reference Scenario and Operating Method described in the OSED and validated through the exercises described in the VALP and recorded in the synthesis of validation results VALR. An on-going activity (questionnaires, pilot and flight crew feedback, post analysis and de-briefing activities) is being performed to map the safety objectives and requirements generated here to the validation objectives and results, to ensure that all requirements have been assessed. For that reasons some of the Solution high level safety requirements are evaluated together and the outcomes has been complementary.

Ref	Phase of Flight / Operational Service	Related AIM Barrier	Achieved by / Safety Objective [SO xx]
SP3	Create and maintain spacing/separation between aircraft (rotorcraft) in converging arrival flows of the landing sequence	B10	SO 01
AFA	Facilitate acquisition of the Final approach path	B7 B9	SO 02
SPO	Separate arrivals from departures, transit flights, overflights and other arrivals (i.e. to other airports)	B5 B7 B9	SO 02
SPT	Separate arrivals from terrain/obstacles	B7	SO 02
PAW	Prevent adverse weather encounters		SO 04

Table 8: PJ02.05 Solution Operational Services & Safety Objectives (success approach)

With reference to the solution/validation activities collected in VALR, no specific change in the functional requirements or in the navigation features, rotorcraft specific, has been identified.

In order to flown the same procedures based on GBAS signal instead of SBAS augmentation, the coded procedure has to be implemented according to GBAS FAS data block.

The ATCOs shall be able to perform tactical coordination of flights across SNI operations with a possible support to monitor trajectories adherence to the PinS procedures for rotorcraft approaching route.

ID	Description
SO 01	The ATCOs shall be able to perform tactical coordination between fixed-wing and rotorcraft in SNI PinS procedures for arrival planned routes
SO 02	The ATCOs shall be able to monitor conformance to the approaches route for IFR rotorcraft operations, consequently, difficult to detect rotorcraft deviations (potential pilot/aircraft induced conflict)
SO 03 (new)	The ATCOs shall be provided with support to monitor trajectories adherence to the SNI PinS procedures for arrival planned routes

Table 9: List of Safety Objectives (success approach) for Normal Operations

Overall the recommendations collated for each validation exercise (at solution level) should be taken into consideration by SESAR Deployment Manager.

3.6.3 Analysis of the Concept for a Typical Flight

See the Solution 02-05 SPR-INTEROP/OSED Part I V3 (D4.1.012-1)[7].

3.7 PJ02.05 Solution Operations under Abnormal Conditions

The purpose of this section is to assess the ability of the Solution to work through (robustness), or at least recover from (resilience) any abnormal conditions, external to the Solution System, that might be encountered relatively infrequently.

3.7.1 Identification of Abnormal Conditions

The following abnormal conditions are relevant in the new concept:

Adverse weather conditions encounters (unknown).

3.7.2 Potential Mitigations of Abnormal Conditions

In this chapter the abnormal conditions identified above, will be further analysed. Table 10 shows for each abnormal condition, the assessed immediate operational effect and the possible mitigations of the safety consequence of the operational effect with a reference to existing safety objectives (as per Table 8 and Table 9) or to new safety objectives described in Table 11 below

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SO xx]
1	Adverse weather conditions encounters (e.g.: strong wind, thunderstorm, …)	Adverse weather conditions can led to a	SO 04

		missed approach procedure	

Table 10: Additional Safety Objectives (success approach) for Abnormal Conditions

The following additional Safety Objectives (success approach) is defined to cover the abnormal conditions identified above.

ID	Description
SO 04	The ATCOs shall support the pilot when approaching the MAPt (Missed Approach Point), to decide whether to continue or abort the approach.

Table 11: List of Safety Objectives (success approach) for Abnormal Operations

3.8 Mitigation of System-generated Risks (failure approach)

Before any conclusion can be reached concerning the adequacy of the safety specification of SNI PinS Rotorcraft operations, at the OSED level, it is necessary to assess the possible adverse effects that failures internal to the Solution System might have upon the provision of the relevant operational services described in section 3.6 and to derive safety objectives (failure approach) to mitigate against these effects.

3.8.1 Identification and Analysis of System-generated Hazards

The identification and analysis of system-generated hazard has been performed in accordance with the Safety Reference Material methodology. For each safety objective, what would happen if the objectives were not satisfied (i.e. negate the safety objectives derived), the following system-generated hazards were identified:

1. Failure to perform tactical coordination between fixed-wing and rotorcraft in SNI PinS procedures for arrival planned routesFailure to monitor conformance to the approaches route for IFR rotorcraft operations and to detect rotorcraft deviations (potential pilot/aircraft induced conflict)

3. Loss of display/tool/support to monitor the trajectories adherence to the SNI PinS procedures for arrival planned routes

The analysis of the hazards included the following activities, for each hazard

- Identification of possible causes of the hazard and prevention mitigation means (mitigation to prevent the hazard occurring)
- Identification of operational effects of the hazard and protection mitigation means (mitigation to minimize the effects of this hazard)

- Identification of the precursor associated to the hazard and determination of the severity, according to the AIM barrier model.

The main activities are:

- A list of new Safety Objectives, derived from mitigation means
- A list of hazards classified according to their severity, to be derived into Integrity & Reliability Safety Objectives (see section 3.8.2).

Table 15 below presents the summary of the hazard identification and assessment activity. These tables are organized as follows:

- Column 1 indicates the operational hazard reference (HZ-XXX)
- Column 2 provides the description of the operational hazard,
- Column 3 indicates the related Functionality & Performance Safety Objectives i.e. whose failure originated the hazard,
- Column 4 describes the assessed Operational Effects of each hazard, including the AIM precursor of the MAC model corresponding to the hazard [Figure 1: Mid Air Collision Barrier Model],
- Column 5 indicates the mitigations means for the hazards' effects, referred to the AIM MAC model barrier where they are allocated. F&P Safety Objectives that were derived during the success case are mentioned here. Additional F&P Safety Objectives that were not derived during the success case but have been proposed during the failure case are also included here and later presented in Table 16.
- Column 6 indicates the allocated severity as per TC severity classification scheme [Appendix D],

ID	Description	Related SO *(success approach)*	Operational Effects	Mitigations of Effects	Severity *(most probable effect)*
	Failure to perform tactical coordination between fixed-wing and rotorcraft in SNI PinS procedures for arrival planned routes	SO 01		Barrier B10	SC5
	Failure to monitor conformance to the approaches route for IFR rotorcraft operations and to detect rotorcraft deviations	SO 02		Barrier B5/B6/B7/B9	SC4a/ SC4b

	(potential pilot/aircraft induced conflict)				
	Loss of display/tool/support to monitor the trajectories adherence to the SNI PinS procedures for arrival planned routes	SO 03		Barrier B5/B6/B7/B9	SC4a/ SC4b

Table 12: System-Generated Hazards and Analysis

Table 13 presents additional Functionality & Performance Safety Objectives that have been detected during the failure assessment, as functional mitigations for the effects of some hazards.

ID	Description
SO-FP-11	The ATCOS shall always have the possibility to perform the tactical coordination between fixed-wing and rotorcraft in SNI PinS procedures for arrival planned routes.
SO-FP-12	The ATCOs shall have the possibility to detect IFR rotorcraft approaches route deviations (potential pilot/aircraft induced conflict).
SO-FP-13	The ATCOs shall have the possibility to monitor the trajectories adherence to the SNI PinS procedures for arrival planned routes in case of loss of display/tool/support.

Table 13: Additional Safety Objectives (functionality and performance) in the case of internal failures

Table 14 presents the list of Integrity & Reliability Safety Objectives derived from the mitigation means during the failure approach.

3.8.2 Derivation of Safety Objectives (integrity/reliability)

The following Safety Objectives (integrity and reliability) defined in Table 18 describe the frequency limitation with which the above Solution System generated hazards could be allowed to occur. For the determination and mathematical calculation the relevant Risk Classification Scheme(s) from Guidance E.3 and SO mathematical calculation guidance in Guidance E.4 of Guidance to Apply the Safety Reference Material were used.

The calculation is done via the following formula:

$$SO = \frac{MTFoO_{relevant\_severity\_class}}{N\ x\ IM}$$

$MTFoO_{relevant\_severity\_class}$: Maximum Tolerable Frequency of Occurrence being the maximum probability of the hazard's effect

N: Overall number of operational hazards for a given severity class at a given barrier

IM: Impact Modification factor to take account of additional information regarding the operational effect of the hazard

In general the Impact Modification factor has a reference value of IM = 1. In case of a very high impact of a barrier failure and in case a hazard involves multiple (many aircraft) a higher value i.e. IM = 10 can be used.

ID	Safety Objectives
	The frequency of occurrence of a MAC shall not be greater than 1e-1 ***MTFoO*** per flight
	The frequency of occurrence of a MAC shall not be greater than 1e-3 ***MTFoO*** per movement
	The frequency of occurrence of a MAC shall not be greater than 1e-3 ***MTFoO*** per movement

Table 14: Safety Objectives (integrity/reliability)

3.9 Achievability of the Safety Criteria

The Safety Criteria set in section **Error! Reference source not found.** have been achieved through the specification of safety objectives (Functionality & Performance and Integrity) in sections **Error! Reference source not found.** to **Error! Reference source not found.**

The SAR will proceed with the Safe design at SPR level, deriving the Safety Objectives into Safety Requirements.

3.10. Validation & Verification of the Safety Specification

Results of the Safety Analysis by the different exercises can be found in PJ.02.05 V3 VALR.

4 Safe Design at SPR Level

4.1 Scope

This section addresses the following activities:

- Description of the Functional Model (see Guidance G.1.2 of [2]) of the end-to-end Solution ATM System – section 4.2 (not covered in this document: functional model have not been used for this solution OSED parts).
- Description of the SPR-level model (see Guidance G.2 of [2]) of the end-to-end Solution ATM System - section 4.3
- Derivation, from the Safety Objectives (Functionality and Performance) of section 3, of Safety Requirements for the SPR-level design - section 4.3
- Analysis of the operation of the SPR-level design under normal operational conditions – section 4.4
- Analysis of the operation of the SPR-level design under abnormal conditions of the Operational Environment - section 4.5
- Assessment of the adequacy of the SPR-level design in the case of internal failures and mitigation of the System-generated hazards - section 4.6
- Justification that the SAfety Criteria are capable of being satisfied in a typical implementation - section 4.7
- Realism of the SPR-level design - section 4.8
- Validation & verification of the Specification - section 4.9

4.2 The [TBD] Solution Functional Model

No functional model is developed for the PJ02-05. The safety activities at SPR level are based on the SPR-level model developed in section 4.3.1.

[…]

4.3 The PJ02.05 Solution SPR-level Model

4.3.1 Description of SPR-level Model

The following definition of the terms used in the logical SPR model is presented below.

Term	Definition	Where defined
ATM/ANS	ATM/ANS" shall mean the air traffic management functions as defined in Article 2(10) of Regulation (EC) No 549/2004, air navigation services defined in Article 2(4) of that Regulation, and services consisting in the origination and processing of data and formatting and delivering data to general air traffic for the purpose of safety-critical air navigation;	Regulation EC No 1108/2009
AIS	aeronautical information service' means a service established within the defined area of coverage responsible for the provision of aeronautical information and data necessary for the safety, regularity, and efficiency of air navigation;	EC Regulation 549/2004
ANS	'air navigation services' means air traffic services; communication, navigation and surveillance services; meteorological services for air navigation; and aeronautical information services;	EC Regulation 549/2004
ANSP	'air navigation service providers' means any public or private entity providing air navigation services for general air traffic;	EC Regulation 549/2004
ASM	'airspace management' means a planning function with the primary objective of maximizing the utilization of available airspace by dynamic time-sharing and, at times, the segregation of airspace among various categories of airspace users on the basis of short-term needs;	EC Regulation 549/2004
AFTM	'air traffic flow management' means a function established with the objective of contributing to a safe, orderly and expeditious flow of air traffic by ensuring that ATC capacity is utilized to the maximum extent possible, and that the traffic volume is compatible with the capacities declared by the appropriate air traffic service providers;	EC Regulation 549/2004
ATM	'air traffic management' means the aggregation of the airborne and ground-based functions (air traffic services, airspace management and air traffic flow management) required to ensure the safe and efficient movement of aircraft during all phases of operations;	EC Regulation 549/2004
ATS	'air traffic services' means the various flight information services, alerting services, air traffic advisory services and ATC services (area, approach and aerodrome control services);	EC Regulation 549/2004
ATC	'air traffic control (ATC) service' means a service provided for the purpose of: (a) preventing collisions: • between aircraft, and obstructions • in the manoeuvring area between aircraft and obstructions; (b) expediting and maintaining an orderly flow of air traffic;	EC Regulation 549/2004
COM	'communication services' means aeronautical fixed and mobile services to enable ground-to-ground, air-to -ground and air-to-air communications for ATC purposes;	EC Regulation 549/2004
MET	'meteorological services' means those facilities and services that provide aircraft with meteorological forecasts, briefs and observations as well as	EC Regulation 549/2004

	any other meteorological information and data provided by States for aeronautical use;	
SUR	'surveillance services' means those facilities and services used to determine the respective positions of aircraft to allow safe separation;	EC Regulation 549/2004
ASD	Airspace structures and flight procedures shall be properly designed, surveyed and validated before they can be deployed and used by aircraft.	EC Regulation 1108/2009

The figure below presents the SPR-level model of the PJ.02-05 solution. This model is a high-level architectural representation of the solution system design that is entirely independent of the eventual physical implementation. The model describes

- The functional block involved in the PJ-06-01 solution (orange blocks on the model). The functional blocks considered on this model are consistent with the ones in the EATMA model. The functional blocks are not system/tool. One tool can encompass several functional blocks (e.g. PC Aid tool encompass trajectory prediction and conflict management)
- The actors involved in the PJ-06-01 solution (blue blocks on the model)

Procedures are not presented on this model. However, they will be considered for the definition of the Safety Requirements.

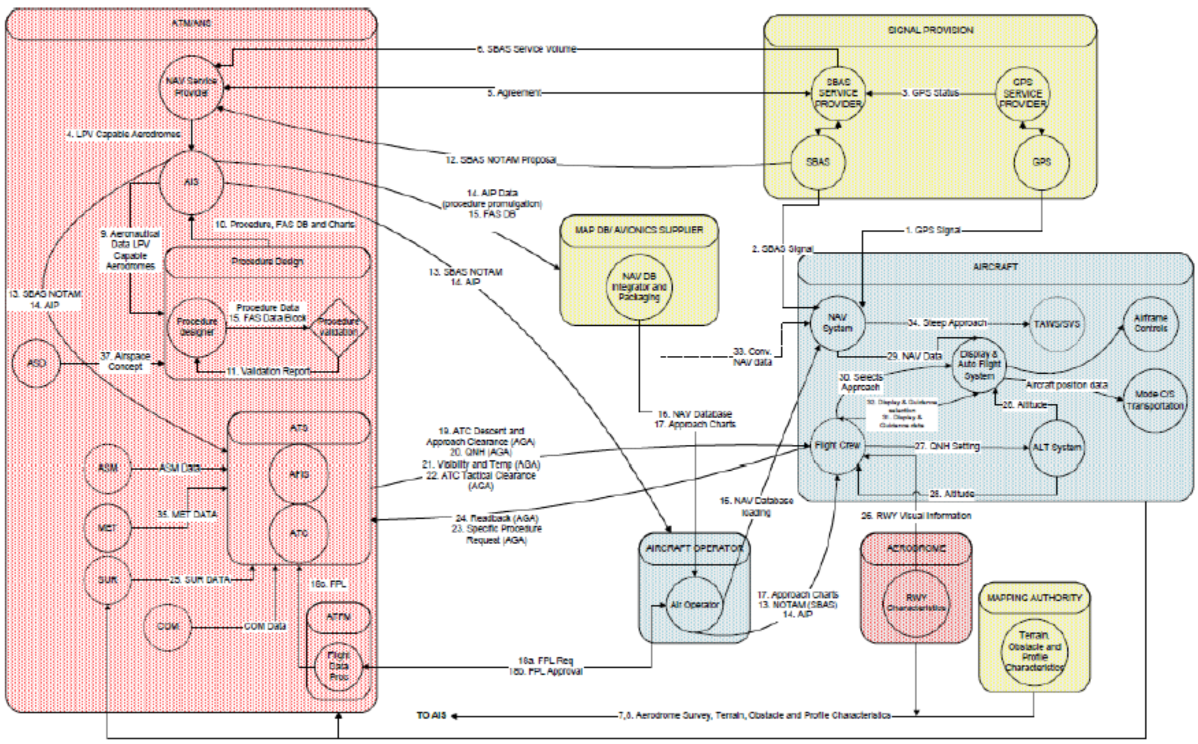
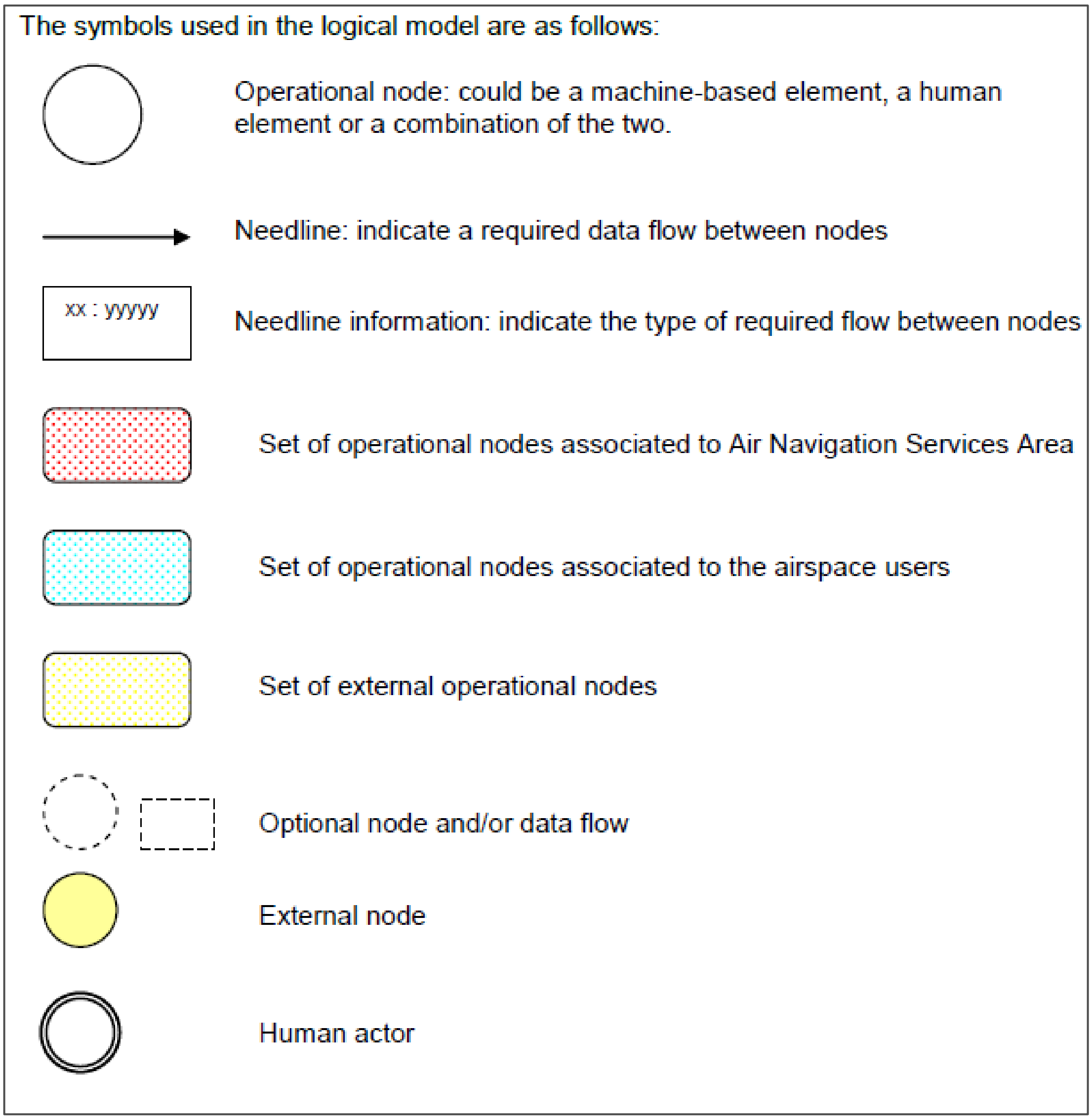


Figure 2: APV (-ADV) SPR level model



A Description of the ADV-APV approach SPR-level Model is made in [2] by identifying and describing all information exchanges that make up all information need lines between operational nodes. The tables identify who exchanges what information, with whom, why the information is necessary, and with what quality (requirements) the information exchange must occur.

4.3.1.1 Aircraft Elements

See section 4.3.1

4.3.1.2 Ground Elements

See section 4.3.1

4.3.1.3 External Entities

N/A

4.3.2 Task Analysis

[...]

4.3.3 Derivation of Safety Requirements (Functionality and Performance – success approach)

[...]

Safety Objectives (Functionality and Performance from success approach)	Requirement (forward reference)	Maps on to
SO 01 The ATCOs shall be able to perform tactical coordination between fixed-wing and rotorcraft in SNI PinS procedures for arrival planned routes	REQ-02.05-SAFE-PSNI.0320 REQ-02.05-SAFE-PSNI.0330 REQ-02.05-SAFE-PSNI.0350 REQ-02.05-SAFE-PSNI.0360 REQ-02.05-SAFE-PSNI.0370 REQ-02.05-SAFE-PSNI.0380 REQ-02.05-SAFE-PSNI.0390 REQ-02.05-SAFE-PSNI.0400 REQ-02.05-SAFE-PSNI.0410 REQ-02.05-SAFE-PSNI.0440 REQ-02.05-SAFE-PSNI.0460	ATC→FCs
SO 02 The ATCOs shall be able to monitor conformance to the approaches route for IFR rotorcraft operations, consequently, difficult to	REQ-02.05-SAFE-PSNI.0420 REQ-02.05-SAFE-PSNI.0430 REQ-02.05-SAFE-PSNI.0450	ATC→SUR

detect rotorcraft deviations (potential pilot/aircraft induced conflict)	REQ-02.05-SAFE-PSNI.0510	
SO 03 The ATCOs shall be provided with support to monitor trajectories adherence to the SNI PinS procedures for arrival planned routes	REQ-02.05-SAFE-PSNI.0420 REQ-02.05-SAFE-PSNI.0470	ATC→SUR

Table 15: Mapping of Safety Objectives to SPR-level Model Elements

Safety Requirement **(functionality & performance)** **[SPR-level Model Element]**	**Requirement**	**Derived from Table 16**
REQ-02.05-SAFE-PSNI.0320	The occurrence of an SBAS system failure during the final approach shall not compromise flight safety.	SO 01
REQ-02.05-SAFE-PSNI.0330	The capabilities to display the followed RNP shall be available to pilots in order to verify and control any possible RNP system failure.	SO 01
REQ-02.05-SAFE-PSNI.0350	In case of loss of signal integrity, the Navigation function shall allow the crew to select an alternative approach procedure or to start a missed approach procedure.	SO 01
REQ-02.05-SAFE-PSNI.0360	The system shall provide indication of loss of navigation capability to the pilot in less than 0.6 seconds in case of SBAS level of service unavailability.	SO 01
REQ-02.05-SAFE-PSNI.0370	In case of an initiation of a go-around due to a loss of GNSS, the FMS shall enable the use of other navigation means to comply with the performance requirements.	SO 01
REQ-02.05-SAFE-PSNI.0380	The Guidance function shall use its sensors to provide the guidance functionality with accuracy, integrity, continuity and availability compliant with APV requirements.	SO 01

REQ-02.05-SAFE-PSNI.0390	Flight crew shall select the APV arrival/approach or departure procedure to be flown from the rotorcraft FMS (the procedure being extracted from the NAV database system), including transition from RNP (with or without VNAV) to LPV guidance mode, based on compliance and certification with EASA AMC 20-27 and 20-28.	SO 01
REQ-02.05-SAFE-PSNI.0400	The APV operations data from the NAV database system shall be displayed to the flight crew, including degraded modes, in accordance with the published procedure (they are RNAV flight path and associated data –e.g. constraint-, timely display, combined RNP 0.3/1NM segments, change from the RNP segment to the LPV segment, missed approach and LPV approach data –e.g. ident, channel…) based on compliance and certification with EASA AMC 20-27 and AMC 20-28.	SO 01
REQ-02.05-SAFE-PSNI.0410	SBAS Service Provider shall inform the NAV Service Provider on a foreseen degradation of the SBAS system performance by providing a NOTAM in accordance with ICAO Annex 15., in order to preventable inform Flight crew on board or before the flight initiation.	SO 01
REQ-02.05-SAFE-PSNI.0420	The Final Approach Segment Data Block (FAS DB) description (including the CRC) shall be provided by the ANS Provider for navigation database coding in compliance with the aeronautical data quality requirements of ICAO Annex 10, ICAO Doc 9613 (PBN Manual) and ICAO Doc 8168 volume II.	SO 02 SO 03
REQ-02.05-SAFE-PSNI.0430	The airspace concept shall be designed with respect to the guidance given by PANS OPS 8168 volume II and ICAO Doc 9613 (PBN Manual).	SO 02
REQ-02.05-SAFE-PSNI.0440	Flight crew (Pilots) shall verify and ensure that the correct approach or departure has been selected before undertaking the -PINS procedure.	SO 01
REQ-02.05-SAFE-PSNI.0450	The probability of an LoA Type 1 or Type 2 error shall be no greater than $1x10^{-5}$ per flight.	SO 02
REQ-02.05-SAFE-PSNI.0460	In case of operational conditions different from ones taken as reference, rotorcraft operations shall be suspended giving priority to normal operations.	SO 01

	Rotorcraft operations shall be resumed when operational conditions abovementioned are restored.	
REQ-02.05-SAFE-PSNI.0470	Interactions between live trial rotorcraft procedures and other IFR procedures shall be available to Air traffic controllers.	SO 03
REQ-02.05-SAFE-PSNI.0510	At least three hours before the beginning of operations, a planning of activities shall be provided to Air traffic controllers.	SO 02

Table 16: Derivation of Safety Requirements (functionality and performance) from Safety Objectives

List of the identified assumptions derived from the SAFE Requirements of the Solution:

ID	Assumptions
	APV Display capable in case of GNSS failures. (was REQ-02.05-SAFE-PSNI.0340)
	Temporary orders of service during activity shall be available for all Units affected by rotorcraft operations. (was REQ-02.05-SAFE-PSNI.0480)
	Orders of service shall specify that rotorcraft operations are performed in VMC conditions. (was REQ-02.05-SAFE-PSNI.0490)
	An AIM shall be put in place in order to inform Airspace users of rotorcraft activities. (was REQ-02.05-SAFE-PSNI.0500)
	The best time slot available to perform the Flight Trial shall be identified taking into account the needs of airport ATS Units. (was REQ-02.05-SAFE-PSNI.0520)
	In order to avoid runway closures or military zones activation (TRA 424) F35 causing runway change from RWY 35L to RWY 35R.a coordination between Milano Malpensa TWR with Italian Airforce and Airport Management Company (SEA) shall be performed. (was REQ-02.05-SAFE-PSNI.0530)
	COPs between LIMC and Milano ACC (TMA/Approach Sectors) shall be provided for the transfer of responsibility of rotorcraft during procedure execution. (was REQ-02.05-SAFE-PSNI.0540)

Table 17: Assumptions made in deriving the above Safety Requirements

[...]

4.3.4 Traceability

As it was decided to use the SPR-level model, there is no traceability between FM-level model and SPR-level model in this document.

4.4 Analysis of the SPR-level Model – Normal Operational Conditions

[...]

4.4.1 Scenarios for Normal Operations

[...]

ID	Scenario	Rationale for the Choice
1		
2		
...		

Table 18: Operational Scenarios – Normal Conditions

4.4.2 Thread Analysis of the SPR-level Model – Normal Operations

[...]

4.4.2.1 Scenario # 1

[...]

4.4.2.2 Scenario # 2

[...]

4.4.2.3 Scenario # ....

[...]

4.4.3 Effects on Safety Nets – Normal Operational Conditions

[...]

4.4.4 Dynamic Analysis of the SPR-level Model – Normal Operational Conditions

[...]

4.4.5 Additional Safety Requirements (functionality and performance) – Normal Operational Conditions

[…]

ID [SPR-level Model element]	Description	Thread [Scenario # xx]	Action	Number

Table 19: Additional SR from Thread Analysis – Normal Operational Conditions

[…]

4.5 Analysis of the SPR-level Model – Abnormal Operational Conditions

This section is concerned with SPR-level Design is coherent with respect to the Safety Requirements (Functionality and Performance) derived for the abnormal operating conditions that were used to derive the corresponding Safety Objectives (success approach) in section 3.6.2.

4.5.1 Scenarios for Abnormal Conditions

Table below lists the abnormal operational scenario

ID	Scenario	Rationale for the Choice
	Approach PinS procedure with possible missed approach due to adverse weather conditions	

Table 20: Operational Scenarios – Abnormal Conditions

4.5.2 Derivation of Safety Requirements (Functionality and Performance) for Abnormal Conditions

Table below lists the abnormal conditions defined with the corresponding Safety Objectives (Functionality and Performance) to mitigate the consequences of the abnormal conditions as well as the corresponding Safety Requirements (Functionality and Performance).

Ref	Abnormal Conditions / SO (*Functionality and Performance)*	Mitigations (SR 0xx and/or A 0xx)

	Adverse weather conditions encounters (e.g.: strong wind, thunderstorm, …) / SO 04	The ATCOs shall assess the local weather conditions and shall support the pilot when approaching the MAPt (Missed Approach Point), to decide whether to continue or abort the approach.

Table 21: Safety Requirements or Assumptions to mitigate abnormal conditions

[…]

4.5.3 Thread Analysis of the SPR-level Model - Abnormal Conditions

4.5.3.1 Scenario # 1

[…]

4.5.3.2 Scenario # 2

[…]

4.5.3.3 Scenario # ….

[…]

4.5.4 Effects on Safety Nets – Abnormal Operational Conditions

[…]

4.5.5 Dynamic Analysis of the SPR-level Model – Abnormal Operational Conditions

[…]

4.5.6 Additional Safety Requirements – Abnormal Operational Conditions

[…]

ID [SPR-level Model element]	Description	Thread Action Number [Scenario # xx]

Table 22: Additional Safety Requirements from Thread Analysis – Abnormal Operational Conditions

4.6 Design Analysis – Case of Internal System Failures

4.6.1 Causal Analysis

System-generated hazards have been analysed in order to determine their causes and possible barriers to prevent them. The failure cases analysis provided the Safe Design at SPR level assessment captured in the next table:

ID	Hz Description	Causes	Possible barriers
HZ 001	Failure to perform tactical coordination between fixed-wing and rotorcraft in SNI PinS procedures for arrival planned routes	<u>Equipment</u> <u>Human:</u> - difficult to manage coordination between fixed-wing and rotorcraft in SNI PinS procedures (potential pilot/aircraft induced conflict) - coordination of SNI ops more workload demanding for ATCOs.	- (B10) - specific training for the coordination between fixed-wing and rotorcraft in SNI PinS procedures - procedures designed to mitigate strategic/pre-tactical conflicts
HZ 002	Failure to monitor conformance to the approaches route for IFR rotorcraft operations and to detect rotorcraft deviations (potential pilot/aircraft induced conflict)	<u>Equipment:</u> N/A (equipment failure) <u>Human:</u> - difficult to detect rotorcraft approaches route deviations (potential pilot/aircraft induced conflict) - conflict situations in IFR rotorcraft ops more workload demanding for ATCOs.	- (B5/B6/B7/B9) - training to ATCOS on IFR rotorcraft ops procedures. - trajectories shaped to avoid low converging angle segments.

ID	Hz Description	Causes	Possible barriers
HZ 003	Loss of display/tool/support to monitor the trajectories adherence to the SNI PinS procedures for arrival planned routes	Equipment: - HMI (Controller Human Machine Interaction Management) fail - Screen freeze Human: - N/A (human causes)	- (B5/B6/B7/B9) - Focus on importance of updating the system - ATCOs to be trained on operations without availability of the display/tool/support.

4.6.2 Common Cause Analysis

Following the Causal Analysis, the barriers and mitigations proposed for the hazards are captured in the next table in the form of Functionality & Performance Safety Requirements, additional to those determined during the design analysis for the success case in normal and abnormal operation conditions.

Safety Requirement		Derived from
Ref	Requirement	
SR FP 01	The ATCO/ shall be trained for to manage/coordinate fixed-wing and rotorcraft in SNI PinS procedures.	Hz-001 Hz-002
SR FP 02	The ATCO/Flight Crew shall check adherence of rotorcraft trajectory to the planned approach route	Hz-001 Hz-002
SR FP 03	ATCOs shall be trained/familiarized on the importance of updating the system (display/tool/support) with changes.	Hz-003

4.6.3 Formalization of Mitigations

[…]

4.6.4 Safety Requirements (integrity/reliability)

Integrity Safety Objectives from Section 3.8.2 are incorporated as quantitative Integrity & Reliability Safety Requirements (these safety objectives are not further allocated on the components of the SPR-level model because such allocation could depend on local implementation):

Hz	SR	Safety Requirement (Integrity/Reliability)
Hz-001	SR_IR_OPS_001	The frequency of occurrence of a MAC shall not be greater than 1e-1 ***MTFoO*** per flight
Hz-002	SR_IR_OPS_002	The frequency of occurrence of a MAC shall not be greater than 1e-3 ***MTFoO*** per movement
Hz-003	SR_IR_SYS_003	The frequency of occurrence of a MAC shall not be greater than 1e-3 ***MTFoO*** per movement

4.7 Achievability of the SAfety Criteria

The Safety Criteria set in section 3.5 have been achieved through the Safety Objectives identified in sections 3.6 to 3.8 have been derived into safety requirements (Functionality & Performance and Integrity) in sections 4.3 to 4.6.

The Safety Criteria should be achieved by implementing these safety requirements.

4.8 Realism of the SPR-level Design

4.8.1 Achievability of Safety Requirements / Assumptions

The Safety Requirements identified in section 4.2 to 4.5 have been determined and validated through safety workshop, based on the results of the validation activities as explained in section 4.8. The involvement of operational and technical experts during these workshops endure the achievability of the safety requirements and assumptions.

Some of these safety requirements have been evaluated during the validation activities, even if no formal traceability between the safety requirements and the safety validation objectives has been developed.

4.8.2 "Testability" of Safety Requirements

4.9 Validation & Verification of the Safe Design at SPR Level

[...]

5 Detailed Safe Design at Physical Level

N/A

6 Acronyms and Terminology

[…]

Term	Definition
AC	Advisory Circular
ADD	Architecture Definition Document
ADS-C	Automatic Dependent Surveillance - Contract
AIM	Accident Incident Model
AMSL	Above Mean Sea Level
AMC	Acceptable Means of Compliance
ANSP	Air Navigation Service Provider
APCH	Approach
APV	Approach Procedure with Vertical guidance
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATM	Air Traffic Management
AU	Airspace User
BADA	Base of Aircraft Data
CAA	Civil Aeronautics Authority
CDA	Continuous Descent Approach
CDFA	Continuous Descent Final Approach
CDO	Continuous Descent Operation
CDTI	Cockpit Display of Traffic Information
CNS	Communications, navigation and surveillance
CM	Context Management
COORD	Coordinator
CPDL-C	Controller Pilot Data Link Communications

CRC	Cyclic Redundancy Check
CTR	Control Zone
DA/H	Decision Altitude/ Height
DA	Decision Altitude
DB	Database
DOD	Detailed Operational Description
DRA	Direct Route Airspace
DSS	Desk System Suite Hardware
E-ATMS	European Air Traffic Management System
EGNOS	European Geostationary Navigation Overlay Service
ENB	Enabler
E-OCVM	European Operational Concept Validation Methodology
ETSO	European Technical Standard Order
EU-OPS	This refers to European Union (EU) regulations specifying minimum safety and related procedures for commercial passenger and cargo fixed-wing aviation
EXE	Executive
FAF	Final Approach Fix
FAP	Final Approach Point
FAS	Final Approach Segment
FAS DB	Final Approach Segment Data Base
FATO	Final Approach & Take-Off areas
FCS	Flight Control System
FMS	Flight Management System
FNHD	Finmeccanica Helicopters Division
FPDO	Flight Procedures Design Organization
FTA	Fix Tolerance Area

GPA	Glide Path Angle
GPS	Global Positioning System
GNSS	Global Navigation Satellite System
HMI	Human Machine Interface
HP	Human Performance
HRP	Heliport Reference Point
ICAO	International Civil Aviation Organization
ICP	Initial Climb Procedure
IDF	Initial Departure Fix
IFR	Instrument Flight Rule
ILS	Instrument Landing System
INTEROP	Interoperability Requirements
I/O	Input/Output
IRS	Interface Requirements Specification
JRE	Java Runtime Environment
LLR	Low Level IFR Routes
LPV	Localizer Performance with Vertical Guidance
LNAV	Lateral Navigation
MAHF	Missed Approach Holding Fix
MAP	Missed Approach
MAPt	Missed Approach Point
MCA	Minimum Crossing Altitude
MCDU	Multipurpose Control & Display Unit
MET	Meteorological
MLS	Microwave Landing System
MOC	Minimum Obstacle Clearance
M/M	Medium complexity / Medium density

NOTAM	Notice To AirMen
OCA	Obstacle Clearance Altitude
OCA/H	Obstacle Clearance Altitude/Height
OFA	Operational Focus Areas
OIS	Visual Identification Surface
OSED	Operational Service and Environment Definition
PANS-OPS	Procedures for Air Navigation Services – Aircraft Operations
PBN	Performance Based Navigation
PC	Personal Computer
PDG	Procedure Design Gradient
PDG	Procedure Design Gradient
PFD	Primary Flight Display
PI	Performance Indicator
PinS	Point-in-Space
PRE	Predictability
QFU	Aviation Q-code for magnetic heading of a runway
R&D	Research & Development
R/C	Rotorcraft
RF	Radius to Fix
RHP	Runway Holding Point
RNAV	Area Navigation
RNP	Required Navigation Performance
RTS	Real Time Simulator
RWY	Runway
SBAS	Satellite-Based Augmentation System
SESAR	Single European Sky ATM Research Programme
SID	Standard Instrument Departure

SJU	SESAR Joint Undertaking (Agency of the European Commission)
SME	Subject Matter Expert
SNI	Simultaneous non-interfering
SPR	Safety and Performance Requirements
SPV	Supervisor
SSR	Secondary Surveillance Radar
STAR	Standard Instrument Arrival
SUT	System Under Test
TAD	Technical Architecture Description
TIA	Turn Initiation Area
TMA	Terminal Manoeuvring Area
TS	Technical Specification
TSO	Technical Standard Order
UC	Use Case
VALP	Validation Plan
VALR	Validation Report
VALS	Validation Strategy
VNAV	Vertical Navigation
VP	Verification Plan
VR	Verification Report
VS	Verification Strategy
WIMS	Weather Information Management System
WL	Workload
WP	Waypoint
WPT	Waypoint
WP	Waypoint
XTK	Cross Track

Table 23: Acronyms and terminology

7 References

Safety

[1] SESAR, Safety Reference Material, Edition 4.0, April 2016

[2] SESAR, Guidance to Apply the Safety Reference Material, Edition 3.0, April 2016

[3] SESAR Safety Assessment Plan Template

[4] SESAR Solution PJ02.05 Safety Plan

[5] SESAR, Final Guidance Material to Execute Proof of Concept, Ed00.04.00, August 2015

[6] SESAR, Resilience Engineering Guidance, May 2016

[7] SESAR Solution 02-05 SPR-INTEROP/OSED Part I V3 (D4.1.012-1)

[8]

Appendix A Safety Objectives

A.1 Safety Objectives (Functionality and Performance)

A.2 Safety Objectives (Integrity)

Appendix B Consolidated List of Safety Requirements

B.1 Safety Requirements (Functionality and Performance)

B.2 Safety Requirements (Integrity)

Appendix C Assumptions, Safety Issues & Limitations

C.1 Assumptions log

The following Assumptions were necessarily raised in deriving the above Functional and Performance Safety Requirements:

Ref	Assumption	Validation
	APV Display capable in case of GNSS failures. (was REQ-02.05-SAFE-PSNI.0340)	Expert judgement
	Temporary orders of service during activity shall be available for all Units affected by rotorcraft operations. (was REQ-02.05-SAFE-PSNI.0480)	Expert judgement
	Orders of service shall specify that rotorcraft operations are performed in VMC conditions. (was REQ-02.05-SAFE-PSNI.0490)	Expert judgement
	An AIM shall be put in place in order to inform Airspace users of rotorcraft activities. (was REQ-02.05-SAFE-PSNI.0500)	Expert judgement
	The best time slot available to perform the Flight Trial shall be identified taking into account the needs of airport ATS Units. (was REQ-02.05-SAFE-PSNI.0520)	Expert judgement
	In order to avoid runway closures or military zones activation (TRA 424) F35 causing runway change from RWY 35L to RWY 35R.a coordination between Milano Malpensa TWR with Italian Airforce and Airport Management Company (SEA) shall be performed. (was REQ-02.05-SAFE-PSNI.0530)	Expert judgement
	COPs between LIMC and Milano ACC (TMA/Approach Sectors) shall be provided for the transfer of responsibility of rotorcraft during procedure execution. (was REQ-02.05-SAFE-PSNI.0540)	Expert judgement

Table 24: Assumptions log

C.2 Safety Issues log

The following Safety Issues were necessarily raised during the safety assessment:

Ref	Safety issue	Resolution

Table 25: Safety Issues log

C.3 Operational Limitations log

The following Operational Limitations were necessarily raised during the safety assessment:

Ref	Operational Limitations	Resolution

Table 26: Operational Limitations log

Appendix D RCS for MAC in En-route & TMA operational environments and for Controlled Flight Into Terrain

The maximum tolerable frequency of occurrence for each severity class related to MAC accidents as defined in section § E.3.1 [2].

Severity Class	*Hazardous situation*	*Operational Effect*	*MTFoO [per fh]*
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
MAC-SC5	A situation where, on the day of operations, a tactical conflict (planned) was prevented by Traffic Planning and Synchronization.	Pre tactical conflict (MF5.2)	1e-1

Table 27: Risk Classification Scheme for Mid Air Collision (TMA and En-Route)

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

The maximum tolerable frequency of occurrence for each severity class related to Controlled Flight Into Terrain as defined in section § E.3.3 [2].

Severity Class	*Hazardous situation*	*Operational Effect*	*MTFoO [per flgt]*
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]	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 28: Risk Classification Scheme for CFIT

[note 1] as per the CFIT model, the aircraft trajectory geometry does not allow to prevent the collision with terrain/water/ obstacle for a near CFIT. Thus Near CFIT is classified as an 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

-END OF DOCUMENT-