INDUSTRIAL RESEARCH

sesar JOINT UNDERTAKING

SESAR Solution 53B SPR-INTEROP/OSED for V3 – Part II – Safety Assessment Report

Deliverable ID:	**D2.2.101**
Dissemination Level:	**PU**
Project Acronym:	**PJ18W2 4DSKYWAYS**
Grant:	**872320**
Call:	**H2020-SESAR-2019-1**
Topic:	**SESAR-IR-VLD-WAVE2-09-2019**
Consortium Coordinator:	**EUROCONTROL**
Edition Date:	**19th April 2023**
Edition:	**01.00.00**
Template Edition:	**00.00.04**

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Authoring & Approval

Authors of the document

Beneficiary	Date
INTEGRA	03/03/2023

Reviewers internal to the project

Beneficiary	Date
SKYGUIDE	07/03/2023
BULATSA	16/03/2023
AIRBUS	16/03/2023
EUROCONTROL	30/03/2023
PANSA	05/04/2023
Egis	05/04/2023

Reviewers external to the project

Beneficiary	Date

Approved for submission to the S3JU By - Representatives of all beneficiaries involved in the project

Beneficiary	Date
AIRBUS	19/4/2023*
B4	19/4/2023
COOPANS	19/4/2023
ENAIRE	19/4/2023*
DFS	19/4/2023*
DSNA	19/4/2023*
EUROCONTROL	19/4/2023
ENAV	19/4/2023*
INDRA	19/4/2023
NATS	19/4/2023
AT-ONE	19/4/2023*
SKYGUIDE	19/4/2023
THALES LAS	19/4/2023*

* Silent approval

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Rejected By - Representatives of beneficiaries involved in the project

Beneficiary	Date

Document History

Edition	Date	Status	Beneficiary	Justification
00.00.01	21/01.2022	Draft	INTEGRA	New document
00.00.02	03.03.2023	Draft	INTEGRA	Completed section 4-6
00.00.03	23.03.2023	Final Draft	INTEGRA	Update after the review
00.01.00	06.04.2023	For approval	INTEGRA	Ready for submission to SJU
00.02.00	12/4/2023	Pre-submission	EUROCONTROL	Quality check and PMB approvals

PJ18W2 4DSKYWAYS

SOLUTION 53B: IMPROVED PERFORMANCE OF CD/R TOOLS ENABLED BY REDUCED TRAJECTORY PREDICTION UNCERTAINTY

This Safety Assessment Report is part of a project that has received funding from the SESAR3 Joint Undertaking under grant agreement No 872320 under European Union's Horizon 2020 research and innovation programme.

Abstract

This document specifies the results of the safety assessments carried out in SESAR 2020 Wave 2 by Project PJ18-Solution 53-B 4DSkyways.This Safety Assessment Report (SAR) is contributing to the /Safety and Performance Requirements (SPR) - Interoperability (INTEROP) / Operational Service and Environment Definition (OSED) and Technical Specifications (TS)/Interface Requirement Specification (IRS) documents.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Table of Contents

EUROPEAN PARTNERSHIP

Co-funded by the European Union

EUROPEAN PARTNERSHIP
Co-funded by the European Union

List of Tables

EUROPEAN PARTNERSHIP

Co-funded by the European Union

List of Figures

EUROPEAN PARTNERSHIP

Co-funded by the European Union

1 Executive Summary

This document contains the Specimen Safety Assessment Report for the application of the PJ.18-W2-53B Solution.

The Safety Assessment Report (SAR) has been generated by the safety assessment activities in support of the Design and Validation activities according to SESAR Safety Reference Material for ATS operational solution.

It addresses the following activities:

- derivation of Safety Requirements at ATS Service level (SRS) in view of mitigating the relevant risks inherent to aviation in normal conditions of operation
- assessment of the adequacy of the ATS operational services provided by the PJ.18-W2-53B Solution under abnormal conditions of the Operational Environment and derivation of necessary SRSs
- assessment of the adequacy of the ATS operational services provided by the Solution in the case of internal failures and mitigation of the Solution functional system-generated hazards through derivation of SRSs
- introduction of the design model of the Solution functional system used within the scope of the safety assessment
- derivation of Initial Safety Requirements (functionality & performance) at Design level (SRD) in normal and abnormal conditions of operation from the SRS (functionality & performance)
- assessment of the adequacy of the design in the case of internal failures and mitigation of the Solution operational hazards through derivation from SRS (integrity/ reliability) of Initial Safety Requirements (functionality & performance) and Safety Requirements (integrity & reliability) at Design level (SRD).

EUROPEAN PARTNERSHIP

Co-funded by the European Union

2 Introduction

This document reports on the safety assessment activities performed in the scope of the Solution PJ.18-W2-53B in line with SESAR Safety Reference Material [3].

2.1 Background

This solution is a progression of the work performed in SESAR Wave 1 by solutions PJ.10-02a2, PJ.10-02b, PJ.18-06a, PJ.18-06b and PJ.31. In particular, improved performance of separation management tools, which forms the subject of PJ.18-W2-53B, is a progression of Wave 1 solution PJ10-02a2 (to V2 on-going), and therefore this SPR-INTEROP/OSED inherits much of the concepts and requirements developed by that solution.[1]

2.2 General Approach to Safety Assessment

This safety assessment is conducted as per the SESAR Safety Reference Material (SRM) which itself is based on a twofold approach:

- a success approach which is concerned with the safety of the Solution operations in the absence of failure within the end-to-end Solution functional system, encompassing both Normal operation and Abnormal conditions,
- a conventional failure approach which is concerned with the safety of the Solution operations in the event of failures within the end-to-end Solution functional system.

These two approaches are applied to the derivation of safety properties at each of the successive lifecycle stages of the Solution development (Safety Requirements at service level and at design level).

The main objective of the Solution PJ.18-W2-53B is to improve Separation Management Tools in order to increase the quality of separation management services and to support controllers in the separation management tasks i.e., the way ATCOs interact and make use of Separation Management Tools in view of delivering ATS.

Based on the safety impact of the solutions, PJ.18-W2-53B Solution is considered an ATS operational solution and aims at achieving V3 maturity level in the scope of the Wave 2 activities.

2.3 Scope of the Safety Assessment

Building on top of the safety assessment initiated in Wave 1, the following aspects per phases of safety assessment lifecycle need to be covered in relation to the maturity level V3 (targeted by the Solution at the end of Wave 2):

- V1 - through re-visiting the initial identification of safety implications of the Change and the definition of Safety Criteria performed in Wave 1.

[1] The opinions expressed herein reflect the author's view only. Under no circumstances shall the SESAR3 Joint Undertaking be responsible for any use that may be made of the information contained herein.

- V2 – through updating the ATS service level Safety Requirements (SRS), previously referred to as Safety Objectives in Wave 1, to take into account the design developments of PJ.18-W2-53B in Wave 2 , in view of mitigating the relevant risks inherent to aviation in normal conditions of operation, abnormal conditions of the operational environment and in the case of internal failures of the functional system in the scope of the Solution. And through updating the safety requirements at initial design level (previously referred to as Safety Requirements at SPR level in Wave 1).
- V3: -e.g. safe refined design (a second iteration of the process conducted at the safe initial design level, mainly deriving Safety Requirements at refined design level – rSRD to be documented as appropriate in SPR-INTEROP/OSED and TS/IRS).

Since the properties of the operational environment (OE) are crucial to the safety assessment, this assessment is specific to the OE defined in PJ18-W2-53B INTEROP/OSED for V3 [5] and consequently, the term 'specimen' safety assessment needs to be used.

2.4 Layout of the Document

Section 1 presents the executive summary of the document.

Section 2 provides background and presents the principles of the safety assessment in SESAR Programme and the scope of this safety assessment.

Section 3 addresses the scene of the safety assessment, operational concept, operational environment description, and intended use of the service.

Section 4 addresses the safety specification at operational service level (mainly establishing Safety Requirements at Service level - SRS).

Section 5 is dedicated to safe refined design (a second iteration of the process conducted at the safe initial design level, mainly deriving Safety Requirements at refined design level).

Section 6 demonstrates the achievability of safety requirements.

Section 7 lists Acronyms used in the document.

Section 8 provides the documents referred to in this Safety Assessment Report.

Appendix A presents the preliminary safety system assessment.

Appendix B describes the process of derivation of the Safety Requirements at ATS Service level (SRS) for Normal conditions of operation.

Appendix C describes the process of derivation of the Safety Requirements at ATS Service level (SRS) for Abnormal conditions of operation.

Appendix D describes the process of derivation of Safety Requirements at ATS Service level (SRS) to mitigate system generated hazards.

Appendix E describes the process of derivation of the Safety Requirements at Design level (SRD) for normal conditions of operation.

Appendix F describes the process of derivation of the Safety Requirements at Design level (SRD) for abnormal conditions of operation.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix G describes the process of derivation of the Safety Requirements at Design level (SRD) for mitigate system generated hazards.

Appendix H demonstrates achievability of Safety Criteria.

Appendix I presents safety assumption log.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

3 Setting the Scene of the safety assessment

3.1 Operational concept overview and scope of the change

Solutions PJ.18-W2-53A and PJ.18-W2-53B, together, improve Separation Management and Monitoring Tools (planned and tactical layers) in the en-route and TMA operational environments in order to increase the quality of separation management services, reducing controller workload per aircraft, reducing separation buffers and facilitating more efficient controller team organisations.

The table below illustrates the mapping of PJ.18-W2-53B to its Wave 1 predecessor solutions, and shows how the targeted maturity of its OI steps is consistent with the maturity achieved by the corresponding Wave 1 OI steps.

Wave 1 Solution	OI Step	OI Title	Maturity Achieved	Wave 2 Solution	OI Step	OI Title	Maturity Targeted
PJ.10-02a2	CM-0209-b	Conflict Detection and Resolution in En-Route using aircraft data in Predefined and User Preferred Routes environments	V2 ongoing	PJ.18-W2-53B	CM-0209-b	Improved Separation Management with the use of Aircraft Data in Conflict Detection and Resolution Tools in En-Route Predefined and User Preferred Routes environments	V3
PJ.18-06a	POI-0012-IS	ATC Planned Trajectories improvement with new ADS-C reports, eFPL and surveillance information	V2		CM-0212	Improved Separation Management with the use of Aircraft Data in Conflict Detection and Resolution Tools in the TMA	V3

Table 1: Mapping of PJ.18-W2-53B Wave 1 Solutions

Solution PJ.18-W2-53B encapsulates the more mature separation management elements for which V3 maturity is targeted. This solution builds on the work performed in Wave 1 solutions PJ.10-02a and PJ.18-06a and addresses the improvement of conflict detection and resolution tools that are derived from the improvement of ground Trajectory Prediction (TP) with the use of advanced data from ATN B2 ADS-C reports messages as defined in the EUROCAE standards ED228A and ED75C and improved meteorological data.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

The improvements of ground TP in Solution PJ.18-W2-53B address the use of ADS-C data beyond the items that were studied in Wave 1 (gross mass, speed schedule, TOC and TOD altitudes, and the predicted speeds at route points) to address in particular:

- The use of the EPP profile to calibrate the BADA performance model;
- Improvements in the calculations of turning manoeuvres thanks to the use of turn radius and the turning strategy (overfly vs fly-by);
- The implementation of catch-up manoeuvres (modelling the interception of an aircraft in descent with its optimal descent profile).

In addition, the solution encompasses the handling of MET data and other surveillance data from aircraft (ADS-C reports containing wind and temperature at current aircraft position, NOWCAST from Mode S enhanced surveillance data, ADS-B out reports).

In continuation of the work performed in Wave-1 PJ.10-02a2 using ADS-C MET data to improve CD/R functions, the scope is further enhanced to improve the TP performance of ground trajectories by creating a local MET grid. This local MET grid is composed of ADS-C MET data (downlinked from various ADS-C equipped aircraft in the airspace) overlaid with the MET provider forecast data. The overlaying of ADS-C MET data is carried out by extrapolating in a regressive way so that the applicability of its usage in the ground TP calculations is limited by spatial and/or temporal bounds from the point of its downlink to the ground. The resultant MET grid is used to determine applicable MET parameters for each point in the AoI for ground TP calculations and is applied in both TMA and en-route airspace.

The reduced uncertainty in the TP and the use of the aircraft performance extracted from ADS-C EPP reports in the CD/R Tools, allowing a more accurate calculation of the detection envelopes (thinner envelopes) are expected to and improve the usability of CD/R tools and allow the better identification of actual conflicts. Furthermore, the improved TP should provide a more reliable sector sequence (particularly for vertically evolving flights in complex airspace), easing the burden of coordination and transfer between sectors.

The technical mechanisms that are used to improve the ground TP are described in the Technical Specification [8].

The OIs addressed by PJ.18-W2-53B with their respective enablers are listed in the table overleaf.

OI Steps ID	OI Steps Title	Enabler ID	Enabler Title	OI Step/Enabler Coverage
CM-0209-b	Improved Separation Management with the use of Aircraft Data in Conflict Detection and Resolution	A/C-37a	Downlink of trajectory data according to contract terms (ADS-C) compliant to ATN Baseline 2 (FANS 3/C)	OI step • Full Enabler • Required • Use
		A/C-48a	Air broadcast of position/vector (ADS-B OUT) compliant with DO260B	Enabler • Optional • Use

EUROPEAN PARTNERSHIP

Co-funded by the European Union

	Tools in En-Route Predefined and User Preferred Routes environments	ER APP ATC 100	4D trajectory management by synchronization or air and ground trajectories through EPP	Enabler • Required • Use
		ER APP ATC 104b	Adapt Controller Conflict Detection and Resolution Tools to Use Enhanced Trajectory Prediction	Enabler • Required • Develop
		ER APP ATC 167	ATC Planned Trajectories improvement with new ADS-C reports, and surveillance information	Enabler • Required • Develop
		ER APP ATC 200	ATC Improvement to receive and use more granular MET forecasts	Enabler • Required • Develop
		ER APP ATC 201	ATC Improvement to build and use local MET model using ADS-C reported MET data from A/Cs	Enabler • Required • Develop
		ER APP ATC 82	Enhance EN/APP ACC to use eFPL data	Enabler • Optional • Use
		ER APP ATC 149a	Air-ground data exchange to support i4D – Extended Projected Profile (EPP)	Enabler • Optional • Use
		ER APP ATC 214	Conflict Detection envelope trajectories improvement with new ADS-C reports	Enabler • Optional • Develop
CM-0212[2]	Improved Separation Management with the use of Aircraft Data in Conflict Detection and Resolution Tools in the TMA	A/C-37a	Downlink of trajectory data according to contract terms (ADS-C) compliant to ATN Baseline 2 (FANS 3/C)	OI step • Full Enabler • Required • Use
		A/C-48a	Air broadcast of position/vector (ADS-B OUT) compliant with DO260B	Enabler • Optional • Use
		ER APP ATC 100	4D trajectory management by synchronization or air and ground trajectories through EPP	Enabler • Required • Use

[2] Enablers assigned via Change Request 07135.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

		ER APP ATC 104b	Adapt Controller Conflict Detection and Resolution Tools to Use Enhanced Trajectory Prediction	Enabler • Required • Develop
		ER APP ATC 167	ATC Planned Trajectories improvement with new ADS-C reports, and surveillance information	Enabler • Required • Develop
		ER APP ATC 200	ATC Improvement to receive and use more granular MET forecasts	Enabler • Required • Develop
		ER APP ATC 201	ATC Improvement to build and use local MET model using ADS-C reported MET data from A/Cs	Enabler • Required • Develop
		ER APP ATC 82	Enhance EN/APP ACC to use eFPL data	Enabler • Optional • Use
		ER APP ATC 149a	Air-ground data exchange to support i4D – Extended Projected Profile (EPP)	Enabler • Optional • Use
		ER APP ATC 214	Conflict Detection envelope trajectories improvement with new ADS-C reports	Enabler • Optional • Develop

Table 2: SESAR Solution PJ18-W2-53B Scope and related OI steps and enablers

3.2 Solution Operational Environment and Key Properties

The detailed description of the solution operational environment and key properties is provided in the section 3.2 of the SESAR Solution 53 B Final SPR-INTEROP/OSED for V3 – Part I [5].

3.3 Stakeholders' expected benefits with potential Safety impact

Enhanced Conflict Management shall enhance the following KPIs in the provision of separation in both En Route and TMA environments:

- Sector (Traffic) Capacity, in particular in dense/congested areas
- ATCO Cost Efficiency
- Predictability
- Flight Efficiency (Time and distance, fuel)
- While maintaining the overall level of Safety at ECAC level

This is expected to be achieved through:

- Advanced conflict detection and resolution tools fed by most accurate trajectory predictions (including based on ADS-C data), accurate aircraft position and other available aircraft derived data, and fully compatible with 2D RNP environments.

Therefore, following impacts have been identified associated with Solution 53B:

Area	Impact with respect to the reference scenario/ previous working methods
1. Human actors' roles and responsibilities;	The affected human actors are ATC Executive Controller, ATC Planning Controller for en-route and TMA sectors and no changes in the roles and responsibilities have been identified.
2. Operating methods (procedures), tasks, practices, change in teams and communication (e.g. task redistribution within the planner–executive controllers' team), change in human-performance-related transition factors (staffing, competence, acceptance, and job satisfaction)	Due to new functionality/ies of the CD/R tools (e.g. what next) some changes to the operating methods are expected. Improvements in performance of controller's tasks is expected due to advanced conflict detection and resolution tools. More accurate information with a longer look-ahead time is expected to improve controllers' task performance due to an increased opportunity for the controllers to optimise trajectories. At the same time, provision of the resolution support for some conflicts will reduce their cognitive workload. No changes in team composition and task allocation were identified. Due to availability of more accurate data, and more efficient tools, the job satisfaction is expected to increase. The controllers that are able to solve conflict in more efficient manner, and therefore potentially decrease their workload, are likely to have higher job acceptance. No changes in competence requirements, recruitment and selection or training needs were identified.
3. Technical systems (architecture, functionalities and performance);	The performance of technical system is expected to improve due to more accurate trajectory predictions available (including EPP), accurate aircraft position and additional advanced MET information. It is expected that nuisance/spurious alerts are reduced to minimum.
4. Human and technical systems: allocation of tasks (man–machine) and new or modified human–machine interface (HMI)	The support tools reduce the need for the ATCOs to actively detect separation infringements to minimum and situational awareness is increased through highlighting relevant traffic only.
5. Impact on services other than the service being changed	No impact on other services was identified

Table 3 The impact of the change introduced by PJ18-W2-53B

3.4 Safety Criteria

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Based on the information collected during the HP&SAF scoping & change assessment session (encompassing the preliminary hazard identification) and on the hazards identified in sub-sections 4.2.1 and 4.2.2, the Safety Criteria (SAC) for PJ18-W2-53B have been identified and are listed in Table 4. Identification of the following SACs is driven by the ENR and TMA Mid Air Collision AIM model.

SAC ID	Description	Barrier / Precursor
SAC-18-W2-53b-ER-TMA - 001	There shall be no increase in the number of planned (tactical) conflicts arising from inadequate information for conflict management, ATCO failure to identify conflict in time and/or inadequate ATCO conflict management, taking into consideration increase in traffic.	B5 Plan Induced Conflict Management/ MF5.1 Planning Conflicts
SAC-18-W2-53b-ER-TMA - 002	There shall be no increase in ATC-induced tactical conflicts arising from inadequate resolution strategy taking into consideration increase in traffic.	B7 ATC Induced Conflict Management/ MF7.1 ATC induced Tactical conflict
SAC-18-W2-53b-ER-TMA - 003	There shall be no increase in pre-tactical conflicts due to Inadequate Trajectory Info taking into consideration increase in traffic	MF10 Pre-tactical Conflicts MB10.1.1.2 Inadequate Trajectory Info

Table 4 Safety Assessment Criteria for SolutionPJ18-W2-53.

SACs' Rationale: Due to improvement of TP, availability of downlinked trajectory data and more accurate MET information, and thanks to improved performance of the CD&R tools, the ATCO is able to timely identify relevant conflicts and to apply adequate resolution strategies.

The performance benefits are expected due to the use of ADS-C EPP data, Mode-S data, ADS-B data and MET data acquired and downlinked from the aircraft to improve ground TP (Planned and Tactical trajectories). In particular:

- Applying reverse engineering to the EPP profile to compute adjustment factors to tune aircraft performances (e.g. Thrust/energy) in the ground TP for the given trajectory (planned, tactical, What-If, What-Else …).
- Use of new EPP data, i.e.: type of turns.
- Extrapolating EPP data for the computation of what-if trajectories (lateral, speed, flight level).
- Use of the downlinked SFL by ground systems with EPP integration of ground constraints.
- Real-time tuning/optimization of the BADA parameters used in prediction and to implements a "catch-up" manoeuvre.

Improvements of the Conflict Detection & Resolution tools include:

- Identification of improved vertical profiles through non-penalising constraints.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

- Improvement of CD&R envelope detection as a result of improved predicted Trajectory and use of airborne downlinked data (EPP)
- Tactical MTCD operational improvement resulting from ADS-C-enhanced TP.
- Enhancement of CD&R tools with MET information and the resulting operational improvement.

Figure 1 illustrates the anchoring of the SACs into the ENR Mid Air Collision simplified AIM model.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

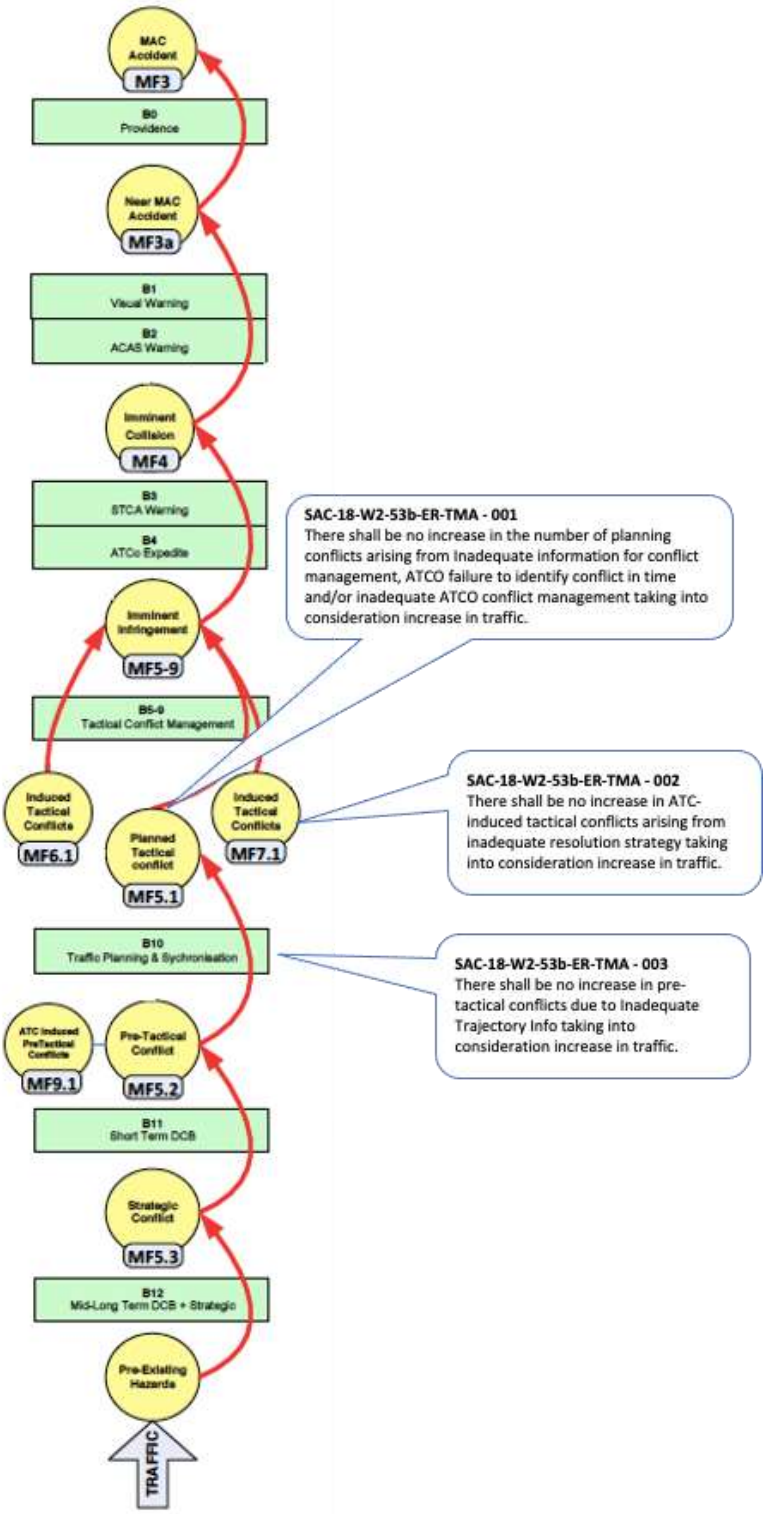

Figure 1 ENR-TMA Mid Air Collision Simplified AIM and related SACs.

4 Safety specification at ATS service level

This section provides the Safety Requirements at Service level for the Solution PJ.18-W2-53B.

The Safety Requirements at ATS Service level (SRS) specify the desired safety behaviour of the change at its interface with the ATS operational context considering normal and abnormal conditions of the context (success approach) and the failures of the functional system (failure approach).

The interface of the change with the ATS operational context might be at the level of the ATS service provided by the Solution functional system to an aircraft or a group of aircraft (i.e. the WHAT of the ATS service specification) or at the level of the specification of the ATS service in terms of the ATCOs and Pilots action, mutual interaction and use of functionalities/information/other services (i.e. the HOW of the ATS service specification).

SRS are placed on the services of the Solution PJ.18-W2-53B functional system that are changed or affected by the change (through change in behaviour or through new interactions introduced).

4.1 Overview of activities performed

This section addresses the following activities:

- derivation of Safety Requirements at ATS Service level (SRS) in view of mitigating the relevant risks inherent to aviation in normal conditions of operation– section 4.2
- assessment of the adequacy of the ATS operational services provided by the Solution under abnormal conditions of the Operational Environment & derivation of necessary SRSs – section 4.3
- assessment of the adequacy of the ATS operational services provided by the Solution in the case of internal failures and mitigation of the Solution functional system-generated hazards through derivation of SRSs – section 4.4
- verification of the operational safety specification process (mainly about obtaining Backing evidence from the properties of the processes by which Direct Evidence was gleaned) – section 4.5.

4.2 Mitigation of Risks Inherent to Aviation – Normal conditions

The set of Safety Requirements at the ATS Service level (SRS) in this section specifies the desired safety behaviour of the change at its interface with the operational context considering normal conditions.

The SRS are derived taking into account:

- All relevant Use Cases
- EATMA Models at operational specification level (NOV-5 diagrams).
- Impact on adjacent airspace or on neighbouring ATM Systems.

4.2.1 Safety Requirements at ATS Service level (SRS) for Normal conditions of operation

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Based on the hazards inherent to aviation identified in A.1 and following Guidance E.3 of SESAR Safety Reference Material, in Table 5 are presented the ATS operational services potentially impacted by the Change provided in the relevant operational environment to address and mitigate the hazards inherent to aviation (the change impacts either the WHAT or the HOW of the operational services).

ID	ATS Operational Service	Hazards inherent to aviation
ATS-01	Separation Provision • Provide Aircraft-to-Aircraft Separation: The ATCO is responsible to provide the required separation between aircraft at all time. • ATC Planning Conflict Detection: The PC is responsible to detect conflicts between two or more aircraft in a planning time horizon. Planning Conflict Detection tools can support the PC to carry out his work. • ATC Planning Conflict Resolution: The PC is responsible to solve conflicts between two or more aircraft in a planning time horizon. Planning Conflict Resolution tools can support the PC to carry out his work. • ATC Tactical Conflict Detection: The EC is responsible to detect conflicts between two or more aircraft in a tactical time horizon. Tactical Conflict Detection tools can support the EC to carry out his work. • ATC Tactical Conflict Resolution: EC is responsible to solve conflicts between two or more aircraft in a tactical time horizon. Tactical Conflict Resolution tools can support the EC to carry out his work. • Pre-tactical planning & coordination: The ATCO is responsible for the pre-tactical planning and coordination of all flights allocated to him. • ATC short term conflict detection: The EC is responsible to detect conflicts between two or more aircraft in a short-term time horizon. Short-Term Conflict Detection and Resolution tools support the EC in this task. • ATC short term conflict resolution: The EC is responsible to solve conflicts between two or more aircraft in a short-term time horizon. Short Term Conflict Detection and	Hi#1: Situation in which the intended trajectories of two or more aircraft are in conflict

EUROPEAN PARTNERSHIP

Co-funded by the European Union

	Resolution tools support the controller in this task.	
ATS-02	Separation Provision The ATCO is responsible to provide separation between aircraft and adverse weather area.	Hi#2: Aircraft encounters with severe weather conditions

Table 5: ATS Operational services potentially impacted and Hazards inherent to aviation.

In Table 6 is provided the consolidated list of the SRS for normal conditions of operation that have been derived in Appendix B.

These SRS are also included in the Section 4 of SPR-INTEROP/OSED Part I in order to ensure a correct and complete safety specification at operational level in normal conditions of operation.

SRS ID	SRS for Normal conditions of operation	Related SAC
SRS-001	Conflict detection tool shall indicate pairs of aircraft which have planning encounters at the entry or exit sector boundary based on the improved TP data (i.e., airborne downlinked MET and Trajectory (EPP) data).	SAC-18-W2-53B-ER-TMA -001 SAC-18-W2-53B-ER-TMA -003
SRS-002	The planning controller shall assess the exit conditions based on ATC Planned Trajectory using airborne downlinked MET and Trajectory (EPP) data.	SAC-18-W2-53B-ER-TMA -001 SAC-18-W2-53B-ER-TMA -003
SRS-003	The planning controller shall assess trajectory profile through the AoR for tactical controller suitability based on improved planned trajectory prediction, using airborne downlinked MET and Trajectory (EPP) data.	SAC-18-W2-53B-ER-TMA -001 SAC-18-W2-53B-ER-TMA -003
SRS-004	EC shall determine whether there are any problems between the aircraft's trajectory profiles based on improved planned trajectory prediction, using airborne downlinked MET and Trajectory (EPP and Mode S) data.	SAC-18-W2-53B-ER-TMA -001 SAC-18-W2-53B-ER-TMA -003

Table 6: List of SRS (functionality and performance) for normal conditions of operation

4.2.2 Additional SRS related to adjacent airspace or neighbouring ATM Systems

No requirements related to neighbouring ATM systems were identified.

4.3 Mitigation of Risks Inherent to Aviation - Abnormal conditions

The Safety Requirements at ATS Service level (SRS) derived for Abnormal conditions refer to the ability of the Solution to work through (robustness), or at least recover from (resilience) any abnormal

EUROPEAN PARTNERSHIP

Co-funded by the European Union

conditions, external to the Solution functional system, that might be encountered relatively infrequently (i.e. abnormalities of the context in which the Solution functional system is intended to operate).

4.3.1 Identification of Abnormal Conditions

The following list of abnormal conditions has been identified as relevant for PJ.18-W2-53B based on the review of relevant documents from WAVE 1. In the following step, the safety and operational experts from the solution have revised the impact.

- ABN-01 Bad weather (CBs, turbulences, icing)
- ABN-02 Sudden closure of airspace (SUA)
- ABN-03 Severe ATC technical system failure - Total loss of surveillance system
- ABN-04 Severe ATC technical system failure - Total loss of air/ground communication system
- ABN-05 Severe ATC technical system failure - Total loss of FDPS
- ABN-06 Severe ATFCM technical system failure - Total loss of local DCB tool
- ABN-07 Aircraft in emergency
- ABN-08 Severe aircraft technical system failure - Radio communication failure
- ABN-09 Severe aircraft technical system failure - Transponder failure

4.3.2 Safety Requirements at ATS Service level (SRS) for Abnormal conditions of operation

The details of the derivation process of the SRS for abnormal conditions of operation are provided in Appendix C. No new SRS were identified.

4.4 Mitigation of System-generated Risks (failure conditions)

The SRS provided in this section complete the safety specification of the Solution PJ.18-W2-53B at operational service level, providing the adequate mitigation against the possible adverse effects that failures internal to the Enhanced CD/R tools might have upon the provision of the relevant ATS operational services. Two types of SRS are considered:

- Additional SRS (functionality and performance) to mitigate against operational hazard effects (protective mitigation)
- SRS addressing integrity/reliability in order to limit the frequency with which the Solution functional system-generated operational hazards could be allowed to occur.

4.4.1 Operational Hazards Identification and Analysis

The consolidated list of hazards derived from the hazard identification analysis and HAZID workshop (details of the analysis are provided in Appendix D) are shown in Table 7.

For each identified operational hazard, operational effect and the mitigations taken into account for assessing the operational effect (protecting against effect propagation) with a reference to existing

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SRS (functionality and performance) or to new derived SRS (functionality and performance) are described.

In addition, in the table is also presented a reference to existing safety barriers (as per the relevant AIM model) and the assessed severity of the most probable effect from hazard occurrence as per the relevant AIM-based Severity Classification Scheme(s) (SCS) from Guidance G.3 of Safety Reference Material.

Operational Hazard Description	**Operational Effects**	**Mitigation of effects propagation**	**Severity *(most probable effect)***
Hz #01: PC Failure to assess correctly planned/desired profile for problems in AoI	- In case the problem is not (timely) detected and/or not correctly managed, the encounter might evolve into tactical conflict. -In case of nuisance alerts, decrease situational awareness	-Suppression of nuisance alerts. -New alert in case the severity of the encounter would change. - CD&R Tools will detect the conflict. -Indication in radar label if aircraft is transmitting ADS-C data -PC verifies the data received, i.e. the conflict detection quality assessment (figure of merit), allowing them to adapt their strategies and approach according to it, if deemed necessary.	No safety impact
Hz#02 EC Failure to assess correctly planned/desired profile for problems in AoR leading to a tactical conflict MAC SC4b / 1e-2	The encounter might evolve into tactical conflict.	Suppression of nuisance alerts New alert in case the severity of the encounter would change EC solves the conflict in tactical phase. Indication in radar label if aircraft is transmitting ADS-C info EC verifies the data received The radar label indicates the capability and if the data are not of sufficient quality, there must be an indication of whether the data received comes from the AC or from ground systems.	MAC SC4b 1e-2

Hz#03 Late detection of tactical conflict due to corrupted EEP data.	Late detection of tactical conflict	TCT detects the conflict. Existing conformance monitoring tools will detect the discrepancy in the trajectory flown. EC solves the conflict within tactical time horizon.	MAC SC4b 1e-2
Hz#04 CD&R tool failure to detect the conflict	-If the conflict is within pre-tactical horizon, then it may evolve into planned tactical conflict to be solved by TC, increasing TC's workload -If the conflict is within tactical horizon, the tactical conflict may be detected with a delay	-TCT detects the conflict -EC solves the conflict in tactical phase.	MAC SC4b 1e-2
Hz#05 CD&R tool failure to support the ATCO in the resolution of the conflict.	- If the conflict is within pre-tactical horizon, then it evolves into planned tactical conflict to be solved by TC, increasing TC's workload -If the conflict is within tactical horizon, the tactical conflict may be detected with a delay -Inadequate resolution strategy may create knock on effect increasing ATCO's workload.	-TCT detects the conflict. -Existing conformance monitoring tools will detect the discrepancy in the trajectory flown. -EC solves the conflict within tactical time horizon.	MAC SC4b 1e-2

Table 7: Operational Hazards and Analysis

4.4.2 Safety Requirements at ATS Service level (SRS) associated to failure conditions

Table 8 presents the consolidated list of additional SRS (functionality and performance) associated to failure conditions and therefore mitigating against operational hazard effects (protective mitigation), derived during the operational hazard assessment addressed in previous section and referenced in Table 7 above.

SRS ID	Additional Safety Requirements at ATS Service level *(functionality & performance)*	Mitigated Operational Hazard
SRS-101	The CD/R tools shall indicate if the probability of the encounter increases.	Hz #01 Hz #02
SRS-102	ATCO shall have an indication in radar label if aircraft is transmitting ADS-C data (or information is received from ground system).	Hz #01 Hz #02
SRS-103	ATCO shall verify the data received, i.e. the conflict detection quality assessment (figure of merit), allowing them to adapt their strategies and approach according to it, if deemed necessary.	Hz #01 Hz #02

Table 8: Additional SRS (functionality and performance) to mitigate operational hazards

The SRS addressing integrity/reliability in order to limit the frequency with which the operational hazards (listed in section 4.4.1) could be allowed to occur are provided in Table 9.

For the calculation of the frequency of hazards, it has been decided to apply a reduced IM, as it is considered that the last barrier negatively impacted by the corresponding operational hazard is not completely broken, but its efficiency is only reduced to some extent. Another element that the IM also accounts for is the exposure time before the operational hazard detection and subsequent mitigation; the shorter the exposure time, the lower the risk is for which a smaller IM is more appropriate.

SRS ID	Safety Requirements at ATS Service level *(integrity/reliability)*	Hazard	Severity & IM
SRS 104	The frequency of EC failure to assess correctly planned/desired profile for problems in AoR leading to a tactical conflict shall not be greater than 3.33E-04 [per fh].	Hz #02	MAC SC4b /1e-2 IM=0.3
SRS 105	The frequency of late detection of tactical conflict due to corrupted EEP data shall not be greater than 3.33E-04 [per fh].	Hz #03	MAC SC4b /1e-2 IM=0.3
SRS 106	The frequency of failure of enhanced CD&R tools to detect the conflict shall not be greater than 3.33E-04 [per fh].	Hz #04	M MAC SC4b /1e-2 IM=0.3
SRS 107	The frequency of failure of enhanced CD&R tool to support the ATCO in the resolution of the conflict shall not be greater than 3.33E-04 [per fh].	Hz#05	MAC SC4b /1e-2 IM=0.3

Table 9: Safety Requirements at Service level - integrity/reliability

EUROPEAN PARTNERSHIP
Co-funded by the European Union

4.5 Process assurance of the Safety Specification at ATS Service level

The safety assessment was conducted according to SRM [3]. The Safety Requirements at Service level were derived by specifying the change in the operational services under normal, abnormal conditions and to mitigate Operational Hazards caused by failures internal to the ATM/ANS functional system and analyse the associated mitigation measures in order to meet the Safety Criteria.

The current safety assessment started with a preliminary safety impact assessment, including initial hazard identification, involving the operational experts concerned with the use of the concept. This approach allowed to understand the potential safety implication of the solution.

The following safety activities were performed (Table 1) with the participation of PJ.18-W2-53B solution partners including operational experts, concept developers, ATM experts, human factors, and safety experts.

Safety assessment event	Scope	Deliverable receiving the outcome
HP&SAF Scoping & Change Assessment session	Definition of safety strategy and safety planning	Safety Plan
Safety metrics and indicators session	Identification of metrics and indicators to capture safety evidence.	Safety Plan

Table 10 Safety activities performed to derive SRS.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

5 Safe Design of the Solution functional system

The purpose of this section is to document the Safety Requirements at Design level (SRD) for the corresponding ATS operational Solution.

The Safety Requirements at Design level (SRD) are design characteristics/items of the Solution functional system to ensure that the system operates as specified and is able to achieve the SAC (because based on the verification/demonstration of these characteristics/items, it could be concluded that the SAC are met).

The set of Safety Requirements at Service level (SRS) enables the derivation of a correct and complete set of Safety Requirements at Design level (SRD) for ensuring the achievability of the Safety Criteria.

5.1 Overview of activities performed

This section addresses the following activities:

- introduction of the design model of the Solution functional system – section 5.2
- derivation of Safety Requirements (functionality & performance) at Design level (SRD) in normal conditions of operation from the SRS (functionality & performance) of section 4.2 and supported by the analysis of the initial or refined design model above - section 5.3
- derivation of Safety Requirements (functionality & performance) at Design level (SRD) in abnormal conditions of operation from the SRS (functionality and performance) of section 4.3 and supported by the analysis of the operation of the initial or refined design under abnormal conditions of operation - section 5.4
- assessment of the adequacy of the design (initial or refined) in the case of internal failures and mitigation of the Solution operational hazards (identified at section 4.4) through derivation from SRS (integrity/ reliability) of Safety Requirements (functionality & performance) and Safety Requirements (integrity & reliability) at Design level (SRD)- section 5.5
- realism of the refined safe design (i.e. achievability and “testability” of the SRD) - section 5.6.
- safety process assurance at the initial or refined design level – section 5.7.

5.2 Design model of the Solution functional system

5.2.1 Description of the Design Model

In the frame of PJ.18-W2-53B, the EATMA Operational activity models (NOV-5 diagram Operational activity model) used by the Project to specify the operational and interoperability requirements have been also used for the safety assessment at the initial design level.

In addition, the safety assessment at the design level was supported by more detailed EATMA models like NSV-4 diagrams. The details of the models are described in [8].

5.2.2 Task Analysis

EUROPEAN PARTNERSHIP

Co-funded by the European Union

PJ.18-W2-53B did not produce a Task Analysis. However, in order to complement the Safety Assessment, several HP-relevant inputs from the HP Assessment Report [6] and from internal meetings involving the Human Performance team have been taken into account for the derivation and agreement of the initial Safety Requirements.

5.3 Deriving Safety Requirements at Design level for Normal conditions of operation

5.3.1 Safety Requirements at Design level (SRD) – Normal conditions of operation

Table 11 provides the consolidated list of Safety Requirements at Design level (functionality and performance) for Normal conditions of operations derived by mapping the SRS for Normal conditions of operations (documented in section 4.2) onto the related elements of the Design Model. For each SRD is indicated the element of the design model on which the SRD is placed, as well as the associated SRS. The detail of the derivation process is included in E.1.

Safety Requirement ID [Design Model Element]	Safety Requirement (functionality & performance)	Derived from SRS (ID)
NSV-4 for the reception of the EPP data Trajectory Prediction Management	REQ-18-W2-53B-SPRINTEROP-UU01.0001 ADS-C EPP data validity information The Separation Assurance process shall adapt itself to the quality and reliability of each flight's predicted trajectory.	SRS-001 SRS-002 SRS-003 SRS-004
NSV-4 for the Trajectory Computation and Conflict Detection process Trajectory Prediction Management	REQ-18-W2-53B-SPRINTEROP-SAF1.0004 Detection of True Conflicts The enhanced TP shall contribute to the CD/R tool detecting true conflicts with a greater accuracy than the current TP and CD/R tools.	
	REQ-18-W2-53B-SPRINTEROP-SAF1.0002 Nuisance Alerts The rate of nuisance alerts shall be reduced as compared to the current operating method.	
	REQ-10.02a-SPRINTEROP-UU01.3100 System Tuning Envelope The parameters governing the notification of potential conflicts shall be tuned such that missed and nuisance notifications at given prediction times meets locally-defined values, given the following assumptions: · the input data are reliable; · aircraft trajectory data is downlinked via ADS-C; · no unexpected aircraft manoeuvre will occur in the time horizon.	

Table 11. Safety Requirements at design level (functionality and performance) satisfying SRS for Normal conditions of operation

5.3.2 Static analysis of the functional system behaviour – Normal conditions of operation

EUROPEAN PARTNERSHIP
Co-funded by the European Union

No additional requirements were identified.

5.3.3 Dynamic Analysis of the functional system behaviour – Normal conditions of operation

No additional requirements were identified.

5.3.4 Effects on Safety Nets – Normal conditions of operation

No additional requirements related to negative effect on ground-based and airborne safety nets were identified.

5.4 Deriving Safety Requirements at Design level for Abnormal conditions of operation

5.4.1 Safety Requirements at Design level (SRD) for Abnormal conditions of operation

5.4.2 Analysis of the functional system behaviour – Abnormal conditions of operation

The following abnormal conditions were investigated during validation activities:

- Emergency (EXE-008)
- Military operations and activation of SUAs (EXE-008 and EXE-012)
- Adverse weather Area (CB Area) – (EXE-012)

The analysis of the scenarios covering abnormal conditions included both quantitative and qualitative data covering human performance (workload level, situational awareness, acceptance), as well as the conflicts (pre-tactical planned conflicts, planned tactical conflicts, imminent separation infringement).

Based on the evidence coming from the exercises it was confirmed that the existing requirements cover sufficiently the abnormal conditions.

5.5 Safety Requirements at Design level addressing Internal Functional System Failures

Safety requirements at design level SRD are derived from the SRS (functionality and performance) and SRS (integrity and reliability) which have been identified when mitigating system generated risks (section 4.4).

5.5.1 Design analysis addressing internal functional system failures

In order to ensure the identification of a complete list of Solution functional system failures that could cause each operational hazard, both top-down and bottom-up analyses were performed.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

The mitigation means preventing causes to occur or preventing their effect to propagate towards each operational hazard were identified. An overview of the main outcomes of the analysis is included in Appendix G.

5.5.2 Safety Requirements at Design level associated to internal functional system failures

Table 12 provides the consolidated list of Safety Requirements at Design level (functionality and performance) associated to internal system failures. It includes:

- the SRD (functionality and performance) derived from the SRS (integrity/reliability) from section 4.4.2 to provide adequate mitigations to reduce the likelihood that specific failures would propagate up to the operational hazard, with due consideration for mitigating the common cause failures,
- the SRD (functionality and performance) derived to provide mitigation against operational hazard effects (protective mitigation, from the SRS (functionality & performance) derived during the operational hazard assessment at §4.4.1), with due consideration for mitigating the common cause of failures.

The detail of the derivation process is included in Appendix G.

Safety Requirement ID	Safety Requirement at Design level (SRD) (functionality & performance)	Derived from SRS (ID) or Common cause failure
REQ-18-W2-53B-SPRINTEROP-SAF1.0007	Contingency procedures should be in place for transition to conventional TP and CD/R tools in case of improved TP failure or lack of data (ADS-C/EPP).	Lack of EPP data
REQ-18-W2-53B-SPRINTEROP-SAF1.0008	Contingency procedures should be in place for transition to the conventional TP and CD/R tools in case corrupted data is received	Corruption of EPP data
REQ-18-W2-53B-SPRINTEROP-SAF1.0009	CD/R tool reversion TP and CD/R tools shall dynamically revert to "conventional" functioning mode (management of flight data without ADS-C/EPP) and use FDP based TP functions as an input.	Corruption of EPP data
REQ-18-W2-53B-SPRINTEROP-SAF1.0010	ATCO notification for reverting ATCOs shall be informed with the appropriate notification (system reverting to reference scenario TP and CD/R tools performance)	Corruption of EPP data
REQ-18-W2-53B-SPRINTEROP-UU01.0002	Awareness of ADS-C Availability and Validity for a Flight The ATCO shall be able to identify flights for which ADS-C data has been received and is valid.	Lack of ADS-C/EPP data
REQ-18-W2-S53b-TS-0100.0010	Filtering outliers	Corruption of ADS-C/ EPP data

EUROPEAN PARTNERSHIP
Co-funded by the European Union

	The En-Route / Approach ATC System shall check the downlinked data (including gross Mass, Speed schedule and EPP profile) for credibility prior to use it in ATC applications.	
REQ-18-W2-53B-SPRINTEROP-SAF1.0005	Aircraft Equipage Where the controller's separation strategy is adapted based on aircraft ADS-C equipage and availability of EPP data, the availability of ADS-C/EPP data related to a specific flight (aircraft equipage and quality of data received) shall be displayed to the controller in an unambiguous manner.	SRS-102
REQ-18-W2-53B-SPRINTEROP-SAF1.0006	Non-equipped Aircraft When legacy aircraft (non- ADS-C/EPP -equipped) are participating in a conflict detection and resolution event, the ATM system shall use existing CD/R tool capabilities and parameters.	SRS-102
REQ-18-W2-53B-SPRINTEROP-SAF1.0011	Conflict detection confidence level The information about the conflict detection quality assessment (figure of merit) should be available to ATCOs, allowing them to adapt their strategies and approach according to it, if deemed necessary.	SRS-103

Table 12. SRD (functionality & performance) to mitigate the operational hazards

Table 13 provides the consolidated list of Safety Requirements at Design level (integrity/reliability) associated to internal system failures derived from the Service Requirements at Service level (integrity/reliability) documented in section 4.4.2.

Safety Requirement ID	Safety Requirement at Design level (SRD) (functionality & performance)	Derived from SRS (ID) or Common cause failure
REQ-18-W2-53B-SPRINTEROP-SAF1.0012	The frequency of failure of CD/R tools due to corrupted ADS-C/EPP data shall not be greater than 3.33E-04	SRS-104 SRS-105 SRS-106 SRS-107

Table 13 SRD (integrity & reliability) to limit the frequency of the operational hazards.

5.6 Realism of the safe design

The current safety assessment considers the technical systems to the extent of their support /enabling the V3 maturity level of the concept. The safety requirements associated to human roles and procedures are considered as reasonable and achievable. The evidence coming from the exercises indicate that the concept is acceptable from the HP point of view but requires further refinement. More information on the human performance related results is provided in the HPAR [6].

5.7 Process assurance for a Safe Design

EUROPEAN PARTNERSHIP
Co-funded by the European Union

The safety assurance activities applied are in line with the activities envisaged for V3 concept development phase, as defined in SRM [3].

The Safety Requirements (functionality & performance) at Design level (SRD) in normal and abnormal conditions of operation from the SRS (functionality & performance) were identified through the analysis of the operation of the design under normal and abnormal conditions of operations. Further to this, the Safety Requirements (functionality & performance) and Safety Requirements (integrity & reliability) at Design level (SRD) were identified from SRS (integrity/ reliability) through the assessment of the adequacy of the design in the case of internal failures and mitigation of the Solution operational hazards. The complementary online HAZID workshop with the safety experts and the operational experts involved in the solution was performed.

Safety assessment event	Scope	Outcomes
HAZID workshop Hazard refinement	Safety Requirements at Service Level	SRS
Online workshop	Safety requirements at Design level and their consolidation at solution level	SRD Input to OSED Part I

Table 14 Safety activities Safety activities performed to derive SRD.

The evidence to support the safety assessment was obtained through the technical evaluation, gaming exercises and human-in-the-loop RTS conducted within representative operational environments with participation of licensed air traffic controllers. The obtained results represent the consolidation of the quantitative and qualitative data recorded during the simulation and the subjective opinions of the participating controllers contributing to the operational significance of the evidence.

6 Safety Criteria achievability

The safety assessment conducted across the exercises had been shown to be comprehensive and relies on a range of data sources (Real-Time simulations, technical demonstration, gaming exercises and workshops). Overall, it has been concluded that the level of safety is maintained with the enhanced TP improvements feeding CD/R tool. Based on quantitative and qualitative results (data logs) the level of safety is maintained with the use of the new functionalities while traffic has been increased. The following safety related evidence was captured:

EXE008: The quantitative outcomes showed that there was no increase in the imminent separation infringement. Therefore, the level of safety was maintained. Moreover, the subjective feedback demonstrated predominant neutral and unlikely results for the human performance to be deteriorated in TMA environment. In ENR environment – the results predominantly pointed to likely as for the human performance to deteriorate in longer term due to overreliance on automation.

EXE009: Reduction of false alerts and identification of undetected conflicts could potentially increase situational awareness while reducing the workload for unnecessary checking for false alerts. There was no indication that human performance was deteriorated, especially no negative effect on safety.

EXE010 did not address safety validation objective.

EXE011: ATCOs considered that EPP neither affected their decision making regarding planned conflicts nor the number of real conflicts compared to the number of tactical ones. These results could be explained by the fact that ATCOs did not always consider EPP to manage their traffic because of their irrelevance due to some simulations or HMI limits rather than the solution itself. Moreover, they reported some issues about the behaviour of the alerts and thus they considered that alerts did not help them in their work. However, no increase in the number of infringements was reported in solution scenario. Finally, despite the simulation issues and the inaccuracy of EPP, some benefits on the situational awareness have been reported for both ACC and Approach provided some improvements are done on the system, and on average, the ATCOs have even reported a slightly more efficient management of the traffic. To conclude, some issues have been reported during exercises, and even if no major negative points have been reported leading to a decrease either of human performance or safety aspects, it seems necessary to confirm these results.

EXE012: The implementation of support tools did not deteriorate human performance impacting safety.

The evidence coming from validation related to abnormal conditions (EXE-008 and EXE-012) demonstrated that although in some cases the number of conflicts increased, the safety was maintained. No specific effect on human performance deteriorating safety was identified.

The validation did not explicitly address degraded modes of operation however, some technical issues happened (loss of ADS-C EPP) in EXE-012. The CD&R tools were designed to dynamically revert to conventional functioning mode (flight data treating without ADS-C EPP) and ATCOs were informed with the appropriate warning (reverting to reference scenario CD&R tools performance). Although the ATCO reported that the degradation did not affect their working methods, further investigation of degradation was recommended.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

The safety-related outcomes of the validation exercises (traced back to the safety validation objectives) bring an essential contribution to the demonstration of the Safety Criteria achievability by the Solution design. The safety-relevant results of the validation exercises are summarized in the Table 25 in the Appendix H whilst indicating for each safety validation objective / success criteria which relevant SRS have been covered.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

7 Acronyms and Terminology

Acronym	Definition
A/C	Aircraft
ADS-B	Automatic Dependent Surveillance – Broadcast
ADS-C	Automatic Dependent Surveillance – Contract
AIM	Accident Incident Model
ANSP	Air Navigation Service Provider
AoI	Area of Interest
AoR	Area of Responsibility
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATM	Air Traffic Management
ATS	Air Traffic Service
ATSU	Air Traffic Service Unit
AWA	Adverse Weather Area
CB	Cumulonimbus
CD/R	Conflict Detection and Resolution
CPDLC	Controller/Pilot Data Link Communications
CWP	Controller Working Position
D/L	Datalink
DST	Decision Support Tool
EATMA	European ATM Architecture
E-ATMS	European Air Traffic Management System
EC	Executive Controller
eFPL	Extended Flight Plan
ER	En-Route
FH	Flight Hour
EPP	Extended Projected Profile
FMS	Flight Management System
Hi	Hazard Inherent to aviation
HMI	Human Machine Interface

EUROPEAN PARTNERSHIP

Co-funded by the European Union

HPAR	Human Performance Assessment Report
Hz	Hazard
IFR	Instrument Flight Rules
INTEROP	Interoperability Requirements
KPA	Key Performance Area
KPI	Key Performance Indicator
LoA	Letter of Agreement
MAC	Mid Air Collision
MONA	Monitoring Aids
MTCD	Medium-Term Conflict Detection
NM	Network Management
OI	Operational Improvement
OSED	Operational Service and Environment Definition
PC	Planning Controller
OH	Operational hazard
RBT	Reference Business Trajectory
R&D	Research and Development
R/T	Radio Telephony
SAC	Safety Criteria
SAR	Safety Assessment Report
SCS	Severity Classification Scheme
SESAR	Single European Sky ATM Research Programme
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SPR	Safety and Performance Requirements
SRD	Safety Requirements at Design level
SRS	Safety Requirements at Service level
SUA	Special use Airspace
STCA	Short Term Conflict Alert
TC	Tactical Controller (used interchangeably with “EC”)
TCT	Tactical Controller Tool
TMA	Terminal Manoeuvring Area
TP	Trajectory Prediction
TS	Technical Specification

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Table 15: Acronyms

EUROPEAN PARTNERSHIP

Co-funded by the European Union

8 References

Safety

[1] (EU) No 2017/373 laying down common requirements for service providers and the oversight in air traffic management/air navigation services and other air traffic management network functions, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011 and (EU) No 1035/2011 and amending Regulation (EU) No 677/2011 (and associated AMC and GM)

[2] SAM EUROCONTROL Safety Assessment Methodology, Edition 2.0

[3] SESAR Safety Reference Material, Ed. 00.04.01, 14 December 2018

[4] Guidance to Apply SESAR Safety Reference Material D.0.050 14 December 2018 Ed.00.03.01

Project documentations

[5] SESAR Solution PJ.18-W2-53B Final SPR-INTEROP/OSED for V3 Part I

[6] SESAR Solution PJ.18-W2-53B-V3 Final Human Performance Assessment Report

[7] SESAR Solution PJ.18-W2-53B-V3 Final VALR

[8] SESAR Solution PJ.18-W2-53B-V3 Final TS/IRS

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix A Preliminary safety impact assessment

A.1 Relevant Hazards Inherent to Aviation

The following Table 16 indicates hazards inherent to aviation the ATM-related accident type and consequently the relevant AIM model.

Hazards inherent to aviation	ATM-related accident type & AIM model
Hi#1: Situation in which the intended trajectories of two or more aircraft are in conflict	Mid-Air Collision (MAC) TMA AIM model

Table 16. Hazards inherent to aviation relevant for the Solution

A.2 Functional system-generated hazards (preliminary)

Table 17 provides the preliminary list of the hazards generated by the functional system in the scope of the Solution. For each functional system-generated hazard the way they are impacted by the change is analysed investigating

- New or modified causes
- New or modified preventive mitigations
- New or modified protective mitigations

HAZARD-ID	Description of hazard	Potential cause(s)	Potential effect(s)
Hz#01 PC	Failure of PC to assess correctly planned/desired profile for problems in AoI/AoR	ATCO receives corrupted data (credible inaccurate data)	▪ The pre-tactical conflict may evolve into planned tactical conflict to be solved by TC, increasing TC's workload
		The CD tool identifies potential conflicts which are nuisance ones	▪ increased PC's workload in identifying nuisance alerts from true alerts
Hz#02 TC	Failure of TC to assess correctly planned/desired profile for problems in AoI/AoR	ATCO receives corrupted data (credible inaccurate data)	▪ The planned tactical conflict may evolve into imminent infringement
		The CD tool identifies potential conflicts which are nuisance ones	▪ Increased TC's workload in identifying nuisance alerts from true alerts
Hz#03	TC fails to establish necessary separation	TC receives corrupted data (credible inaccurate data)	▪ TC fails to establish proper resolution strategy to avoid imminent infringement ▪ TC fails to establish proper resolution strategy creating

EUROPEAN PARTNERSHIP
Co-funded by the European Union

HAZARD-ID	Description of hazard	Potential cause(s)	Potential effect(s)
			knock on effect and increasing workload
		PC fails to execute resolution strategy to establish separation at the sector entry	▪ TC fails to establish proper resolution strategy to avoid imminent infringement
Hz#04	CD&R tool failure to detect the conflict	CD&R tool receives corrupted data (credible inaccurate data) Non availability of required data (ADS-C/EPP) due to legacy aircraft	▪ If the conflict is within pre-tactical horizon, then it may evolve into planned tactical conflict to be solved by TC, increasing TC's workload ▪ If the conflict is within tactical horizon, the planned tactical conflict may evolve into imminent infringement
Hz#05	CD&R tool failure to support the ATCO in the resolution of the conflict	Corrupted data (credible inaccurate data) causes CD&R tool to propose inadequate resolution strategy Corrupted data (credible inaccurate data) causes CD&R tool to fail to provide a resolution strategy Non availability of required data (ADS-C/EPP) due to legacy aircraft	▪ If the conflict is within pre-tactical horizon, then it evolves into planned tactical conflict to be solved by TC, increasing TC's workload ▪ If the conflict is within tactical horizon, the planned tactical conflict evolves into imminent infringement ▪ Inadequate resolution strategy may create knock on effect increasing ATCO's workload

Table 17. Functional system-generated hazards applicable to the Solution (preliminary list)

EUROPEAN PARTNERSHIP
Co-funded by the European Union

Appendix B Derivation of SRS (Functionality & Performance) for Normal conditions of operation

This appendix presents the derivation of the SRS (functionality and performance) in order to mitigate the hazards inherent to aviation under normal conditions of operation, i.e. those conditions that are expected to occur on a day-to-day basis.

Derivation of the SRS was based on the description of the operating method with the Solution, in order to specify through SRS the safety-relevant changes in the delivery of each impacted operational service based on the step by step review of:

- Solution OSED Use Cases
- the EATMA representation as per the Operational layer (i.e. NOV-5 diagrams where each Functional Process/Use Case is described through a process model made up of activities interacting via information flows).

B.1 EATMA Process models or alternative description

The Use Cases and EATMA models used for further safety assessment of the solution are provided in the main body of the OSED document, section 3.3.2.

B.2 Derivation of SRS for Normal Operations

The Table 18 provides the derivation of SRS in Normal Operations driven by EATMA Process Models.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

ATS Operational Service	EATMA Use Case- Activity or Flow	Derived SRS	Related SAC# (AIM Barrier or Precursor)
Use Case 1: Provide Planning Separation Assurance with Reduced Uncertainty (53B)			
Air traffic separation provision	Determine planning problems at offered entry conditions	SRS-001 Conflict detection tool shall indicate pairs of aircraft which have planning encounters at the entry or exit sector boundary based on the improved TP data (i.e., airborne downlinked MET and Trajectory (EPP) data).	SAC-18-W2-53B-ER-TMA -001 B5 Plan Induced Conflict Management/ MF5.1 Planning Conflicts SAC-18-W2-53B-ER-TMA -003 MF10 Pre-tactical Conflicts/ MB10.1.1.2 Inadequate Trajectory Info
Coordination & Transfer management	Agree entry coordination	No Change	
Air traffic separation provision	Determine safe potential exit conditions	SRS-002 The planning controller shall assess the exit conditions based on ATC Planned Trajectory using airborne downlinked MET and Trajectory (EPP) data.	SAC-18-W2-53B-ER-TMA -001 B5 Plan Induced Conflict Management/ MF5.1 Planning Conflicts SAC-18-W2-53B-ER-TMA -003 MF10 Pre-tactical Conflicts/ MB10.1.1.2 Inadequate Trajectory Info
Air traffic separation provision	Assess trajectory profile through the AoR for tactical controller suitability	SRS-003 The planning controller shall assess trajectory profile through the AoR for tactical controller suitability based on improved planned trajectory prediction, using airborne downlinked MET and Trajectory (EPP) data.	SAC-18-W2-53B-ER-TMA -001 B5 Plan Induced Conflict Management/ MF5.1 Planning Conflicts SAC-18-W2-53B-ER-TMA -003 MF10 Pre-tactical Conflicts/ MB10.1.1.2 Inadequate Trajectory Info
Coordination & Transfer management	Make coordination offer to downstream sector	No Change	
Use Case 2: Provide Tactical Separation Assurance with Reduced Uncertainty			

EUROPEAN PARTNERSHIP

Co-funded by the European Union

ATS Operational Service	EATMA Use Case- Activity or Flow	Derived SRS	Related SAC# (AIM Barrier or Precursor)
Air traffic separation provision	Assess planned/desired profile for problems within AoR/AoI	SRS-004 EC shall determine whether there are any problems between the aircraft's trajectory profiles based on improved planned trajectory prediction, using airborne downlinked MET and Trajectory (EPP) data.	SAC-18-W2-53B-ER-TMA -001 B5 Plan Induced Conflict Management/ MF5.1 Planning Conflicts SAC-18-W2-53B-ER-TMA -002 B7 ATC Induced Conflict Management/ MF7.1 ATC induced Tactical conflict.
Air traffic separation provision	Establish Necessary Separation	No change	
Air traffic separation provision	Issue clearances	No change	
Coordination & Transfer management	Agree coordination actions	No change	
Air traffic separation provision	Modify trajectory	No change	

Table 18: Derivation of SRS for Normal Operations driven by EATMA Process models

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix C Risk analysis of Abnormal conditions and derivation of SRS (functionality&performance)

For each abnormal condition of operation identified and listed in section 4.3.1, the results of the risk analysis assessing the immediate operational effect and the possible mitigations of the safety consequences of the abnormal condition are provided in the Table 19 below.

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SRS]
ABN-01	Bad weather (CBs, turbulences, icing)	Effects in planning phase: In case of bad weather, some DCB measure might be implemented in planning phase, for instance reduction of the capacity (existing mitigation means). Aircraft path avoids areas of forecast adverse weather (e.g. lower RFL in areas of forecast icing) based on e.g. SIGMET data (existing mitigation means) Effects in execution phase Case of CBs: Aircraft will possibly avoid the area with lateral deviation. Flight crew asks the ATCO before deviation. It will be a problem for MTCD encounters, relying on planning TPs, which are not applicable anymore. Deviating aircraft will not fly according to their planned TPs. The new operating method will improve the accuracy of the TP even when deviating due to the downlinked EPP and improved MET data availability (EC is able to anticipate the effect of the adverse weather and plan in advance e.g. the direction of the diversion etc.)	SRS-004 EC shall determine whether there are any problems between the aircraft's trajectory profiles based on improved planned trajectory prediction, using airborne downlinked MET and Trajectory (EPP) data.
ABN-02	Sudden closure of airspace (SUA)	The airspace is closed at short notice, the capacity might be decreased. Deviating aircraft will not fly according to their planned TPs. The new operating method will improve the accuracy of the TP even when deviating due to the downlinked EPP and improved MET data availability (EC is able to plan in advance e.g. the direction of the diversion etc.)	SRS-004 EC shall determine whether there are any problems between the aircraft's trajectory profiles based on improved planned trajectory prediction, using airborne downlinked MET and Trajectory (EPP) data.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

ABN-03	Severe ATC technical system failure - Total loss of surveillance system	In case of failure of the surveillance system ADS-C is based on data link and the basic data set provided by ADS-C also includes position information. If the ATC system itself is functioning and only the processing of surveillance data is failing, then it would be possible to see ADS-C equipped aircraft based on the information they provide in their reports. However, the minimum update interval of ADS-C messages is 64 seconds and ADS-C itself is not approved as a surveillance method so it would not provide a mitigation measure	Severe ATC technical system failure - Total loss of surveillance system No change with respect to current operations
ABN-04	Severe ATC technical system failure - Total loss of air/ground communication system	In case of loss of radio, CPDLC can be used as a backup If CPDLC is not available, then in the absence of ground instruction, aircraft will continue on their flight plan.	No change with respect to current operations: ATCO will contact adjacent centre to ask them to relay the messages to the aircraft (existing mitigation means) Capacity of the sector/ATSU is reduced (existing mitigation means)
ABN-05	Severe ATC technical system failure - Total loss of FDPS	In case of failure of FDPS, all trajectory derived information is impacted. Depending on local implementation, impacts could be: No more flight data. Impossible to display the planned trajectory of the aircraft on the HMI Detection tool based on flight plan information (MTCD and TC aid) are unavailable or degraded Degradation / loss of automatic coordination functions Surveillance information should be displayed as long as possible Radar tracks are not correlated anymore	No change with respect to current operations: Mitigation means shall be defined depending upon local architecture for the management of the short term degraded situation. When the short-term situation has been managed, control services are provided in degraded mode: capacity thresholds are reduced. (existing mitigation means)
ABN-06	Severe ATFCM technical system failure -	In case of loss of local DCB tool, FMP is not able to perform the local demand and	No change with respect to current operations:

EUROPEAN PARTNERSHIP

Co-funded by the European Union

	Total loss of local DCB tool	capacity balancing activities in nominal conditions.	FMP can ask NM to put regulations (existing mitigation means)
ABN-07	Aircraft in emergency	In case of emergency situation (such as loss of pressurization or loss of engine), the flight crew will apply the appropriate emergency procedure.	No change with respect to current operations
ABN-08	Severe aircraft technical system failure - Radio communication failure	In the absence of ground instruction, flight crew will follow the flight plan until the IAF. The ATCO will be in charge of providing separation via appropriate clearances relayed to surrounding aircraft. If the aircraft is being radar vectored: the standard procedure that might depend on the ICAO regional regulation has to be applied. In case of ADS-C/EPP data is still provided, it gives an additional layer of assurance to the controller that the aircraft is following the procedure and the controller is able to verify the A/C intentions based on the EPP profile.	No change with respect to current operations
ABN-09	Severe aircraft technical system failure - Transponder failure	Impact on ground: Loss of the flight track on the CWP (En Route CWP are only based on secondary radar). If possible EC allocates a specific FL to this aircraft, with a fine update of longitudinal evolution via regular radio reports, and provides non-radar separation between this aircraft and the other ones. Position data available via ADS-C/EPP periodic reports would provide limited position data depending on the frequency of the reports but could not be used for separation purposes as they would only be available at the minimum every 64 seconds.	No change with respect to current operations Ask for regular frequency reports on this aircraft and ensure non-radar separation minima (existing mitigation means)

Table 19: Risk analysis for Abnormal conditions of operation

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix D Risk analysis addressing internal functional system failures and derivation of SRS

This appendix presents the risk analysis done at the level of the ATS service specification, including operational hazards. For the latest, the SRS derivation is to be performed according to the mathematical calculation of the previous Safety Objectives integrity & reliability as per **Guidance G.2** of **Safety Reference Material** and using the relevant AIM-based Risk Classification Scheme(s) from **Guidance G.4** of **Safety Reference Material**.

D.1 HAZID workshop

The outcomes from the preliminary safety impact assessment included in Appendix A have been used as input for the HAZID workshop.

The table resulting from the HAZID workshop containing the detailed results and used for further safety assessment assurance activities is presented in Table 7.

It provides causes of the operational failure mode and associated preventive mitigations, the assessed immediate operational effect, the mitigations taken into account for defining the operational effect (protecting against effect propagation).

Two types of SRS have been derived from this process (and the consolidated list is provided in section 4.4.2):

- Additional SRS (functionality and performance) to mitigate against operational hazard effects (protective mitigation)
- SRS addressing integrity/reliability in order to limit the frequency with which the operational hazards could be allowed to occur.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Use Case / Operational failure mode	Example of causes & preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
Use Case 1 Provide Planning Separation Assurance with Reduced Uncertainty	-The CD tool identifies potential conflicts which are nuisance ones -In mix mode environment: ATCO over-estimates the precision of the predicted trajectory of a flight due to wrongly assuming that it is transmitting ADS-C information -In cases where the CD separation parameters have been reduced to take into account the improved TP accuracy, conflicts might be missed (false negative) more easily due to corrupted or out-lying data (wind, aircraft performance, etc). -Late detection of the conflict.	- In case the problem is not (timely) detected and/or not correctly managed, the encounter might evolve into tactical conflict. -In case of nuisance alerts, decrease situational awareness	-Suppression of nuisance alerts. -New alert in case the severity of the encounter would change. - CD&R Tools will detect the conflict. -Indication in radar label if aircraft is transmitting ADS-C data -PC verifies the data received, i.e. the conflict detection quality assessment (figure of merit), allowing them to adapt their strategies and approach according to it, if deemed necessary.	Hz #01: PC Failure to assess correctly planned/desired profile for problems in AoI No safety impact
Use Case 2: Provide Tactical Separation Assurance with Reduced Uncertainty	The CD tool identifies potential conflicts and triggers nuisance alerts In mix mode environment: ATCO over-estimates the precision of the predicted trajectory of a flight due to wrongly assuming that it is transmitting ADS-C information In cases where the CD separation parameters have been reduced to take into account the improved TP accuracy, conflicts might be missed	The encounter might evolve into tactical conflict.	Suppression of nuisance alerts New alert in case the severity of the encounter would change EC solves the conflict in tactical phase. Indication in radar label if aircraft is transmitting ADS-C info EC verifies the data received	Hz#02 EC Failure to assess correctly planned/desired profile for problems in AoR leading to a tactical conflict MAC SC4b / 1e-2

EUROPEAN PARTNERSHIP

Co-funded by the European Union

	(false negative) more easily due to corrupted or out-lying data (wind, aircraft performance, etc).		The radar label indicates the capability and if the data are not of sufficient quality, there must be an indication of whether the data received comes from the AC or from ground systems.	
Use Case 2: Provide Tactical Separation Assurance with Reduced Uncertainty	ATCO receives corrupted data and therefore establishes wrongly the separation.	Late detection of tactical conflict	TCT detects the conflict. Existing conformance monitoring tools will detect the discrepancy in the trajectory flown. EC solves the conflict within tactical time horizon.	Hz#03 Late detection of tactical conflict due to corrupted EEP data. MAC SC4b / 1e-2
Use Case 2: Provide Tactical Separation Assurance with Reduced Uncertainty	CD&R tool receives corrupted data (credible inaccurate data) Non availability of required data (ADS-C/EPP) due to legacy aircraft	-If the conflict is within pre-tactical horizon, then it may evolve into planned tactical conflict to be solved by TC, increasing TC's workload -If the conflict is within tactical horizon, the tactical conflict may be detected with a delay	-TCT detects the conflict -EC solves the conflict in tactical phase.	Hz#04 CD&R tool failure to detect the conflict MAC SC4b / 1e-2
Use Case 2: Provide Tactical Separation Assurance with Reduced Uncertainty	Corrupted data (credible inaccurate data) causes CD&R tool to propose inadequate resolution strategy Corrupted data (credible inaccurate data) causes CD&R tool to fail to provide a resolution strategy	- If the conflict is within pre-tactical horizon, then it evolves into planned tactical conflict to be solved by TC, increasing TC's workload -If the conflict is within tactical horizon, the tactical	-TCT detects the conflict. -Existing conformance monitoring tools will detect the discrepancy in the trajectory flown. -EC solves the conflict within tactical time horizon.	Hz#05 CD&R tool failure to support the ATCO in the resolution of the conflict. MAC SC4b /1e-2

	Non availability of required data (ADS-C/EPP) due to legacy aircraft	conflict may be detected with a delay -Inadequate resolution strategy may create knock on effect increasing ATCO's workload.		

Table 20. Full HAZID working table.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

D.2 HAZID participation list

Alty, Peter PJ18 Project manager (EUROCONTROL)

Salinas Sanz, Hugo PJ18-W2-53 Project Manager (INDRA)

Morton, Stephen PJ18-W2-53 OSED and EX004 Lead

Alonso, Roland EXE0013 Validation Lead (Egis)

Ferreira, Ana HP Lead (Deep Blue)

Castell Orozco, Pablo (AIRBUS)

GUNDLAKUNTA, Srikanth Reddy (AIRBUS)

Pinska Chauvin, Ella Safety Lead (INTEGRA)

Koczowski, Szymon EXE-013 (PANSA, INDRA)

Kasperska, Urszula EXE-013 (PANSA, INDRA)

Jemiolo, Krzysztof EXE-013 (PANSA, INDRA)

Puetz, Thomas (DFS)

Huart Olivier (Skyguide)

Velay, Didier EXE-003 (DSNA, ONERA, LDO, AIRBUS)

Raynaud, Béatrice EXE-003 (DSNA, ONERA, LDO, AIRBUS) and VALP Lead

Verdonk Gallego, Christian Eduardo CBA Lead (CRIDA/ENAIRE)

Fabio Bracero, Adrian EXE-007 (ENAIRE, AT-ONE, INDRA)

Lema Esposto, Maria Florencia (CRIDA/ENAIRE)

Paino, Marco EXE-001 (LDO, ENAV)

Rodríguez González, Pelayo TS/IRS Lead (INDRA)

Giovannetti, Maria Gabriella EXE-001 (LDO, ENAV)

Zakariyya, Mohammed VALR Lead (NATS)

Vitekov, Valentin (BULASTA)

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix E Designing the Solution functional system for normal conditions

E.1 Deriving SRD from the SRS

In Table 21below, the Safety Requirements at ATS Service level (SRS) for normal conditions of operation derived in section 4.2 are mapped onto the related elements of the Design Model (i.e. NSV-4 models). The Safety Requirements at Design level (SRD) (functionality and performance) derived from related SRS.

SRS for Normal Operation (ID & content)	Safety Requirement at Design level[3] (SRD) or Assumption	Maps onto
SRS-001 Conflict detection tool shall indicate pairs of aircraft which have planning encounters at the entry or exit sector boundary based on the improved TP data (i.e., airborne downlinked MET and Trajectory (EPP) data).	**REQ-18-W2-53B-SPRINTEROP-UU01.0001** ADS-C EPP data validity information The Separation Assurance process shall adapt itself to the quality and reliability of each flight's predicted trajectory. **REQ-18-W2-53B-SPRINTEROP-SAF1.0004** Detection of True Conflicts The enhanced TP shall contribute to the CD/R tool detecting true conflicts with a greater accuracy than the current TP and CD/R tools. **REQ-18-W2-53B-SPRINTEROP-SAF1.0002** Nuisance Alerts The rate of nuisance alerts shall be reduced as compared to the current operating method. **REQ-10.02a-SPRINTEROP-UU01.3100** System Tuning Envelope The parameters governing the notification of potential conflicts shall be tuned such that missed and nuisance notifications at given	NSV-4 for the reception of the EPP data Trajectory Prediction Management Support Functions – Build grid with ADS-C MET data NSV-4 for the Trajectory Computation and Conflict Detection process Trajectory Prediction Management
SRS-002 The planning controller shall assess the exit conditions based on ATC Planned Trajectory using airborne downlinked MET and Trajectory (EPP) data.		
SRS-003 The planning controller shall assess trajectory profile through the AoR for tactical controller suitability based on improved planned trajectory prediction, using airborne downlinked MET and Trajectory (EPP) data.		
SRS-004 EC shall determine whether there are any problems		

[3] iSRD for the initial design or rSRD for the refined design

EUROPEAN PARTNERSHIP
Co-funded by the European Union

between the aircraft's trajectory profiles based on improved planned trajectory prediction, using airborne downlinked MET and Trajectory (EPP) data.	prediction times meets locally-defined values, given the following assumptions: · the input data are reliable; · aircraft trajectory data is downlinked via ADS-C; · no unexpected aircraft manoeuvre will occur in the time horizon.	

Table 21: SRD derived by mapping SRS for normal conditions of operation to Design Model Elements

E.2 Static analysis of the solution functional system behaviour

N/A

E.3 Dynamic analysis of the Solution functional system behaviour

N/A

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix F Designing the Solution Functional system for Abnormal conditions of operation

F.1 Deriving SRD from SRS

No new SRD were derived for abnormal conditions.

F.2 Analysis of the Solution functional system behaviour for abnormal conditions of operation

The following abnormal conditions were investigated during validation activities:

- Emergency (EXE-008)
- Military operations and activation of SUAs (EXE-008 and EXE 0012)
- Adverse weather Area (CB Area) EXE-012)

The analysis of the scenarios covering abnormal conditions included both quantitative and qualitative data covering human performance (workload level, situational awareness, acceptance), as well as the conflicts (pre-tactical planned conflicts, planned tactical conflicts, imminent separation infringement).

Based on the evidence coming from the exercises it was confirmed that the existing requirements cover sufficiently the abnormal conditions.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix G Designing the Solution functional system addressing internal functional system failures

This appendix presents the detailed risk evaluation and mitigation of the operational hazards identified in §4.4, performed at the level of the design of the Solution functional system.

G.1 Deriving SRD from the SRS (integrity/reliability)

The purpose is to derive from the SRS (integrity/reliability) that have been derived in §4.4.2:

- SRD (functionality and performance) in order to provide adequate mitigations to reduce the likelihood that specific failures would propagate up to the operational hazard
- SRD (integrity/ reliability) to limit the frequency with which failure of modified/new equipment elements in the Solution Functional system could be allowed to occur.

G.1.1 Top-down causal analysis

Further analysis of the impact of the hazards revealed that the safety impact will be derived from the hazards related to the Tactical Separation Assurance. Therefore, the top-down identification of Solution functional system failures was performed at the generic level. To achieve that, a table of causes and a Fault Tree showing for tactical operational hazard, its causes and the associated mitigations was used. The latter represent preventive mitigations for the operational hazard, but they might either prevent a basic cause to occur or they protect against the propagation of the basic cause effect up to the operational hazard occurrence.

The Safety Requirement identifiers in the table below are the same as or consistent (for newly identified requirements) with the ones defined in Section 4 of SPR-INTEROP/OSED Part I. The consolidated list of SRD is included in section 5.5.2.

Tolerable frequency allocated to the operational hazards has been calculated as follows:

- Tolerable frequency for MAC-SC4b = 1E-02 [per ft]
- IM=0.3*
- Pre-defined number of ops hazards N=100
- Tolerable frequency allocated to Hz#02 and Hz#05 = (1E-02)/100*03= 3.33E-04 [per ft].

*It has been decided to reduce the IM, as it is considered that the last barrier negatively impacted by the corresponding operational hazard is not completely broken, but its efficiency is only reduced to some extent. Another element that the IM also accounts for is the exposure time before the operational hazard detection and subsequent mitigation; the shorter the exposure time, the lower the risk is for which a smaller IM is more appropriate.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

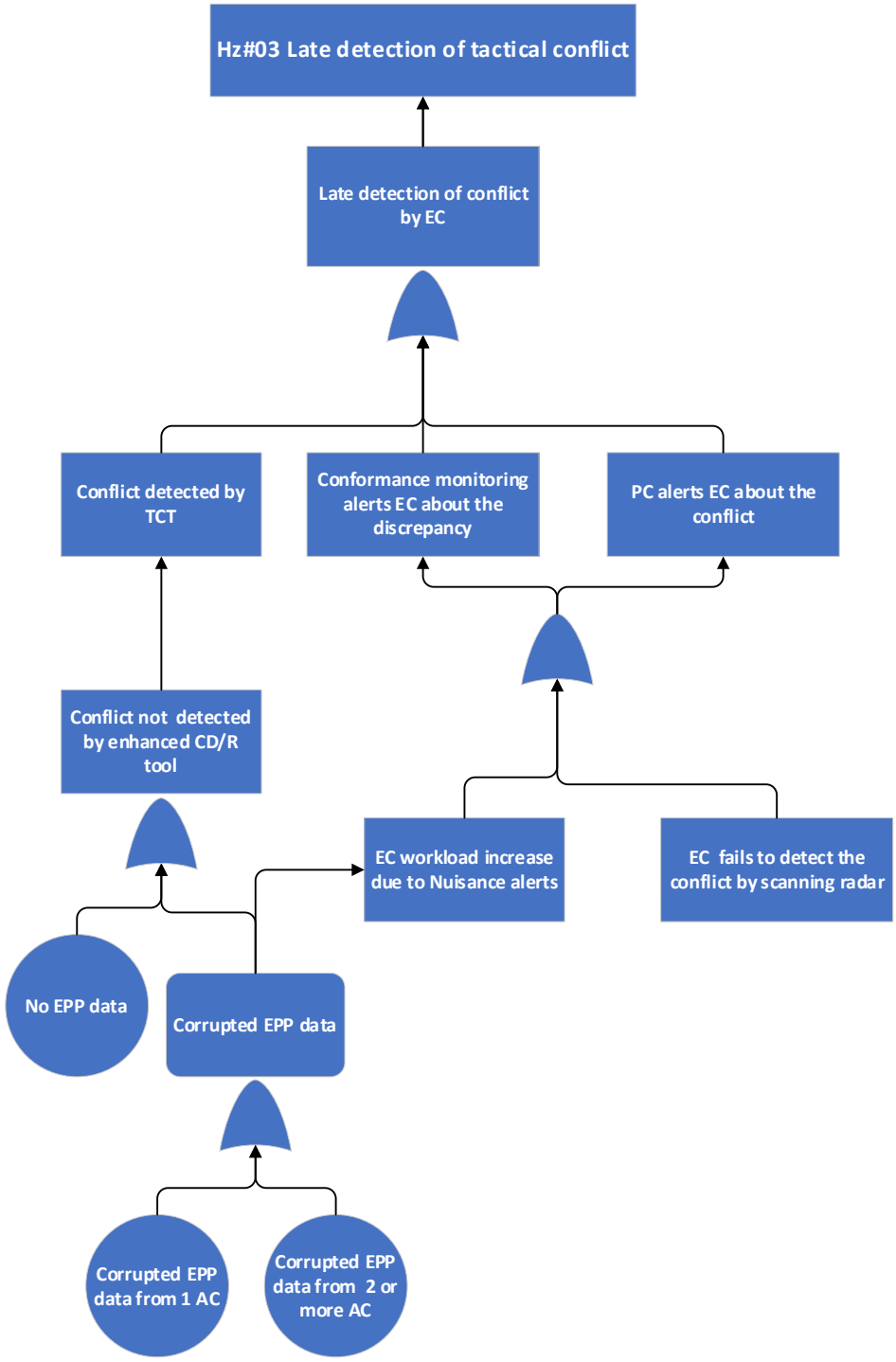

Figure 2. Fault Tree (supporting the causal analysis of Provide Tactical Separation Assurance with Reduced Uncertainty)

Cause	Detailed description	Mitigation/Safety Requirement
No data input	The CD/R tools use FDP based TP functions as an input and detect conflict	REQ-18-W2-53B-SPRINTEROP-UU01.0001 ADS-C EPP data validity information

EUROPEAN PARTNERSHIP
Co-funded by the European Union

	based on conventional parameters/tools. EC and PC adapt the separation strategy accordingly	The Separation Assurance process shall adapt itself to the quality and reliability of each flight's predicted trajectory. REQ-18-W2-53B-SPRINTEROP-UU01.0002 Awareness of ADS-C Availability and Validity for a Flight The ATCO shall be able to identify flights for which ADS-C data has been received and is valid. REQ-18-W2-53B-SPRINTEROP-SAF1.0007 Contingency procedures should be in place for transition to conventional TP and CD/R tools in case of improved TP failure or lack of data (ADS-C/EPP).
Corruption of ADS-C/EPP data CD/R tool either does not detect the conflict or provides false alert	The corruption of ADS-C/EPP data of a single A/C; if not detected by EC/PC, will be detected by conformance monitoring tools (lateral or vertical deviation) In later stages the TCT will detect the conflict prior to separation infringement. The corruption of EPP data of multiple AC Same as for single aircraft but with workload increase	REQ-18-W2-S53b-TS-0100.0010 Filtering outliers The En-Route / Approach ATC System shall check the downlinked data (including gross Mass, Speed schedule and EPP profile) for credibility prior to use it in ATC applications. *RE*Q-18-W2-53B-SPRINTEROP-UU01.0002 Awareness of ADS-C Availability and Validity for a Flight The ATCO shall be able to identify flights for which ADS-C data has been received and is valid. REQ-18-W2-53B-SPRINTEROP-SAF1.0008 Contingency procedures should be in place for transition to the conventional TP and CD/R tools in case corrupted data is received

Table 22. Fault tree causes and associated mitigations (SRD, preventing operational hazard occurrence).

G.1.2 Bottom-up failure modes and effects analysis

The bottom-up analysis of the failure modes of the TP enhancement to CD/R tools elements / element-to-element interfaces and of their effects has been performed in order to determine potential common cause failures but also in order to allow a more in-depth causal analysis of certain parts of the technical system design.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Functional system element	Failure mode	Effects	Mitigation/Safety Requirement	Operational hazard
TP	Corruption of ADS-C/EPP data	CD/R tool either does not detect the conflict or provides false alert	REQ-18-W2-53B-SPRINTEROP-SAF1.0009 TP and CD/R tools shall dynamically revert to "conventional" functioning mode (management of flight data without ADS-C/EPP) and use FDP based TP functions as an input. REQ-18-W2-53B-SPRINTEROP-SAF1.0010 ATCOs shall be informed with the appropriate notification (system reverting to reference scenario TP and CD/R tools performance) Assumption: The ADS-C/EPP data corruption as per EUROCAE ED-228A : 1.0E-03	All hazards MAC-SC4b
CD/R tools	Conflict not detected by enhanced CD/R tool	CD/R tool either does not detect the conflict	REQ-18-W2-53B-SPRINTEROP-SAF1.0011 The frequency of failure of CD/R tool with enhanced data (ADS-C/EPP) shall not be grated than 3.33E-04	All hazards MAC-SC4b

Table 23. Failure Modes and Effects Analysis

G.2 Deriving SRD from the SRS (functionality&performance) for protective mitigation

The purpose is to derive SRD (functionality&performance) from the SRS (functionality&performance) that have been derived in §4.4.2 to provide mitigation against operational hazard effects (protective mitigation), with due consideration of the potential common cause failures that might affect the operational hazard causes and its protective mitigation.

Table 24 shows the Safety Requirements at ATS Service level (SRS) functionality&performance derived in section 4.4.2 for protective mitigation map onto the related elements of the Design Model (functional system components or interactions/data flows) and derive additional Safety Requirements

EUROPEAN PARTNERSHIP

Co-funded by the European Union

at Design level (SRD) (functionality and performance) for internal failure conditions of operation. Include the following information:

- the SRS (functionality and performance) derived in §4.4.2 to provide mitigation against operational hazard effects (protective mitigation),
- the derived SRD driven by the mapping of the SRS onto the related elements of the Design Model, together with any necessary assumptions,
- the Design Model elements (functional system components or interactions/data flows or external elements impacted by the Change) relevant for the derived SRD and/or assumptions.

SRS (functionality&performance) for protective mitigation (ID & content)	**Safety Requirement at Design level[4] (SRD) or Assumption**	**Maps onto**
SRS-101 The CD/R tools shall indicate if the probability of an encounter increases.	REQ-18-W2-53B-SPRINTEROP-SAF1.0002 Nuisance Alerts The rate of nuisance alerts derived from enhanced TP shall be reduced as compared to the current operating method. REQ-18-W2-53B-SPRINTEROP-SAF1.0004 Detection of True Conflicts The enhanced TP shall contribute to the CD/R tool detecting true conflicts with a greater accuracy than the current TP and CD/R tools.	NSV-4 for the reception of the EPP data Trajectory Prediction Management Support Functions – Build grid with ADS-C MET data NSV-4 for the Trajectory Computation and Conflict Detection process Trajectory Prediction Management
SRS-102 ATCO shall have an indication in radar label if aircraft is transmitting ADS-C/EPP info (or information is received from ground system).	REQ-18-W2-53B-SPRINTEROP-SAF1.0001 Data Verification The data received through ADS-C and other external sources (MET provider data) shall only be used once verified	NSV-4 for the Trajectory Computation and Conflict Detection process Trajectory Prediction Management

[4] iSRD for the initial design or rSRD for the refined design

	and checked for timeliness, accuracy, completeness and consistency. REQ-18-W2-53B-SPRINTEROP-SAF1.0005 Aircraft Equipage Where the controller's separation strategy is adapted based on aircraft ADS-C equipage and availability of EPP data, the availability of ADS-C/EPP data related to a specific flight (aircraft equipage and quality of data received) shall be displayed to the controller in an unambiguous manner.	
SRS-103 ATCO shall verify the data received, i.e. the conflict detection quality assessment (figure of merit), allowing them to adapt their strategies and approach according to it, if deemed necessary.	REQ-18-W2-53B-SPRINTEROP-SAF1.0011 Conflict detection confidence level The information about the conflict detection quality assessment (figure of merit) should be available to ATCOs, allowing them to adapt their strategies and approach according to it, if deemed necessary.	NSV-4 for the Trajectory Computation and Conflict Detection process Trajectory Prediction Management

Table 24: SRD derived by mapping SRS (functionality&performance) for protective mitigation on to Design Model Elements

Appendix H Demonstration of Safety Criteria achievability

The demonstration of the achievability of the SAfety Criteria holds to the extent where these exercises/analyses address all the SRS (functionality&performance), and more specifically, all the derived SRD (functionality&performance) (the SAC achievability accounting for internal functional system failures, i.e. considering the integrity&reliability safety requirements can be demonstrated only by predictive safety assessment – see sections 4.4 and 5.5).

The safety-related outcomes of the validation exercises (traced back to the safety validation objective and related success criteria) bring an essential contribution to the demonstration of the Safety Criteria achievability by the Solution design.

The safety-relevant results of the validation exercises are summarized in the Table 25, whilst indicating for each safety validation objective / success criteria which relevant SRS have been covered.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

OBJ-18-W2-53B-V3-VALP-005 To assess the impact of enhanced CD&R tools using aircraft data on safety.					
SAC	Coverage (SRS and/or SRD)		Success criterion	Exercises Results	
SAC-18-W2-53B-ER-TMA -001	SRS-001 SRS-002 SRS-003 SRS-101 SRS-102 SRS-104	CRT-18-W2-53B-V3-VALP-005-001	There is no increase in the number of pre-tactical planned conflicts taking into consideration increase in traffic.	The two exercises that addressed this SC (EXE009, and EXE012) concluded that there is no increase in the number of pre-tactical planned conflicts taking into consideration increase in traffic	OK
SAC-18-W2-53B-ER-TMA -002	SRS-004 SRS-103 SRS 105 SRS 106 SRS 107	CRT-18-W2-53A-V2-VALP-004-002	There is no increase in the number of planned tactical conflicts taking into consideration increase in traffic.	The two exercises that addressed this SC (EXE009, and EXE012) concluded that there is no increase in the number of planned tactical conflicts taking into consideration increase in traffic.	
		CRT-18-W2-53B-V3-VALP-005-003	There is no increase in the number of ATC-induced tactical conflicts taking into consideration increase in traffic.	No exercise addressed this SC.	
SAC-18-W2-53B-ER-TMA -003	SRS-001 SRS-002 SRS-003 SRS-004	CRT-18-W2-53B-V3-VALP-005-004	There is no increase in the number of imminent separation infringements taking into consideration increase in traffic.	The two exercises that addressed this SC (EXE008, and EXE012) concluded that there is no increase in the number of imminent separation infringements taking into consideration increase in traffic.	

EUROPEAN PARTNERSHIP

Co-funded by the European Union

All SACs	SRS-001 SRS-002 SRS-003 SRS-004	CRT-18-W2-53B-V3-VALP-005-005	The implementation of CD&R support tools does not deteriorate human performance impacting safety.	Four exercises addressed this SC: EXE008, EXE009, EXE011 and EXE012. EXE008, EXE009 and EXE012 concluded that the implementation of CD&R support tools does not deteriorate human performance impacting safety. For EXE011 some issues have been reported during exercises, and even if no major negative points have been reported leading to a decrease either of human performance or safety aspects, it seems necessary to confirm these results. As a conclusion the SC was considered Partially OK. Considering the results of the four exercises the SOL53B overall conclusion for this SC is considered OK.	

Table 25: Solution Safety Validation result

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix I Assumptions, Safety Issues & Limitations

I.1 Assumptions log

Ref	Assumption	Validation
A001	The EUROCAE ED-228A (Ref [12]) is the standard of reference related to ADS-C and ADS-C EPP (We recall that EPP is provided by ADS-C).	Current regulations
A002	According to Commission Implementing Regulation (EU) No 1028/2014, published on 26/09/2014, amending EU Regulation No 1207/2011, by June 2020, all aircraft operating IFR/GAT in Europe and with a maximum certified take-off mass exceeding 5 700 kg or having a maximum cruising true airspeed capability greater than 250 knots are required to carry and operate Mode S Level 2s transponder(s) with Mode S Elementary Surveillance (ELS), Enhanced Surveillance (EHS) (for fixed wing aircraft) and ADS-B 1090MHZ Extended Squitter (ES) capabilities.	Current regulations
	The Planning conflict detection aid tool shall be active at all CWPs at all times	Current operations
	The Tactical conflict detection aid tool shall be active at all CWPs at all times.	Current operations

Table 26: Assumptions log

I.2 Safety Issues log

N/A

I.3 Operational Limitations log

N/A

EUROPEAN PARTNERSHIP

Co-funded by the European Union

-END OF DOCUMENT-

EUROPEAN PARTNERSHIP

Co-funded by the European Union

EUROPEAN PARTNERSHIP

Co-funded by the European Union