INDUSTRIAL RESEARCH

sesar JOINT UNDERTAKING

SESAR Solution 38 SPR-INTEROP/OSED for V3 - Part II - Safety Assessment Report

Deliverable ID:	**D2.1.008**
Dissemination Level:	**PU**
Project Acronym:	**PJ07-W2-OAUO**
Grant:	**874465**
Call:	**H2020-SESAR-2019-1**
Topic:	**SESAR-IR-VLD-W2-06-2019**
Consortium Coordinator:	**EUROCONTROL**
Edition Date:	**22 February 2023**
Edition:	**00.01.01**
Template Edition:	**00.00.03**

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Authoring & Approval

Authors of the document

Beneficiary	Date
EUROCONTROL	22/02/2023

Reviewers internal to the project

Beneficiary	Date
AIRBUS SAS	16/12/2022
EUROCONTROL	16/12/2022
METRON	16/12/2022
Navblue	16/12/2022
DSNA	16/12/2022
ENAV	16/12/2022
Dassault	16/12/2022
Thales Air Sys	16/12/2022

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 SAS	10/01/2023
EUROCONTROL	10/01/2023
METRON	10/01/2023
Navblue	10/01/2023
DSNA	10/01/2023
ENAV	10/01/2023
Dassault	10/01/2023
Thales Air Sys	10/01/2023

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Rejected By - Representatives of beneficiaries involved in the project

Beneficiary	Date
NIL	

Document History

Edition	Date	Status	Beneficiary	Justification
00.00.01	01/09/2022	Initial draft	EUROCONTROL	Initiation of the document
00.00.02	28/10/2022	Draft	EUROCONTROL	Document updated to complete sections 4 & 5
00.00.03	28/11/2022	Final draft	EUROCONTROL	Final draft for review
00.01.00	13/01/2023	Final	EUROCONTROL	Final update for transmission to the SJU
00.01.01	22/02/2023	Final	EUROCONTROL	Final version after SJU review and internal Maturity Assessment

PJ07-W2-OAUO

PJ07-W2 OAUO OPTIMISED AIRSPACE USERS OPERATIONS

This Safety Assessment Report is part of a project that has received funding from the SESAR3 Joint Undertaking under grant agreement No 874465 under European Union's Horizon 2020 research and innovation programme.

Abstract

This document specifies the results of the safety assessment activities carried out in SESAR2020 Wave 2 by Project PJ.07-W2 Solution 38 "Enhanced integration of AU trajectory definition and network management processes".

This Safety Assessment Report (SAR) represents the Part II of the SPR-INTEROP/OSED (Safety and Performance - Interoperability Requirements/ Operational Service and Environment Definition) and contributes to the SPR-INTEROP/OSED Part I and TS/IRS (Technical Specifications/ Interface Requirement Specification) documents.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Table of Contents

EUROPEAN PARTNERSHIP

Co-funded by the European Union

List of Tables

EUROPEAN PARTNERSHIP

Co-funded by the European Union

List of Figures

No figures entries found.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

1 Executive Summary

This document contains the Specimen Safety Assessment for a typical application of the PJ07-W2 Solution 38 “Enhanced integration of AU trajectory definition and network management processes”. The Safety Assessment Report (SAR) represents Part II of the SPR-INTEROP/OSED document and presents the assurance that the Safety Requirements for the V1-V3 phases are complete, correct and realistic, thereby providing all material to adequately inform the PJ07-W2-38 Solution SPR-INTEROP/OSED and TS/IRS.

This Safety Assessment Report (SAR) represents the Part II of the SPR-INTEROP/OSED (Safety and Performance - Interoperability Requirements/ Operational Service and Environment Definition) and contributes to the SPR-INTEROP/OSED Part I and TS/IRS (Technical Specifications/ Interface Requirement Specification) documents.

This safety analysis is based on the work done by projects PJ07-01 and PJ09 in SESAR2020 Wave 1, contained in the corresponding SARs [7] [8]. The current version of the document contains updates with the work done for the PJ07-W2-38 concept in SESAR 2020 Wave 2.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

2 Introduction

2.1 Background

Solution PJ07-W2-38 validation builds upon the results delivered by:

SESAR 1

- P7.6.2 Step 1: The analysis of the FF-ICE Planning, in particular as an evolution of the Extended Flight Plan processes to align with the FF-ICE Provisions
- P7.6.2 Step 2: The development of the process of submission of the Airspace User's 4D business trajectory to the Network Management Function (NMF) for accommodation in the ATM network during the Business Trajectory Short Term Planning Phase
- SWP11.1, EXE 713: The EFPL concept was developed and validated reaching a V3 maturity level

and SESAR 2020 Wave1

- PJ.07-01 & PJ.09-03: Development of AOWIR (trial requests) and FDCI (mechanism to notify critical flights to NM/FMP; by sharing this information via the NOP) concepts.

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 service provision 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 service provision 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 V2 and V3 of the Solution development (Safety Requirements at service level and at design level).

From a safety assessment perspective, this safety assessment is considered as Other than ATS operational solution, meaning that the change affects the services delivered to ATS providers, other service providers or aviation undertakings (the WHAT and the HOW). The design safety driver is the specification of the changed service limited to the potential safety implication on the side of the ATS service provider or aviation undertaking (e.g. airline) using that service. Solution PJ07-W2-38 addresses the interaction between the Airspace Users and the Network Management function (NMf) for defining the trajectory of a flight in the planning phase by enhancing the integration of AU trajectory definition and network management processes. Therefore, the change brought by the solution does not affect directly ATS services (no direct impact on the way ATCOs and Pilots act, interact and make use of tools/equipment in view of delivering ATS), but rather focuses on the planning phase, therefore services delivered AU and ANSPs prior to the execution phase.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

2.3 Scope of the Safety Assessment

The PJ.09-W2-38 safety assessment makes extensive use of outcomes from previous PJ07.01 and PJ09 SARs [7][8].

The following parts of the safety assessment lifecycle are covered by the safety assessment work undertaken and documented in this Safety Assessment Report (SAR):

This Safety Assessment Report contains the results of a safety assessment conducted according to SESAR SRM up to and including V3 maturity level. This contains:

- V1 - through initial identification of safety implications of the Change and the definition of the Safety impact of the Intended Use (fully covered within this document and in the Safety Plan),
- V2: e.g. safety specification at operational service level (mainly establishing Safety Requirements at Service level- SRS), safe initial design (mainly deriving Safety Requirements at initial design level -iSRD to be documented as appropriate in SPR-INTEROP/OSED and TS/IRS),
- 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).

PJ07-W2-38 addresses the following Operation Improvements (OIs):

- AUO-0219: Use of Enriched DCB Information and Enhanced What-Ifs to Improve AU Flight Planning
- AUO-0208: Use of Simple AU Preferences in DCB Processes

The improvements brought by PJ07-W2-38 per concept area can be found in section **Error! Reference source not found.** of this document or in the corresponding SPR-INTEROP/OSED [10].

The Safety assurance activities will be conducted in line with the SESAR 2020 Safety Policy, SESAR SRM [2] and accompanying Guidance [3].

2.4 Layout of the Document

Section 1 presents the executive summary of the document

Section 2 provides the background of the concept, the general approach to safety assessment in SESAR and the scope of this safety assessment

Section 3 provides the operational concept overview and the scope of the change, summarises the solution operational environment and key properties together with the stakeholder's expectations and derives the Safety Drivers

Section 4 addresses the safety specification at Service level, through the definition of SRSs

Section 5 addresses the safe design of the solution, through the derivation of SRDs and link to validation results

Section 6 demonstrates the achievability of the service safety specification

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Section 7 presents the acronyms and terminology

Section 8 presents the list of references

Appendix A presents the EATMA models

Appendix B presents the collection of Assumptions, Safety Issues and Operational limitations

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

The information provided in this section is a short summary. For more details, please refer to the PJ.09-W2-38 SPR-INTEROP/OSED [10].

The Solution PJ.07-W2-38 aims to reduce the impact of ATM planning on Airspace Users' constraint and criteria (especially costs and efficiency of operations) by allowing them to better cope with ATM constraints and network opportunities. Among other benefits, enhancing the CDM planning between the providers and the users ensures a better adherence to the agreed trajectory during execution, hence a better predictability on the traffic demand.

Its main objective is to improve Airspace Users flight planning and network management through improved FOC participation into the ATM network collaborative processes in the context of FF-ICE and its potential evolutions.

Enriched DCB information

FF-ICE/1 Services include basic DCB information. The new operating method relies on the distribution of Enriched DCB information, which consists of more specific and complete DCB information, including information on opportunities for the Airspace Users but also risks of activation of constraints in the future.

In addition to the DCB measures information, Network Operations regional will include enriched DCB information in terms of hotspot information, congestion level indicators and pre-allocated CTOT/TT (CTOT/TT information before officially published) along the submitted Desired Route/Trajectory. That information sharing will propitiate common situational awareness, which will improve the AU decision-making process.

To mitigate DCB negative impact on flights, AU will be able to use the trial request service to ask Network Operations what-if analysis related to trajectory acceptability, DCB constraints and enriched DCB information to check new routes with their DCB situation before making a decision. This will allow the AU to adopt the most convenient trajectory adapted to the Network DCB situation.

Protection Hotspots

Two types of hotspots are envisaged as part of Enriched DCB information provided to the AUs along a trajectory:

- Resolution hotspot: Hotspot associated to an overloaded traffic volume and for which the FMP plan to apply DCB measures (cherry-picking/STAM measures principally) to solve the overload. This type of hotspot is not new.
- Protection hotspot: Hotspot associated to a traffic volume which is usually close to saturation to protect an airspace from undesired rerouted flights and prevents the application of DCB measures

The protection hotspots will follow the same rules as the current (resolution) hotspots for their publication, and will be used for several purposes:

- Avoid an increase of network instability: in particular, the creation of last minute airspace overloads due to AUs re-routings inducing new DCB constraints and further re-rerouting.

- Keep spare capacity in some specific airspace when needed to increase safety and efficiency of tactical DCB flow measures.

The protection hotspot information will be provided to the AUs after flight plan filing or in the context of the what-if & what-else functions use. FPLs which had already been filed through the concerned TV before PH declaration are not concerned.

NMF will consider protection hotspots when proposing trajectory options to AUs either in the context of what-if requests or FPL improvements. Trajectory options on-loading a protection hotspots will not be proposed.

Simple preferences

Provision of additional information released by the Airspace User to NMF to indicate the importance of some critical flights to progress on time or other preference as for instance flight level preference. Hence, flow management should preferably assign no delay or limited ATFCM delay to those flights and adapt the measure to AU preference.

FDCI is a parameter provided by the Airspace User to indicate the importance for the flight to progress on time. Hence, the flight should preferably not be assigned any or much delay and it should even be tried to decrease an allocated delay if possible by NMf.

Two types were identified:

- Proactive FDCI (to be validated during W2): issued for really critical flights before any DCB measure is allocated to the flight. The intention is that NMF consider this information before implementing any measure. Reasons to use P-FDCI are for example to avoid a curfew, not to miss an important connection, crew hours, to avoid incurring unnecessary high costs to the AU.

- Reactive FDCI (validated during W1, V3 maturity, no further research in PJ07-W2-38): issued when a DCB measure is already affecting the flight with the aim that NMF can take any corrective action to reduce the impact.

The FDCI consists of three attributes:

- A first attribute reflecting the criticality, which will be shown in the flight list as an additional column.

- A second indicator containing the reason.

- A third one being the time tolerance (maximum acceptable delay) that will be used by NMF as a help to resolve the problem.

Other information managed by NMF:

- Status, to indicate the situation of the flight: Proposed, Accepted, Unable, Under Work, On Hold.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Rules to prevent abusive use of FDCI:

- Maximum number of FDCI request per AU per day.
- Maximum number is weighted considering the number of flights that the airline has in ECAC area.

Management of Pro-active FDCIs in flow management (NM regional and local levels)

- Both NMOC operators and INAP will have the P-FDCI information and take it into account to:
  - Coordinate for slot exemptions (or force slots) in regulations
  - Use P-FDCI information to determine which type of DCB measures (e.g. regulation vs re-routing/level capping measures) should be applied to solve a DCB problem.
- In addition, INAP will use P-FDCI information – among other criteria - to determine to which flights they will apply MCP delay measures

3.2 Solution Operational Environment and Key Properties

The majority of the functions described in the PJ07-W2.38 SPR-INTEROP/OSED are designed in order to allow their implementation in both the current environment and in the SESAR2020 environment dealing with trajectory management.

3.2.1 Airspace Characteristics

Managed airspace encompassing all ECAC area, even though the solution will focus on medium/high complexity airspaces and airspaces that need to manage high complexity departures and arrivals.

The Airspace layout will be the current ICAO ATS airspace classifications (controlled airspace), regulations and applicable rules.

3.2.2 Airspace Users – Flight Rules

Scheduled IFR flight operations within the ECAC area (encompassing flights departing/arriving/overflying the ECAC area).

3.2.3 Ground ATM/ATFCM capabilities

Ground systems shall need to be updated in order to include the possibility of declaring Protection Hotspots and the reception and processing of FDCI.

The ground ATM capabilities outside scope of but relevant for PJ07-W2-38:

- NOP functionality
- What-If / What-Else functionality
- SWIM matured as per SESAR 2020 (enabling Ground-ground interconnection)

EUROPEAN PARTNERSHIP

Co-funded by the European Union

3.2.4 AU Capabilities

Regarding the FOC system, necessary adaptations for including the Simple Preferences and hosting the What-if related queries & results, only high-level design & requirements are within the Solution scope whilst AUs will manage the detailed design& implementation in their FOC system.

3.3 Stakeholders' expected benefits with potential Safety impact

According to the information included in the VALP document [11], the solution expects to have a positive impact on the Network, by improving (not limited to):

- Punctuality, considering that if there is a better use of the available capacity, then there will be as an effect a reduction in the departure delay, leading to better punctuality. In addition, punctuality for specific flights (those considered critical) will be increased and indirectly for all following flights in the rotation due to the reduction or cancellation of ATFCM delay.
- Increased predictability, thanks to the provision of accurate and enriched DCB information to AUs that will allow them to better plan their Flights. Therefore, reducing the difference between actual & Flight plan durations.
- Network capacity (not official KPA for this solution), taking into account enriched DCB information will allow to better manage network effect and use available capacity and thus minimize the creation of new hotspots and Regulations.

In addition, the solution might have a marginal positive impact on Fuel efficiency and Flight times due to the avoidance of some RADs & scenarios hence contributing to sustainability objectives.

3.4 Intended Operational use of the Service Concept

3.4.1 Intended use identified from SESAR Operational Solutions

No SESAR2020 operational solution has been identified as providing specific requirements for the *NM Flight Planning* and the *NM Flow and Capacity Management* Services.

Following the information included in the Safety Assessment Plan and the potential interaction with PJ07-W2-39:

Pro-active FDCI is somehow related to Selective Flight Protection, considering that there is overlap on traffic prioritisation but with important differences as: FDCI acts in both En-Route and Airport domains and it is limited to very few flights, while the SFP to be developed in Sol 39 is targeted in Arrival management.

As such, no specific requirements coming from PJ07-W2-39 have been identified.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

3.4.2 Other intended use outside-SESAR

Currently, all the Airspace Users make use of the *NM Flight Planning* and the *NM Flow and Capacity Management* Services. In addition, ANSPs in Europe make also use of the NM Flow and Capacity Management Service provided currently by NMOC to solve DCB imbalances (in view of avoiding overloads in ATC). PJ07-W2-38 does not aim to modify the services provided per se, but to introduce new information in the FPL that needs to be properly processed by NM and a new way of solving DCB imbalances while taking into account the AU needs. The solution also aims to provide additional information to AU to be used during FPL filling.

3.5 Relevant applicable standards

AUO-0219: Protection Hotspots

The protection hotpot topic is not relying on or impacting the current implementation of FF-ICE increment 1 as mentioned in Common Project 1 (CP1) regulation.

However further steps of FF-ICE/1 implementation may include the complete integration of flight planning and flow management information exchanges. In that context, protection hotspot information should be provided by NM in the FF-ICE planning, filing and trial services as part planning/filing response to AU FF-ICE/1 flight plan submission/trial.

AUO-0208: P-FDCI

The pro-active FDCI topic is not relying on or impacting the current implementation of FF-ICE increment 1 as mentioned in Common Project 1 (CP1) regulation.

However further steps of FF-ICE/1 implementation may include the integration of fleet prioritisation information in flight planning/flow management information exchanges.

In that context P-FDCI information should be part of FF-ICE/1 fleet prioritization information to be in flight plan information to be considered both in FF-ICE planning and filing services.

For both OIs, there is no need to standardise at worldwide level. This could be addressed in a European FIXM extension.

3.6 Safety Driver

Based on the SESAR2020 SRM guidance update, in order to address the change introduced by PJ07-W2-38 impacting “Other-than-ATS” operational services (e.g. DCB service provided by NMf), a set of SIIU (Safety impact of the Intended Use) have been identified.

The baseline for defining the change for the Other-than-ATS operational services are the services as defined by the regional Network Manager (NM) in the ‘NM Flow and Capacity Management Service Specification’ [12]. Please note that, even though the baseline refers only to regional NM services, the services in the SIIUs defined in this section refer to the NM function (NMf). SIIUs were defined only on the services where it was identified that PJ07-W2-38 is introducing a change with safety impact.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SIIUs:

Due to the indirect safety impact that the service might have in the ATS operations in case the service is not properly delivered, the following initial set of Safety impact of the Intended Use (SIIU) needs to be defined:

The following SIIU was derived in order to express in a high-level manner the impact on the Short Term DCB service:

SIIU000: The change introduced by PJ07-W2.38 to the NM Flow and capacity management service shall not increase the number of overloads.

This high-level SIIU needs to be further fragmented according to the components of the Short Term DCB service:

In order to account for the impact on the "Load and Capacity Monitoring" service (this service includes provision of traffic demand and capacity data to NM users, as well as monitoring of these data to ensure demand does not exceed the declared capacity; it contains two service components: *Demand Data Provision* and *ATC sector load and capacity monitoring*):

SIIU001: The Load and Capacity Monitoring service delivered to ATS, service that is impacted by PJ07-W2.38 with the possibility of publishing Protective Hotspots, provision of Enriched DCB information and AU inputs, shall at least not increase the number of overloads.

In order to account for the impact on the *ATFCM measure design* function inside the "Demand and Capacity Balancing" service (purpose of this service is to react when the predicted traffic demand is higher than the available capacity by considering, assessing and implementing adequate solutions - ATFCM measures; it contains, among others, the following functions identified as impacted by the solution: *ATFCM measure design* and *Network cherry-pick regulations*)

SIIU002: The ATFCM measure design service delivered to ATS, service which is modified by PJ07-W2.38 with the AUs inputs and new functionalities (e.g. What-if/What-else) shall not increase the number of overloads.

SIIU003: The Network cherry-pick regulations service delivered to ATS, service which is modified by PJ07-W2.38 with the AUs inputs and new functionalities (e.g. What-if/What-else) shall not increase the number of overloads.

4 Safety specification at Service level

The purpose of this section is to present the Safety Requirements at Service level for the corresponding "Other than ATS" operational services.

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

4.1 Overview of activities performed

This section addresses the following activities:

- derivation of Safety Requirements at Service level (SRS) in normal conditions of operation for the modified Other-than-ATS operational services – section 4.2
- assessment of the adequacy of the 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 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 0
- 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 Service Safety specification – Normal conditions of operation

The purpose of this section is to derive Safety Requirements at Service Level (as part of the success approach) for the Other-than-ATS Operational Services, in order to ensure that the services are provided as specified under normal operational conditions (i.e. those conditions that are expected to occur on a day-to-day basis) such as to meet the defined SIIUs.

That comes to interpret, from a safety perspective, the SPR-INTEROP/OSED Operational Concept specification (i.e. how the concept contributes to aviation safety) following and making use of the EATMA representation as per the Operational layer (each Use Case being modelled through a process model made up of activities interacting via information flows). This analysis is performed following and making use of the SPR-INTEROP/OSED Use Cases and their representation through EATMA Process Models as defined by the PJ07-W2-38 SPR-INTEROP/OSED [10]. The purpose is to derive a complete list of SRSs, allowing to specify the Change involved by the concept at the Other-than-ATS operational service level. This shows how the SRSs contribute to meeting the Safety Drivers.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

ID	Safety Requirement at Service level (SRS) *(success approach)*	Use Case	Related Safety Driver
SRS 001	NMf shall provide the AU with enriched DCB information	AU usage of Enriched DCB information	SIIU001
SRS 002	NMf shall continue to appropriately assess traffic demand with ATFCM situation	AU usage of Enriched DCB information	SIIU001
SRS 003	NMf shall continue to appropriately define and apply the DCB solution	AU usage of Enriched DCB information	SIIU001 SIIU002 SIIU003

Table 1: List of SRS (functionality and performance) for normal conditions of operation

P-FDCI Use Cases have also been assessed. Considering that R-FDCI concept is already implemented and in operations, and given that P-FDCI would come even before any DCB measure is in place, it is considered that the P-FDCI concept has no impact on safety.

4.3 Service Safety specification - Abnormal conditions of operation

The following list of abnormal conditions has been identified, based on previous SESAR 2020 Wave 1 PJ07-01, and PJ09 safety assessments:

ABN1. NOP failure resulting in loss of information to Local and Regional ATFCM users

ABN2. ETFMS or IFPS failure with major loss of FPLs

ABN3. Unforeseen airspace closure (e.g. Volcanic Ash, nuclear cloud …)

ABN4. Altered weather conditions

ABN5. Sudden change in weather conditions

ABN6. Unplanned Aerodrome closure

ABN7. Unplanned limitation in capacity (ATC ground system failures, unforeseen sector closure/regrouping)

The table below assesses, for each abnormal condition, the immediate effect on the new concept and identifies the possible mitigations of the safety consequence of the operational effect with a reference to the means available in the operational environment. When necessary (i.e. when a change introduced by PJ07-W2-38 was identified) additional mitigation means might be specified in terms of new SRSs.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SRSXXX]
ABN1	NOP failure resulting in loss of information to Local and Regional ATFCM users	NMf will not be able to monitor imbalances and to detect and declare hotspots. Consequently no new ATFCM regulation or STAM measure can be designed and no information will be shared with the AU. If the degradation will last longer (e.g. more than half an hour) restrictive regulations will be implemented. AU will need to wait for failure recovery before being able to optimise their FPLs according to the updated traffic situation	Restrictive regulations in case of long lasting degradation
ABN2	ETFMS or IFPS failure with major loss of FPLs	NMf will not be able to monitor imbalances and to detect and declare hotspots. Neither new ATFCM regulation or STAM measure can be designed, nor the already designed ones can be implemented. Lost FPLs will need to be refiled by AUs and no optimisation will be possible.	Restrictive regulations will be implemented
ABN3	Unforeseen airspace closure (e.g. Volcanic Ash, nuclear cloud …)	In the short term: Source of new hotspots that might turn the existing regulations/STAM insufficient or inefficient and invalid the previous PFP optimisations. In the mid/long term: Information (E.g. Dynamic Airspace Constraint) will be shared with the AU in order to optimise their PFPs	Short term: None (ATC deals with the imbalance in the affected sectors) Mid/long term: Restrictive regulations if needed SRS001 (NMf shall provide the AU with enriched DCB information)

EUROPEAN PARTNERSHIP

Co-funded by the European Union

ABN4	Altered weather conditions	Specific conditions are developing locally which require adopting and coordinating a planned "axis management" scenario implementation with special and possibly earlier scenario activation Information (E.g. Dynamic Airspace Constraint) will be shared with the AU in order to optimise their FPLs	Coordination of a planned "axis management" scenario implementation SRS001
ABN5	Sudden change in weather conditions	In the short term: Source of new hotspots that might turn the existing regulations/STAM insufficient or inefficient and invalid the previous FPL optimisations.	Short term: None (ATC deals with the imbalance in the affected sectors)
ABN6	Unplanned Aerodrome closure	Small/medium Airport: Partial implementation of DCB measures. Large Airport: More global impact than the scope of current safety assessment With regards to the Solution, for all type of Airports: Previous FPL optimisations will be invalidated. Information (E.g. Dynamic Airspace Constraint) will be shared with the AU in order to optimise their PFPs	DCB measures need to be re-assessed and new measures implemented, whenever applicable Restrictive regulation SRS001
ABN7	Unplanned limitation in capacity (ATC ground system failures, unforeseen sector closure/regrouping)	Same as per Small/medium Airports from above	See above

Table 2: Analysis of the impact of the change in Abnormal Conditions

No new SRSs have been derived linked to the analysis of the abnormal conditions

EUROPEAN PARTNERSHIP

Co-funded by the European Union

4.4 Mitigation of the System-generated Risks (failure conditions)

This section addresses the processes in the case of internal failures of the Functional System within the Solution scope. Before any conclusion can be reached concerning the adequacy of the safety specification of the Solution at the OSED level, it is necessary to assess the possible adverse effects that failures internal to the Functional System within the Solution scope might have upon the provision of the relevant operational services and to derive safety requirements at service level (failure approach) to mitigate against these effects.

4.4.1 Service Hazards identification and analysis

The identification and analysis of the system-generated service hazards has been performed based on the analysis of the OSED Topics (represented through the EATMA Process Models). Due to the limited impact on Safety, no formal HAZID (HAZard IDentification) workshop, involving relevant operational and technical experts has taken place. The analysis and safety discussions have been performed through more informal meetings (either presential within EUROCONTROL team or virtually with other stakeholders), during Validation Exercise debrief and through the distribution of this document.

The analysis has been done through the following steps:

- Identification of the relevant operational failure modes at the level of the OSED Use Cases steps for each Topic;
- Immediate operational effect assessment;
- Identification of the possible mitigations of the safety consequence of the operational effect;
- Different failure modes leading to similar operational effects and displaying same mitigations of the safety consequence have been consolidated into Service Hazards;
- Assessment of the effects of the DCB service degradation on the ATS operations and further allocation of severity of the effect accounting for the mitigations of the safety consequences (i.e. available protective means once the service hazard occurred), as per the relevant Severity Classification Scheme(s) from Guidance E.3 of Reference [3].

Error! Reference source not found. represents the Hazard Identification outcomes and it displays for each system-generated service hazard, i.e. consolidated failure modes of the Functional System which were concluded to have a safety impact, the operational effect, their mitigation and the severity class allocated. The service hazards were derived at the level of the Use Case specified in OSED [10]. The table is organized as follows:

- Column 1 indicates the service hazard reference,
- Column 2 provides the description of the service hazard,
- Column 3 indicates the related functionality & performance Safety Requirement at Service Level in normal conditions - success approach (generally the service hazard represents a mode of failure to meet that SRS),
- Column 4 summarizes the effects of the service hazard on the ATS operations,
- Column 5 indicates the mitigations of hazard effects, in terms of available protective means once the service hazard occurred,

- Column 6 indicates the AIM-based severity applicable to the service hazard effects on the ATS operations, together with the Impact Modification factor IM as per Guidance E.3 of the SRM [3]. Note that the hazards involving severe sector(s) overload are assigned a factor IM=10 in order to reflect that the impact on sector results in reduced efficiency of the tactical conflict management barrier (and as such a more stringent integrity SRS will be allocated compared to a service hazard of the same severity, which would result in more demand for risk mitigation).

EUROPEAN PARTNERSHIP

Co-funded by the European Union

ID	Service Hazard Description	Success SRS	Operational effect	Mitigations protecting against propagation of effects	Severity *(most probable effect)*
Hz#01	ATFM measures not designed or not implemented or implemented partially by NMf	SRS 001 SRS 002	Risk for sector overload as the **DCB process** is not respected in terms of roles/responsibilities, procedures and timeline (including hotspot identification / declaration of the associated DCB measure implementation / coordination / implementation)	In case Network Operator (Local) does not identify hotspot, it might be detected at NM level (but that is not systematic) Tactical conflict management	MAC-SC4b IM=10
Hz#02	Inadequate ATFM measure designed and implemented by NMf	SRS 003	Risk for sector overload as a DCB measure is not correctly designed (in terms of problem analysis and impact assessment)	Potentially detected by the Network Operator (local or regional) Tactical conflict management	MAC-SC4b IM=10

Table 3 Service Hazards and Analysis

EUROPEAN PARTNERSHIP

Co-funded by the European Union

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

This section derives SRS (addressing integrity/reliability) to limit the frequency with which the system-generated service hazards could be allowed to occur using the Risk Classification Scheme for AIM MAC En-Route (from Guidance E of Reference [3]).

The SRSs associated to the service hazards (with sector overload as a potential effect) need:

- to be expressed "per sector operational hour", whilst the unit for the maximum tolerable frequency of occurrence in the Risk Classification Scheme is "per flight hour".
- to be computed whilst accounting for an Impact Modification factor (IM=10, which stands for the value that allows to allocate a more stringent SRS to service hazards involving sector overload compared to hazards displaying same severity but involving only individual flights. The value IM=10 has been assumed based on rough expert-based considerations on the acceptable frequency of occurrence of similar operational hazards in current operations)

Conversion from "per flight hour" to "per sector operational hour":

For one service hazard occurrence per hour, the affected traffic corresponds to those flight hours flown during one hour within the impacted area (which might be a high-density En-Route sector). The value used in RTCA/EUROCAE Operational Safety Assessments (e.g. the ADS-B RAD) is an average of 6 flight hours controlled per sector hour[1] for both the high density En-Route sector or the high density terminal area sector.

Illustration of SRS computation

The computation of the SRS (performed in accordance with Guidance E of Reference [3]) is illustrated via the example for Hz 02 below:

Hz 02: Inadequate ATFM measure designed and implemented by NMf

> As Hz 02 has been allocated severity MAC-SC4b (to which corresponds an MTFoO = 1E-02 per flight hour), the SRS is:

[1] The ADS-B-RAD and the Reference systems support the ATC Service in the following traffic densities:

- For a high density en-route airspace (ENVT-2) , a maximum of 6 flight hours controlled per sector hour and a maximum of 20 instantaneous count aircraft in a sector

Note: For high density en-route airspace, the figure is a result from combining a sector capacity with average flight time in sector related to high-density operations,

e.g. 60 flights per hour sector capacity with an average 6 minute flight length in sector, or another example could be 45 flights per hour sector capacity with an 8 minute average flight length.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

$$SRS_{102} = \frac{MTFo \ \ relevant\_severity\_class}{N \times IM} = \frac{1E-02}{100 \times 10} = 1E-05$$ [per flight*hour] = 1E-05 x 6 [per sector operational hour] = **6E-05 [per sector operational hour]**

Where:

N = 100 = overall number of operational hazards for the severity SC4b in the Risk Classification Schemes associated to AIM MAC ER model.

IM = 10 = the Impact Modification factor considered herein (see explanation above, second bullet under first paragraph of current sub-section)

The Max Tolerable Frequency of Occurrence (MTFoO) and the overall number of operational hazards per accident type (N) have been taken from the §E.2.3.3 of SRM Guidance E **Error! Reference source not found.**) as follows:

- MTFoO = 1E-2 and N=100 for Hz 01 and Hz 02 (MAC-SC4b)

The consolidated list of the derived integrity/reliability SRSs (failure approach) is provided in **Error! Reference source not found.** below:

SRS ID	Safety Requirements at Service level *(integrity/reliability)*	Related Service Hazard	Severity & IM
SRS 101	The likelihood of ATFM measures not designed or not implemented or implemented partially by Local ATFCM shall be no more than 6e-5 per sector operational hour	Hz 01	MAC-SC4b IM=10
SRS 102	The likelihood of inadequate ATFM measure designed and implemented by Local ATFCM shall be no more than 6e-5 per sector operational hour	Hz 02	MAC-SC4b IM=10

Table 4: Safety Requirements at Service level - integrity/reliability

4.5 Process assurance of the Safety Specification at service level

This section describes the processes by which Safety Requirements at Service level were derived as well as details of the competencies of the personnel involved.

In the frame of SESAR 2020 Wave 2, some informal meetings were held to address the specific change introduced by the PJ07-W2-38. These meetings were facilitated by SAF experts from EUROCONTROL and it included concept and validation experts but also Flow Managers.

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 (SRDs**) for the PJ07-W2-38 Solution. The SRDs are design characteristics/items of the Solution functional system to ensure that the system operates as specified and is able to achieve the SRS (because based on the verification/demonstration of these characteristics/items, it could be concluded that the SRS' are met, i.e. the SIIUs are satisfied).

In light of the maturity reached by the solution at the end of SESAR Wave 2, the safety assessment has been conducted at the refined design level; that comes to derive the complete set of safety requirements for the SPR-INTEROP/OSED (initial design level) and for the TS/IRS (refined design level), together with the collection of the technical mitigations resulting from the causal analysis of the operational hazards.

SRDs are placed on the elements of the Solution functional System that are changed or affected by the change (through change in behaviour or through new interactions introduced).

Because the Design Model might include interface/link with external elements which are out of the Solution scope but which are impacted by the Change, these external elements might also be identified as relevant and need to be recorded (in view of the stages post V3). Other assumptions might relate to matters outside the scope of the Change but which are essential to the completeness and/or correctness of the safety assessment results.

Operational Limitations might also be defined in case the safety assessment is not able to ensure that a risk is sufficiently mitigated by the derived SRD, considering the given architectural design.

Safety Issues might be raised in case of points remaining open in terms of risk mitigation within the scope of the actual version of the safety assessment. Either actions are taken allowing to resolve the safety issue within the current scope of the SESAR Solution or a strategy is proposed for a resolution beyond SESAR Wave 2 scope.

Any Assumptions, Safety Issues or Operational Limitations identified during the design process are also to be recorded in Appendix B.

Note: ensure all SRS referred in this section are captured in section 4 as necessary (including new ones, which might be identified during the design analysis).

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 and abnormal conditions of operation from the SRS (functionality and performance) of sections 4.2 and 4.3, and supported by the analysis of the design model - section 5.3

EUROPEAN PARTNERSHIP

Co-funded by the European Union

- assessment of the adequacy of the design (initial or refined) in the case of internal failures and mitigation of the Solution service hazards (identified at section 4.4.1) through derivation from SRS (integrity & reliability) of Safety Requirements (functionality & performance) and Safety Requirements (integrity&reliability) at Design level (SRD)- section 5.4
- realism of the refined safe design (i.e. achievability and "testability" of the SRD) - section 5.5
- safety process assurance at the initial or refined design level – section 5.6".

5.2 Design model of the Solution Functional System

The Design Model of the Solution functional system is a high-level architectural representation of the Solution system design that is entirely independent of the eventual physical implementation of the design post V3. It represents the architecture combining the elements composing the Solution Functional System in terms of procedures, human resources and equipment. Safety requirements at design level (SRD) are placed on those elements.

5.2.1 Description of the Design Model

The NOV-5 diagrams from OSED **Error! Reference source not found.** have been used in support of the design analysis.

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

The purpose of this section is to present the Safety Requirements at Design level (SRD) derived for Normal and Abnormal conditions of operation following **related SAF-GUI in STELLAR**.

The derivation of Safety requirements at design level - SRD for Normal and Abnormal conditions of operation is mainly driven by the SRS (functionality and performance) for Normal and Abnormal conditions of operation from sections 4.2 and 4.3.

Meanwhile additional SRD might be identified (and need to be documented here) from the static view and dynamic view analysis of the system behaviour in normal and abnormal operational conditions that needs to be conducted in order to show completeness/correctness of the Safety Requirements (Functionality and Performance).

It is reminded that any assumption, safety issue or operational limitation stated during the derivation of the SRDs for Normal and Abnormal conditions of operation are captured in Appendix B.

Finally, any additional SRD resulting from the analysis ensuring that the System design operates in a way that does not have a negative effect on the operation of related ground-based and/or airborne safety nets must be documented here as well.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

5.3.1 Safety Requirements at Design level (SRD) – Normal and Abnormal conditions

In the specific case of Pj07-W2-38 aiming end of V3 in Wave 2, the Project has already accomplished a significant part of the "success approach" as the derivation of the SPR-INTEROP/OSED requirements has been driven by a complete set of EATMA process models (NOV-5 diagrams). That systematic requirements derivation represents the assurance that the resulting set of requirements (operational, interoperability, and to some extent safety and performance as well) display a rather high degree of completeness, correctness and are provided with the appropriate rationale.

In that context, the work related to the safety requirements derivation at design level has been re-deployed (compared to the SRM-proposed methodology) according to the method explained below.

A Causal Analysis has been performed in the first place (see 5.4.1). This allowed to seek for the origin of the various failure causes, for each operational hazard, and to identify which are the SPR-INTEROP/OSED requirements (derived by the Project) with potential for generating such failure scenarios. In case such a requirement were not satisfied, that would contribute to an operational hazard and consequently that requirement has been placed in the SAFETY category i.e. it is a Safety Requirement (functionality and Performance).

The new derived "success approach" safety requirements and those already existing SPR-INTEROP/OSED requirements that have been identified in the SAFETY category have been further traced to the related operational hazards and ultimately consolidated in Table 6 below. In the meantime, the category SAFETY has been input to the "Category" field in the SPR-INTEROP/OSED requirements from section 4 of the SPR-INTEROP/OSED document.

Safety Requirement ID	Safety Requirement (functionality & performance) description	Related service hazard(s)
REQ-07.38-SPRINTEROP-OP01.0004	NO local should define threshold values for unplanned flights and be alerted when these are reached. The information shall be available in operations and for post operational analysis at NO local and regional level	Hz 01
REQ-07.38-SPRINTEROP-OP01.0009	The Network Operations (Local) should obtain from Network Operations (Regional) the information about refiling flights for ATFCM reasons increasing and/or decreasing the traffic load	Hz 01 Hz 02

Table 5 Safety Requirements at design level (functionality and performance) & potential safety impact (hazards) in case of non-compliance

In addition, it is considered that, when working in normal conditions, the number of overloads might not only remain at the same level but even be a little bit reduced. In order to account for this potential safety benefit, the following Requirement has been identified:

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Safety Requirement ID	Safety Requirement (functionality & performance) description	Derived from SRS (ID)
REQ-07.38-SPRINTEROP-OP01.0003	If a Flight plan with Desired Route/Trajectory is submitted to Network Operations (Regional), Network Operations (Regional) should extend the Planning Status reply to include (initial and subsequent updates) enriched DCB information along the submitted Desired Route/Trajectory	SRS 001

Table 6. Safety Requirements at design level (functionality and performance) satisfying SRS for Normal and Abnormal conditions

5.3.2 Dynamic Analysis of the initial design level Model – Normal Operational Conditions

The Project made full use of the validation exercises feed-back (as documented in the Validation Report [13]) in order to progressively refine and complete the SPR-INTEROP/OSED requirements (the link with the safety requirements for normal operational conditions has been explained in the previous sub-section).

5.3.3 Effects on Safety Nets

This is about checking that the Solution System operates in a way that does not have a negative effect on the operation of related ground-based and airborne safety nets.

The safety assessment concluded that PJ07-W2-38 does not introduce any new impact on any Safety Nets.

5.4 Safety Requirements at design level addressing Internal Functional System Failures

The purpose of this section is to present the Safety Requirements at Design level (SRD) addressing internal system failures derived following the **SAM-PSSA REF _Ref38284963 \r [6]** and **related SAF-GUI in STELLAR**.

Safety requirements at design level - SRD are derived from the SRS associated to failure conditions which have been identified in section 0.

The following Safety Requirements at Design Level (SRD) are to be included (derived from a top-down causal analysis of the Service Hazards identified in section 4.4.1, from a bottom-up failure modes and effects analysis encompassing the analysis of common causes and, if applicable, from the SRS (functionality & Performance) derived during the Service Hazard assessment section 4.4.1):

- SRD (functionality and performance): derived to provide adequate mitigations to reduce the likelihood that specific failures would propagate up to the service 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,

EUROPEAN PARTNERSHIP

Co-funded by the European Union

- If applicable, SRD (functionality and performance) derived to provide mitigation against service hazard effects (protective mitigation, from the SRS (functionality&performance) derived during the Service Hazard assessment.

It is necessary that any assumption, safety issue or operational limitation stated during the derivation of the SRDs addressing internal system failures are captured in Appendix B.

Note: The failure of elements that are external to the Solution functional system might be addressed as source of Abnormal conditions of operations.

5.4.1 Causal analysis

The purpose of the causal analysis is to develop the risk mitigation strategy through the identification of all possible causes of the service hazards. This way it will be possible to identify the corresponding Safety Requirements allowing to meet the SRSs of the Operational Hazard under consideration.

For each system-generated hazard (see section 4.4.1), a top-down identification of internal system failures that could cause the hazard was conducted.

This analysis has been conducted and recorded for each service hazard in a causal analysis-dedicated table. The causal analysis has been initiated from the failure modes already identified as causing operational hazards. The causes for operational hazards are included in the Column 1 of the causal analysis table.

Then, for each cause of service hazard failure, the origins have been identified in terms of which were the SPR-INTEROP/OSED requirements (derived by the Project) with potential for generating such failures. In case such a requirement were not satisfied, that would contribute to a service hazard (and consequently that requirement is in the SAFETY category i.e. it is a Safety Requirement-success approach that is also captured for being included in 0). The causes' origins, in terms of contributing SPR-INTEROP/OSED requirements, are included in the Column 2 of the causal analysis table.

Based on the understanding of the potential causes for the service hazard, the mitigations allowing to limit the occurrence of the cause or its propagation up to the occurrence of the service hazard have been identified from the existing set of SPR-INTEROP/OSED requirements. In case those mitigations were judged insufficient with regards to their efficiency, new mitigations have been defined and formalized as new safety requirements (proposed to be added to the existing set of SPR-INTEROP/OSED requirements).

All the mitigations identified (both the new and the already existing ones) have been consolidated in the table from sub-section 5.4.2.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

5.4.1.1 Hz 01: ATFM measures not designed or not implemented or implemented partially by NMf

Severity Class	SC-4b	*IM factor*	10
SRS	No more than 6e-5 per sector operational hour		

Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
Network operations (local) fails to identify and solve the imbalance	REQ-07.38-SPRINTEROP-OP01.0004 REQ-07.38-SPRINTEROP-OP01.0009	In case Network operations (local) does not solve the imbalance, it might be detected at NM level (but that is not systematic). Tactical conflict management.

Table 7 Causal Analysis for Hazard 01

5.4.1.2 Hz 02: Inadequate ATFM measure designed and implemented by NMf

Severity Class	SC-4b	*IM factor*	10
SRS	No more than 6e-5 per sector operational hour		

Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
Network Operations (local) fails to monitor hotspot resolution	REQ-07.38-SPRINTEROP-OP01.0009	In case Network operations (local) does not identify that hotspot resolution is no more valid, it might be detected at NM level (but that is not systematic). Tactical conflict management.

Table 8 Causal Analysis for Hazard 02

EUROPEAN PARTNERSHIP

Co-funded by the European Union

5.4.2 Safety Requirements at design level addressing internal system failures

This section derives the mitigations to reduce the likelihood that specific failures would propagate up to the Service Hazard (i.e., Service level) – these mitigations are then captured as additional Safety Requirements (Functional and Performance).

These requirements are derived considering the outcome of the causal analysis (see previous sub-section) and more particularly the mitigations identified in each table accompanying the hazard fault trees.

As outcome of the causal analysis, no additional mitigation needs to be derived compared to the ones already indicated in section 0.

5.5 Realism of the safe design

The development and safety analysis of the design would be seriously undermined if it were found in the subsequent Implementation phase that the Safety Requirements at Design Level were either not 'testable' or impossible to satisfy (i.e., not achievable) and / or that some of the assumptions were in fact incorrect.

5.5.1 Achievability of Safety Requirements at Design Level / Assumptions

All the requirements in this SAR have been identified in different meetings at project level, involving the different partners interested in the concept. The requirements have also been coordinated at project level such that to avoid duplications and/or contradictions with the OSED, HP and TS requirements.

The vast majority of the Safety Requirements have been demonstrated as capable of being satisfied in a typical implementation because they have been / will be exercised during validation exercises or because their achievability has been confirmed with subject matter experts during meetings or debriefing sessions.

5.5.2 "Testability" of Safety Requirements at Design Level

Most of the safety requirements are verifiable by direct means which could be by equipment and/or integrated system verification report, training certificate, published procedures, AIP information, etc.

For some safety requirements, verification should rely on appropriate assurance process to be implemented.

5.6 Process assurance for a Safe Design

A safety team encompassing concept experts, flow managers, Safety and Human Performance specialists have supported this safety assessment.

In addition to the activities conducted at Service level, safety requirements at design level have then been derived in normal, abnormal and failure conditions to satisfy the SRSs derived at Service level which are identified in Section **Error! Reference source not found.** of this document.

6 Demonstration of Service specification achievability

The safety-relevant validation results of the PJ07-W2-38 exercises (documented in the PJ07-W2-38 validation report VALR [13]) are summarized in **Error! Reference source not found.** below, whilst indicating for each SRS that has been covered the level of safety evidence that has been obtained.

Val Obj Id	Suc Crit Id	Success Criterion	Ex 01	Ex 02	Ex 03	Ex 04	Validation Results	Validation Objective Status
OBJ-PJ07W238-V3-VALP-K18 Safety Performance Assessment for AUO-0219	CRT-PJ07W238-V3-VALP-K18-001	The enriched DCB information exchange does not increase the level of saturation of regulated TVs.	OK	OK	-	N/A	The answers from exercise participants and the quantitative data on occupancy counts reflect that the change in saturation of regulated TVs is not identified as a problem.	OK
	CRT-PJ07W238-V3-VALP-K18-002	The enriched DCB information exchange does not negatively impact the timely detection of overloads and/or definition of a hotspot.	-	OK	-	N/A	Exercise participants did not detect any impact on the traffic demand.	
	CRT-PJ07W238-V3-VALP-K18-003	The positive treatment of enriched DCB information exchange does not have a negative impact onloading other TVs	-	OK	-	N/A	No over-demand due to rerouting was detected by the participants.	
	CRT-PJ07W238-V3-VALP-T11-003	Enriched DCB information and What-if function have been integrated in one AU System (at least).	-	-	-	OK	Enriched DCB information and What-if function have been integrated in AU Systems (DASSAULT and NAVBLUE)	
	CRT-PJ07W238-V3-VALP-T11-004	Enriched DCB information have been integrated in one FMP System (at least).	-	-	-	OK	Enriched DCB information and What-if function have been integrated in FMP Systems (THALES)	
OBJ-PJ07W238-V3-VALP-K26 Safety Performance Assessment for AUO-0208	CRT-PJ07W238-V3-VALP-K26-001	The treatment of Pro-active FDCI requests does not negatively impact the hotspot resolution.	-	-	OK	OK	The NMF considered that they can manage the protection hotspot area containing the P-FDCI flights.	OK
	CRT-PJ07W238-V3-VALP-K26-002	The treatment of Pro-active FDCI requests does not increase the level of saturation of regulated TVs.	-	-	OK	OK	The NMF considers that the P-FDCI request do not increase the level of saturation of the regulated traffic volumes.	

Table 9 PJ07-W2-38 exercises safety validation objectives, success criteria & Validation results

7 Acronyms and Terminology

Acronym	Definition
4DT	Four Dimensional Trajectory
ACARS	Aircraft Communication Addressing and Reporting System
AFTN	Aeronautical Fixed Telecommunication Network
AIP	Aeronautical Information Publication
AIRAC	Aeronautical Information Regulation And Control
AIS	Aeronautical Information Services
ANSP	Air Navigation Service Provider
AOWIR	Aircraft Operator What-If-Reroute
ASM	Airspace Management
ASP	Air Service Provider
ATFCM	Air Traffic Flow and Capacity Management
ATFM	Air Traffic Flow Management
ATM	Air Traffic Management
ATMRPP	Air Traffic Management Requirements and Performance Panel
ATS	Air Traffic Service
AU	Airspace User
AUP	Airspace Use Plan
AWACS	Airborne Warning and Control System
BA	Business Aviation
CACD	Central Airspace and Capacity Database
CDL	Configuration Deviation List
CDM	Collaborative Decision Making
CDR	Conditional Route
CFSP	Computerised flight plan service provider

EUROPEAN PARTNERSHIP

Co-funded by the European Union

CLI	Congestion Level Indicator
CNS	Communication Navigation and Surveillance
CONOPS	Concept of Operations
CR	Change Request
CTOT	Calculated Take-Off Time
DCB	Demand Capacity Balance
DCT	Direct Routing
eASP	Air Service Provider that is equipped for conducting FF-ICE procedures or interoperability
EATMA	European ATM Architecture
E-ATMS	European Air Traffic Management System
EAUP	European Airspace Use Plan
EET	Estimated Elapsed Time
EUROCAE	European Organisation for Civil Aviation Equipment
EUUP	European Updated Airspace Use Plan
ECAC	European Civil Aviation Conference
eFPL	FF-ICE FPL
EOBT	Estimated Off-Block Time
ETDO	Extended diversion time operations
ETFMS	Enhanced Tactical Flow Management System
ETOPS	Extended range Twin engine Operational Performance Standards
FDCI	Flight Delay Criticality Indicator
FF-ICE	Flight & Flow Information for a Collaborative Environment
FL	Flight Level
FLS	Flight Suspension message
FMP	Flow Management Position
FOC	Flight Operation Centre (also known as “OCC”)
FTM	Flight Time for MET validity

EUROPEAN PARTNERSHIP

Co-funded by the European Union

FUA	Flexible Use of Airspace
GA	General Aviation
GRIB	GRIdded Binary / General Regularly distributed Information in Binary form
HP	Human Performance
Hz	Hazard
HAZID	Hazard Identification
HPAR	Human Performance Assessment Report
ICAO	International Civil Aviation Organization
INTEROP	Interoperability Requirements
KPA	Key Performance Area
LoA	Letter of Agreement
LTM	Local Traffic Manager
MEL	Minimum Equipment List
METAR	METeorological Aerodrome or Aeronautical Report
MTFoO	Max Tolerable Frequency of Occurrence
NM	Network Manager
NMF	Network Management Function
NO	Network Operations (Regional or Local)
NOP	Network Operations Plan
NOTAM	Notice To Airmen
OCC	Operations Control Centre (also named in this document “FOC”)
OI	Operational Improvement
OPAR	Operational Performance Assessment Report
OSED	Operational Service and Environment Definition
PAR	Performance Assessment Report
P-FDCI	Proactive Flight Delay Criticality Indicator
PFP	Preliminary Flight Plan

EUROPEAN PARTNERSHIP

Co-funded by the European Union

PIRM	Programme Information Reference Model
PSSA	Preliminary System Safety Assessment
PTRs	Profile Tuning Restriction
QoS	Quality of Service
R&D	Research and Development
RAD	Route Availability Document
RBT	Reference Business Trajectory
R-FDCI	Reactive Flight Delay Criticality Indicator
RNAV	Area Navigation
RPAS	Remotely Piloted Aircraft Systems
RSA	Restricted Airspace
SAC	Safety Criteria
SAR	Safety Assessment Report
SBT	Shared Business Trajectory
SecAR	Security Assessment Report
SESAR	Single European Sky ATM Research Programme
SID	Standard Instrument Departure
SIIU	Safety Implication of the Intended Use
SITA	Société Internationale de Télécommunications Aéronautiques
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SPR	Safety and Performance Requirements
SRD	Safety Requirement at Design Level
SRS	Safety Requirement at Service Level
SRM	Safety Reference Material
STAM	Short-Term ATFCM Measures
STARS	Surveillance and Tracking Attack Radar System
SWIM	System Wide Information Model

EUROPEAN PARTNERSHIP

Co-funded by the European Union

TAF	Terminal Aerodrome Forecast
TBO	Trajectory Based Operations
TS	Technical Specifications
TV	Traffic Volume
UAS	Unmanned Aircraft Systems
UTC	Coordinated Universal Time
UUP	Update Airspace Use Plan
WAFC	World Area Forecast Centre

Table 10: Acronyms

Term	Definition
AIR-REPORT	A report from an aircraft in flight prepared in conformity with requirements for position, and operational and/or meteorological reporting.
ASP	A unit involved in performing air traffic management responsibilities introduced in the PANS-ATM (Doc 4444).
Airspace Constraints	ATM Constraints resulting from Strategic ATFCM Activities, that organize the traffic into traffic flows to make the best use of available capacity; the routeing organization is defined by a list of restrictions on specific points, ATS route segments, DCT segments or sectors in both the upper and lower airspace. They can be static or dynamic. Static are constraints that NMF can no longer resolve within the framework of the extended FF-ICE Planning Service process; while dynamic are constraints that NMF can resolve within the framework of the extended Planning Service process.
ATC Unit	An ATC Unit is a unit responsible for providing ATC (Air Traffic Control) services (Aerodrome Tower, Approach, Area Control Centre)
ATM Constraint	ATM Constraint is a condition that restricts the use of the airspace and limits the individual AU, Airport and ANSP in its most optimal operation with the purpose to optimize the operations on a network level (regional, sub-regional and local level)
DCB Constraints	ATM Constraints originating from Demand Capacity Balancing (DCB) that impact a trajectory. Example of DCB Constraints: ATFM regulations, Scenarios and STAM applied to a flight
DCB Trajectory Measure	A trajectory change notified to an AU for a flight due to DCB Constraints. Example: CTOT or Target Time (TT), re-routing or level capping imposed in the context of Scenarios or STAMs

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Enriched DCB information	In addition to DCB Constraints and DCB Trajectory Measures, information provided to the AU to give awareness of DCB information along the trajectory. This includes hotspot information (resolution and protection) and traffic volume load.
eASP	The symbol used to designate an ASP that is capable of receiving and responding to FF-ICE Messages, as required.
FDCI	FDCI is a parameter provided by the Airspace User to indicate the importance for the flight to progress on time.
Filed Flight Plan (FPL or eFPL)	The flight plan including any associated updates as filed by the pilot, an operator or a designated representative for use by air traffic services units. It is often referred to as an ATS flight plan.
Filing Status	The expected operational acceptability for a submitted Filed Flight Plan.
HotSpot	A local demand/capacity imbalance on the day of operations, which may result from a complex traffic situation or a short period of high demand. A hotspot is created to raise awareness of the situation and may act as a precursor to solving the imbalance (STAM or ATFM regulation).
Infringer flights (Protection Hotspot)	If a re-filing flight on loads a protection hotspot, the flight will be considered as a protection hotspot infringer.
Network Management Function (NMF) / Network Operations (NO) (Regional or Local)	This document contains both acronyms, NMF and NO. According to the EATMA information, the difference between both lies in the answer to the following questions. • Who is doing what: Network Operations (Regional or Local) • What is being dome: Network Management Function
Planning Status	The expected operational acceptability and applicable constraints for a submitted Preliminary Flight Plan
Preliminary Flight Plan	The flight plan submitted by an operator or a designated representative to conduct collaborative planning of a flight, prior to filing a flight plan for use by ATS units.
Pro-active FDCI	Pro-active FDCI: issued for really critical flights, with no reported delay yet and before any DCB measure is allocated to the flight. The intention is that NMF consider this information before implementing any measure.
Protection Hotspot	Hotspot associated to a traffic volume usually close to saturation to protect an airspace from undesired rerouted flights and prevents the application of DCB measures (e.g. ATFCM regulation, cherry picking measures). This is a new kind of hotspot. In the rest of this document, the term “protection hotspot” is used when referring to this specific type of hotspot

Provisional Delay	The indicative and non-final ATFCM delay incurred by a flight subject to a CASA regulation before the time at which the slot is issued 2 hours before EOBT. This delay may vary as a result of, for instance, slot revision which re-assigns the slots dynamically in function of the changing traffic demand
Short Term ATFCM Measures (STAM)	Specific and dedicated measures for demand capacity balancing (DCB) applied to a limited number of targeted airborne and/or pre-departure flights or flows reducing the complexity and/or demand of anticipated/ identified local traffic peaks on the day of operations
Simple Preferences	Simple preferences is information provided by the Airspace User to NMF to indicate the importance for the flight to progress on time (FDCI) or other indication as for instance flight level preferences.
Slot Issue Time (SIT1)	The time at which the NM issues the SAM to the AO and ATC at the aerodrome of departure.
Scenarios	Scenarios are an ATFCM solution to Network capacity bottlenecks or specific operational needs of an ANSP.
Unplanned flights	It is a flight that after submitting the eFPL or change the eFPL increases or decreases the traffic load of the TV (less than 2 hours before EOBT of the eFPL, for which the change is occurred due to FPL, CHG or refile).
What-if	When the DCB measures affect the AU operations, the AU looks at alternative trajectories based on their operational route library, selects one or several options to avoid the DCB measures and ask to analyse the DCB impact on the alternative trajectories. The alternative trajectory might avoid crossing hotspots that could result in double penalization such as re-routing and the increased severity of the hotspot due to new traffic load. By using a tool such as the What-if reroute (AOWIR) permits the operator to find alternative routes. The tool enables the operator to identify if there is a regulation impacting the alternative route and provides associated delay in that case but does not give the existence and severity of other hotspots along the alternative route that could potentially impact the operators and generate more instability in the Network if operators are not aware about congestion information.
What-else	When the DCB measures affect the AU operations, the AU asks for alternative trajectory options to NMF in order to avoid the DCB measures, and analyses the DCB impact of the alternative trajectories provided by NMF. The alternative trajectory will avoid crossing hotspots that could result in double penalization (the rerouting and the increased severity of the hotspot due to new unexpected traffic load).

Table 11: Glossary of terms

EUROPEAN PARTNERSHIP

Co-funded by the European Union

8 References

Safety

[1] SESAR 2020 Safety Policy

[2] SESAR Safety Reference Material - latest edition accessible in STELLAR Program Library

[3] Guidance to Apply SESAR Safety Reference Material - latest edition accessible in STELLAR Program Library

[4] STELLAR Slideboard, Safety part (complementary guidance)

[5] (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)

[6] SAM EUROCONTROL Safety Assessment Methodology V2.1 (https://www.eurocontrol.int/tool/safety-assessment-methodology)

[7] SESAR Solution PJ07-01 SPR-INTEROP/OSED for V2 - Part II - Safety Assessment Report, Edition 00.01.01, 26/09/2019

[8] SESAR Solution PJ09 SPR-INTEROP/OSED for V2 - Part II - Safety Assessment Report, Edition 00.01.00, 10/09/2019

Other documents

[9] PJ19-W2 Validation Targets Wave 2, Edition 00.01.00, 30 June 2020

[10] SESAR Solution PJ07-W2-38 SPR-INTEROP/OSED for V3 - Part I - Edition 00.00.02, 01/10/2022

[11] SESAR Solution PJ07-W2-40 Validation Plan (VALP) for V3 - Part I – Edition 00.02.00, 04/05/22

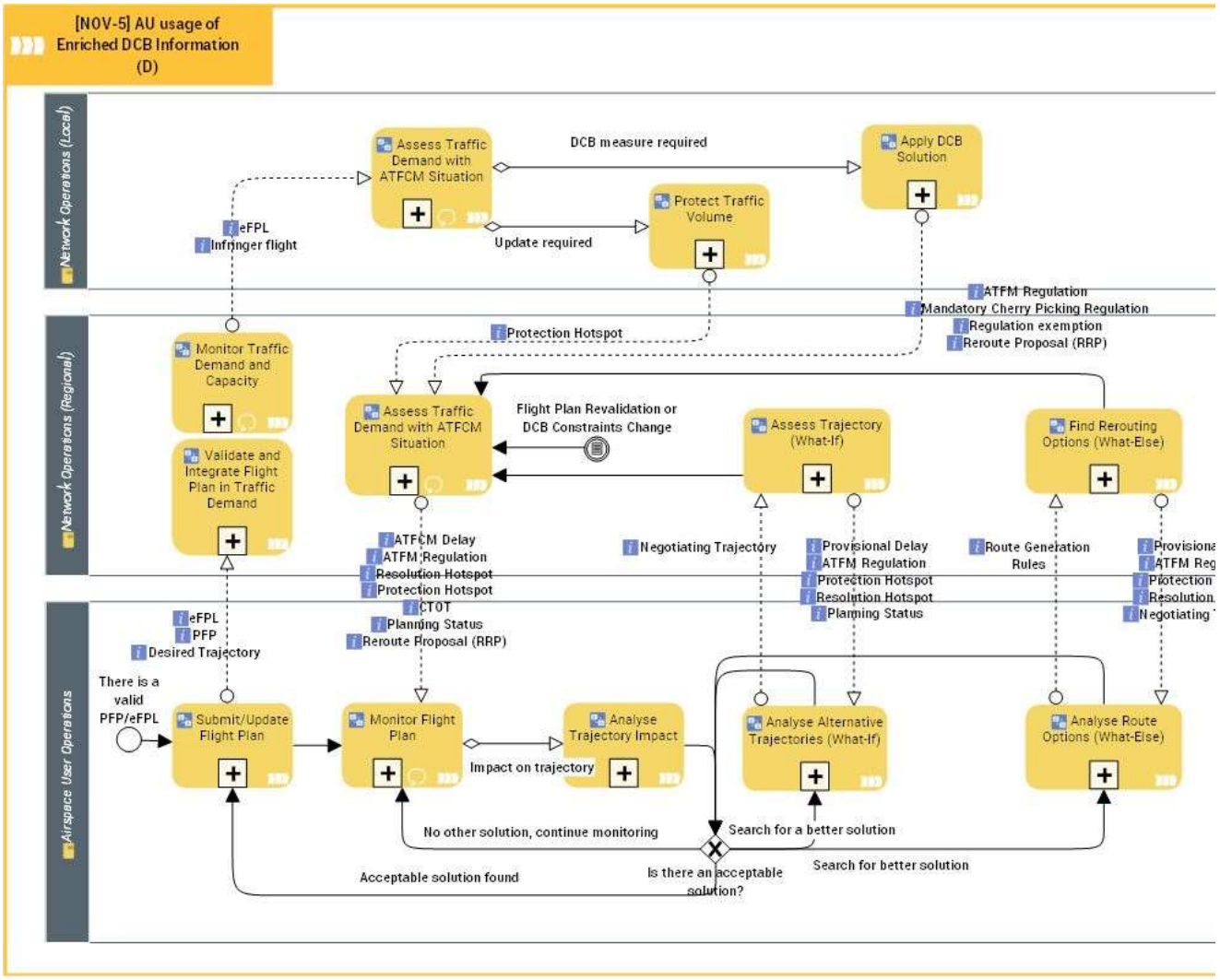
[12] NM Flow and capacity management service specification – EUROCONTROL, Ed. 1.0, 24th September 2020

[13] SESAR Solution PJ07-W2-38 Validation Report (VALR) – Edition 00.00.04, 25/10/2022

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix A EATMA Models



EUROPEAN PARTNERSHIP
Co-funded by the European Union

Appendix B Assumptions, Safety Issues & Limitations

B.1 Assumptions log

Ref	Assumption	Validation
A001		
A002		

Table 12: Assumptions log

B.2 Safety Issues log

Ref	Safety issue	Resolution
I001		
I002		

Table 13: Safety Issues log

B.3 Operational Limitations log

Ref	Operational Limitations
L001	
L002	

Table 14: Operational Limitations log

-END OF DOCUMENT-

Insert project logo here

Insert beneficiary's logos below, if required and remove this sentence

EUROPEAN PARTNERSHIP

Co-funded by the European Union