SESAR Solution 39 SPR-INTEROP/OSED for V3 - Part II - Safety Assessment Report

Deliverable ID:	D3.1.008
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:	09 February 2023
Edition:	00.01.00
Template Edition:	00.00.03

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Authoring & Approval

Authors of the document

Beneficiary	Date
EUROCONTROL	09/02/2023

Reviewers internal to the project

Beneficiary	Date
SKYGUIDE	03/02/2023
SWISS INTERNATIONAL AIRLINES	06/02/2023
ENAIRE/CRIDA	03/02/2023
THALES	03/02/2023
AIRBUS	03/02/2023
METRON AVIATION	03/02/2023
AIR FRANCE	03/02/2023
DSNA	03/02/2023

Reviewers external to the project

Beneficiary	Date

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

Beneficiary	Date
EUROCONTROL	

Rejected By - Representatives of beneficiaries involved in the project

Beneficiary	Date

Document History

Edition	Date	Status	Beneficiary	Justification
00.00.01	16/12/2022	Initial draft	EUROCONTROL	Initiation of the document
00.00.02	24/01/2023	Final draft	EUROCONTROL	Final draft including VALR inputs for solution review
00.01.00	09/02/2023	Final	EUROCONTROL	Version for submission to SJU after internal review

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 39 "Collaborative framework for managing arrival delay within an ATFM regulation".

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.

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This document contains the Specimen Safety Assessment for a typical application of the PJ07-W2 Solution 39 "Collaborative framework for managing arrival delay within an ATFM regulation". 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-W2-39 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 project PJ07-02 in SESAR2020 Wave 1, contained in the corresponding SAR [7]. The current version of the document contains updates with the work done for the PJ07-W2-39 concept in SESAR 2020 Wave 2.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

2 Introduction

2.1 Background

Solution PJ07-W2-39 validation builds upon the results delivered by:

SESAR 1

- SESAR 1 Solution #18 "CTOT and TTA" validated the concept of Target Time Management in the planning phase from a Network perspective for arrival traffic allowing provision for AU interactions
- SESAR 1 Solutions #20 "Initial Collaborative Network Operations Plan (NOP)" and #21 "Airport operations plan (AOP) and its seamless integration with the network operations plan (NOP)", validated the process for local DCB actors to collaborate with the Network in the TTA allocation process

and SESAR 2020 Wave1

- PJ.07-02 "User Driven Prioritisation Process (UDPP)", validating at V2 level the UDPP concept
- Wave 1 PJ24 VLD (Very Large Demonstration) Exercises at Barcelona, Palma de Majorca and Heathrow Airports addressed the hotspot resolution (Local DCB issues) based on TTAs (Target Times of Arrival) proposed for arriving flights (in pre-flight phase) by local DCB tools and applying local business/operational rules. The TTs were defined at local (Airport) level and shared with the Network Manager via the AOP connected to the NOP. Some limited provision was defined for AU integration, but an active AU participation as described within UDPP concept was not integrated in the local processes
- Wave 1 PJ25 shadow mode Exercise at Zurich Airport addressed the hotspot resolution through the local (FMP and AU) management of arrival regulations, for building an optimized sequence based on airlines' priorities. A limited part of UDPP was integrated in the local process

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-W2-39 focuses on the definition of a collaborative framework for managing arrival constraints for Local DCB issues managed at FMP or Airport level, in collaboration with Network Function, and with the participation of Airspace Users (AUs). 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 to AU and ANSPs prior to the execution phase.

2.3 Scope of the Safety Assessment

The PJ.07-W2-39 safety assessment makes extensive use of outcomes from previous PJ07.02 SAR [7].

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 [8]),
- 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).

Initially, PJ07-W2-39 planned to address the following Operation Improvements (OIs):

- AUO 0109: Collaborative framework for managing arrival constraints at Airport
- AUO-0110: Collaborative framework for managing arrival constraints at Local DCB level

However, OI Step AUO-0109, originally associated with Solution 39 has been unlinked from the Solution on the grounds of insufficient maturity. Nevertheless, even if the AUO-0109 is no longer in the Solution, the analysis of AUO-0109 is still included in this report. The outcomes of this SAR exclusively related to this OI (if any) will be placed in a dedicated Appendix so as not to lose it.

The improvements brought by PJ07-W2-39 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

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

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.07-W2-39 SPR-INTEROP/OSED [10].

The Solution PJ.07-W2-39 aims to develop a collaborative framework that will enable the integration and necessary coordination of constraints (limited to arrivals management) from various stakeholders (Airports, ANSPs, AUs and NM). This would ensure the continued stability and performance of the network and would give the opportunity to the Airspace Users to prioritize their flights, thereby reducing the impact of the delays generated by the ATFM planning constraints to limit the excess costs on their operations. In this case, AUs might contribute to a DCB solution such that their operational performance interests are best served.

Its main objective is to define and validate a Collaborative framework for the coordination and collaboration between different ATFM processes (including the so-called User Driven Prioritisation Process - UDPP), dealing with delay constraints on arrivals (considered the most important contributor to Capacity performance issues).

Collaborative framework for managing delay on arrivals

The new operating method builds on existing ones for resolving capacity constraint situations and incorporates additional features:

- Collaborative resolution of the CCS: all key stakeholders are involved in the resolution of DCB imbalance problem on arrivals to an ADES.
- Integration of UDPP into the CCS resolution process: the central part of resolving the DCB imbalance problem on arrivals at ADES is the inclusion and consideration of AU priorities in the process.

The UDPP mechanisms have been validated in SESAR2020 Wave 1 (up to V2), and as such they are part of the concept and new operating method. The concept introduced herein covers the wider operational aspects of new or enhanced methods, enabled by the use of UDPP mechanisms or their components, for resolving DCB imbalance problems on arrivals.

The principal objective of the UDPP solution is to integrate the AUs' needs into the ATM system solution, especially when delays occur, to decrease the impact of delay on the AUs fleet, through the submission of the priority order and sharing preferences with the other ATM stakeholders in CCS. For achieving that, UDPP allows to transfer the resolution of a congested situation from the owner of the resource (for example, the FMP dealing with arrival flights) to the user of the resource (for example, the airlines).

The concept acts on flights which are part of a DCB imbalance solution and which are still in pre-flight stage (i.e. pre off-block at ADEP).

The UDPP service produces an initial solution based on CASA regulation. Afterwards, the solution is updated taking into account the AUs' priorities (Selective Flight Protection (SFP), Fleet Delay Reordering (FDR) and Margins):

- **FDR: Fleet Delay Reordering**

  FDR feature is based on the extension of slot swapping. According to the slot assigned to each flight of an AU, FDR gives the possibility for the AU to assign its own list of flights for each slot. In particular, the flight the AU is interested to decrease the impact of the delay on its fleet can be swapped with another flight from its fleet. For this, the AU can put a priority value on each flight to be reordered accordingly. FDR priority values can be set to a priority number (from 1-highest priority to 999 -lowest priority) or a specific value ("L" -Lowest priority, "B" -Baseline priority or S" to suspend a flight i.e. it is a candidate to avoid the hotspot or to be cancelled later on).

- **SFP: Selective Flight Protection**

  The SFP feature makes use of the specific priority value "P" (protect) to give to the AU the possibility to protect the schedule of a flight (Pflight) even if there is no direct slot allocated to it. To do so, the AU must have at least one slot before the original schedule of the protected flight (within a window called the Pobjective) in order to not negatively affect other AUs by its action.

  If an AU places a P on a flight, the UDPP algorithm will first try to find an AU slot within the Pobjective time window. If no slot is available in the time window Pobjective, the algorithm finds the first available slot prior to the flight's schedule. When a slot is found, the AU's flight with this current slot is swapped to the actual slot of the Pflight and the Pflight is allocated to its new slot closer to the original schedule.

- **Margins**

  Margins on flights provide the AU the possibility to express time constraints on flights directly by times values. Margins on flights can be given by two values:

  - Margin not after: specifies a time for the flight that cannot be later than the given value
  - Margin not before: specifies a time for the flight that cannot be earlier than the given value.

  The objective of the algorithm is to rearrange flights automatically according to these time constraints using the AU's own slots (like FDR but not on Priority values but on time).

  If margins are defined for a specific Pflight, the margins replace the time value of the Pobjective.

The DCB imbalance detection at an Airport triggers the creation of a UDPP measure through the definition of the CCS in coordination with NM.

In some cases, when the DCB imbalance has low impact on traffic, the Airport can trigger a UDPP Network Cherry-Pick measure to involve AUs, through the UDPP prioritisation. The creation of this UDPP NCP measure allows to integrate AU flights constraint (prioritisation) given by AUs, on local solution

The central part of the framework is the NM system managing constraints and delay over the Network and maintaining a coherent and up-to-date situation for all the actors.

The UDPP service, part of the NM system, receives and processes the UDPP prioritisation inputs from AUs to produce a solution to the DCB imbalance problem (taking into account AUs' prioritisation).

UDPP service envisaged as a part of the CASA function, uses NM data and AU prioritisation and continuously re-computes the slot based on the UDPP inputs received from the AUs at any given moment in time (asynchronous AU prioritisation). In case of Network Cherry-Pick measure (UC2) no automatic update and calculation is done by NM and the local DCB actor is responsible of maintaining the measure and its content.

On the AU side, a key interaction supported by a "What-if" facility available to the AUs offers to the AU the possibility to test a set of flight prioritisation for his flights, without formally submitting these inputs to NM service for publication. An AU can choose to run a What-if assessment on its flights with prioritisation and subsequently choose not to "Submit" this set of UDPP inputs. An AU becomes an "AU participating in the UDPP process" only if a formal Submit of UDPP inputs to the UDPP service is made by the AU, otherwise the AU is classed as a non-participating AU. It is expected that in practice any UDPP measure will involve a mix of participating and non-participating AUs.

It should be noted that the impact assessment given to AUs when prioritizing flights through the UDPP service, is supported by the NM system (based on the Network status) integrating AOP data through the AOP/NOP integration capability when available. The AOP/NOP integration is supported by the NM actor and it is developed in coordination with the Airport actors.

Collaborative framework for managing arrival constraints

The increasing need to optimise the traffic flow at airports, taking into account the different stakeholders requirements, produces to a greater extent the implementation of local DCB measures adapted to specific circumstances.

As the UDPP process is related to the current NM flight management, it is proposed that UDPP becomes an NM service to optimise an existing DCB solution, considering the AUs prioritisation for their affected flights. In this case, the local DCB and the airport tools managing flights work in close relation with NM, using and updating the flight times in a coordinated manner. The flight times are always available and published by NM.

Local DCB will detect and set the adequate measure to manage an overload situation. If a UDPP approach is decided to allow AUs to mitigate the impact of the solution, the local DCB will invoke the UDPP as a service, to elicit AUs' input for reordering their flights. Once the cut-off time is reached, local DCB will optimize the result of the UDPP process by monitoring/keeping control of the final overall reordering process in a safely manner while trying to accommodate the AUs' needs as much as possible.

UDPP integration with FDCI

According to the FDCI definition, in some situations UDPP and FDCI will cohabitate.

The figure below shows the time line for P-FDCI and R-FDCI:

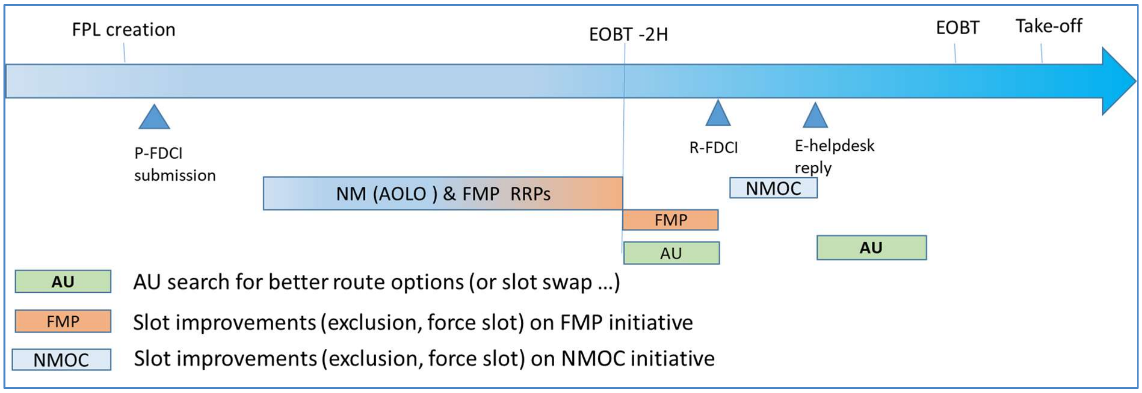


Figure 1: P-FDCI and R-FDCI on time line

A flight which declared P-FDCI and caught by a UDPP regulation will follow the process:

1. Until SIT1 (typically EOBT-2h) NM and FMP will try to avoid affecting that flight with DCB measures.
2. If the flight is affected by a UDPP regulation and the delay is greater than the P-FDCI tolerance, before declaring R-FDCI, the AU can benefit from UDPP following the AU preferred option:
    a. Follow the usual UDPP process in place as the rest of flights and declare the preferences.
    b. Automatically translate the P-FDCI time tolerance into UDPP margins ("Time Not After") and generate the UDPP preferences. As p-FDCI does not include an equivalent to "Time Not Before" it will be allocated to 0 in this particular option.
3. AU acceptance for UDPP solution.
4. If UDPP do not mitigate the delay, AU can declare R-FDCI through NM helpdesk.

In the above step 2, the option b have the advantage of reducing the AU workload by introducing the UDPP solution as part of the P-FDCI and UDPP potential automated actions.

P-FDCI can provide a simple mean for certain categories of AUs to be involved in UDPP.

As already mentioned, in case of UDPP regulation the transition between P-FDCI and R-FDCI will pass through the UDPP process before eventually need to declare R-FDCI.

In typical situations leading to UDPP there would be very few opportunities for NM helpdesk to find solutions for R-FDCI flights, then the transit from P-FDCI to UDPP could be one of the best opportunities to mitigate the delay for such flights.

3.2 Solution Operational Environment and Key Properties

The majority of the functions described in the PJ07-W2-39 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 airports, even though the validation exercise will focus on large and very large airports in the European Civil Aviation Conference (ECAC) area that regularly experiences delay. The solution includes all ECAC airports to look at the network impact.

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 flights operations within the ECAC area.

3.2.3 Ground ATM/ATFCM capabilities

The ground ATM capabilities outside scope of but relevant for PJ07-W2-39:

- NOP functionality
- SWIM matured as per SESAR 2020 (enabling Ground-ground interconnection)

3.2.4 Airports & AU Capabilities

Airport capabilities outside scope of but relevant for PJ07- W2-39:

- AOP system integrated with NOP
- AU capabilities: Note that regarding the FOC system necessary adaptations for managing preference& priorities 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 [12], the solution expects to have a positive impact on the Airspace Users, by improving (not limited to):

- 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, by a better integration of AUs' wishes effect in airport planning (AOP) and Network planning (NOP) activities.
- 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.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

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-W2-38 have been identified.

3.4.2 Other intended use outside-SESAR

Currently, all the ANSPs in Europe make 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-W2.39 does not aim to modify the service provided per se, but to introduce a new way of solving DCB imbalances while taking into account the AU needs.

3.5 Relevant applicable standards

Current NM ATFCM standards and regulations are applicable for this solution.

3.6 Safety Driver

Based on the SESAR2020 SRM guidance update, in order to address the change introduced by PJ07-W2-39 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' [15].

More specifically, the solution impacts the *Demand – capacity balancing* service component, whose main functions are:

- ATFCM measure design
- ATFCM measure promulgation
- ATFCM measure implementation
- Network cherry-pick regulations

The purpose of the *Demand – capacity balancing* is to react when the predicted traffic demand is higher than the available capacity by considering, assessing and implementing adequate solutions - ATFCM measures.

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).

In addition, it is necessary to take into account for the definition of the Safety Drivers the Safety Issue recorded in the SAR for SESAR2020 Wave 1 PJ07-02 [7]:

ID	Description
I001	Impact of several UDPP measures implemented simultaneously at Network level remains to be analysed and tested

The rational for deriving this issue was the following:

'The solution introduces a more collaborative way of resolving a Hotspot. From a Safety point of view, it needs to be ensured that this new procedure solves the hotspot in an appropriate and timely manner, while not creating new hotspots in other sectors in a short notice or impacting the resolution of other existing hotspots as it might exist a risk for not completely resolving a hotspot on time'.

Based on these inputs, SIIUs were defined only on the services where it was identified that PJ07-W2-39 is introducing a change with potential safety impact.

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-W2.39 to the Short Term DCB 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 *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*):

SIIU001: The ATFCM measure design service delivered to ATS, service which is modified by PJ07-W2.39 with the AUs inputs and new functionalities (e.g. What-if/What-else) shall not increase the number of overloads.

SIIU002: The ATFCM measure implementation service delivered to ATS, service which is modified by PJ07-W2.39, shall not increase the number of overloads.

SIIU003: The Network cherry-pick regulations service delivered to ATS, service which is modified by PJ07-W2.39 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 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 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-W2-39 SPR-INTEROP/OSED [10].

- Use Case 1: UDPP measure based on ATFM regulation
- Use Case 2: UDPP measure based on ATFM NCP measure (TTAs allocation)
- Use Case 2b: Use Case 1: UDPP measure based on ATFM regulation and TTAs allocation

Note: Use Cases 2 and 2b have been kept out of the final SPR-INTEROP/OSED due to lack of maturity. Nevertheless, all the work carried out in this SAR for these Use Cases is kept in the document in case the Use Cases are continued in the future.

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.

ID	Safety Requirement at Service level (SRS) *(success approach)*	Use Case	Related Safety Driver
SRS 001	NMf shall continue to appropriately design and apply the DCB solution	UC1 UC2 & 2 bis	SIIU001 SIIU002 SIIU003
SRS 002	NMf shall continue to appropriately verify the resolution of potential overloads in a timely manner	UC1 UC2 & 2 bis	SIIU002 SIIU003
SRS 003	The implementation of several co-existing UDPP measures at ECAC level shall not negatively impact the stability of the Network	UC1 UC2 & 2 bis	SIIU002 SIIU003

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

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 PJ07-02 safety assessment [7]:

- ABN1. Unforeseen airspace closure (e.g. Volcanic Ash, nuclear cloud …)
- ABN2. Sudden change in weather conditions
- ABN3. Severe weather conditions (CBs, turbulences, icing)
- ABN4. Unplanned Airport closure
- ABN5. Unplanned limitation in capacity (ATC ground system failures, unforeseen sector closure/regrouping)
- ABN6. Degradations of NM system (IFPS)
- ABN7. Industrial actions, e.g. strikes

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-W2-39 was identified) additional mitigation means might be specified in terms of new SRSs.

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SRSXXX]
ABN1	Unforeseen airspace closure (e.g. Volcanic Ash, nuclear cloud …)	In case of UDPP already implemented, source of new hotspots that might turn the existing UDPP measures insufficient or inefficient.	Short term: None (ATC deals with the imbalance in the affected sectors) Longer term: Restrictive regulation. Possibility for applying UDPP measures
ABN2	Sudden change in weather conditions	In case of UDPP already implemented, worsening of local meteorological conditions in the short-term that may be source of new hotspots, turning existing UDPP measures insufficient or inefficient.	In case of significant hotspot evolution (e.g. due to sudden change in weather conditions), new DCB measures shall be implemented, whenever applicable. If necessary, manage the problem tactically and/or apply restrictive regulation. Possibility for applying UDPP measures
ABN3	Severe weather conditions (e.g. CBs, turbulences, icing)	Specific conditions are developing locally which require adopting and coordinating a planned “axis management” scenario implementation with special and possibly earlier scenario activation. This abnormal condition might be one of the reasons for applying UDPP	NMf actors (Regional and Local) will adopt and coordinate a planned “axis management” scenario implementation. Possibility for applying UDPP measures
ABN4	Unplanned Airport closure	Unplanned losses of capacity.	DCB measures need to be re-assessed and new measures implemented, whenever applicable

ABN5	Unplanned limitation in capacity (ATC ground system failures, unforeseen sector closure/regrouping)	In case of UDPP already implemented, source of unexpected hotspots due to capacity reduction, turning existing UDPP measure not effective anymore.	New DCB measures needs to be implemented, whenever applicable Restrictive regulation if needed Possibility for applying UDPP measures
ABN6	Degradation of NM system (IFPS)	Lost opportunity for the application of new UDPP measures	Tactical management
ABN7	Industrial actions, e.g. strikes	Pre-notified reduction in capacity due to sector closing/regrouping caused by decrease in ATCO availability.	Restrictive DCB measures Possibility for applying UDPP measures

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

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) and a HAZID (HAZard IDentification) workshop, involving relevant operational and technical experts has taken place.

The HAZID Workshop was held virtually on the 29th June 2021. Due to the low safety impact of the solution, no specific HAZID table was developed. Instead, more informal discussions took place with NM experts, FMP experts, concept experts and Airspace Users about the potential hazards. The outcomes have been included in the assessment below.

The analysis and safety discussions have been also 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].

Table 3 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).

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 001 SRS 002 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

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.

$$SRS_{102} = \frac{MTF \quad relevant\_severity\_class}{N \times IM} = \frac{1E-02}{100 \times 10} = 1E-05$$ [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, a HAZID Workshop and some informal meetings were held to address the specific change introduced by the PJ07-W2-39. These meetings were facilitated by SAF experts from EUROCONTROL and it included concept and validation experts but also Flow Managers.

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-W2-39 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.

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
- 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 Appendix A 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.

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

In the specific case of PJ07-W2-39 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) and related TS/IRS requirements 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 and TS/IRS requirements that have been identified in the SAFETY category have been further traced to the related operational hazards and ultimately consolidated in **Error! Reference source not found.** 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 and in the TS/IRS document.

Safety Requirement ID	Safety Requirement (functionality & performance) description	Related service hazard(s)
REQ-07-W2-39-SPRINTEROP-LDCB.001	Local DCB shall monitor the arrival traffic prediction in Airport, and shall have the possibility to set a UDPP measure	Hz 01
REQ-07-W2-39-SPRINTEROP-LDCB.003	Local DCB shall have the possibility to update or request to update a UDPP measure to manage the change of the constraint on arrival traffic at Airport in coordination with NM	Hz 02
REQ-07-W2-39-SPRINTEROP-LDCB.007	DCB shall have the possibility to optimize the new arrival time of flights by adjusting TTAs	Hz 02
REQ-07-W2-39-SPRINTEROP-NMUD.003	NM internal function shall manage the reference time, calculate the baseline time and cut-off time on each flight according to the current status of the flight, enabling AU prioritisation and the flight transition to Local DCB optimisation	Hz 01
REQ-07-W2-39-SPRINTEROP-NMUD.006	The UDPP functions shall create and maintain the AU UDPP environment to allow AUs prioritisation according to the possible variability of the Network	Hz 02

REQ-S39-TS-LDCB.0001	Local DCB tool can monitor the load and capacity of traffic volumes (En-route, Departure Airport, Arrival Airport)	Hz 01
REQ-S39-TS-LDCB.0002	Local DCB tool shall be able to manage a UDPP measure function (creation, read, update, delete)	Hz 02
REQ-S39-TS-NMUD.0003	The Regional ATFCM system shall maintain for each flight the UDPP cut-off time and prohibit any changes in priority past this time	Hz 01
REQ-S39-TS-NMUD.0006	The Regional ATFCM system shall update the slot allocation when the network evolves or at certain key milestones like SIT1 based on the latest flight prioritisations	Hz 02

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

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).

In addition, a specific Safety Validation Objective was included in the VALP in order to cover the potential impact on the network stability of several UDPPs applied at the same time, already captured through:

- a Safety Issue (*I001: Impact of several UDPP measures implemented simultaneously at Network level remains to be analysed and tested*) in PJ07.02 SAR [7] in Wave 1 and,
- also covered in this document through the *SRS003: "The implementation of several co-existing UDPP measures at ECAC level shall not negatively impact the stability of the Network"*.

Related to this, the outcome of the Fast-time simulation activity in RNEST (RNEST FTS), collected in the VALR [13] is the following:

"The FTS activity was also used to exploit the RNEST computational capability to derive Occupancy counts from the simulated environment and traffic, with the aim to measure the Network stability in the context of the use of UDPP. This is related to the safety validation objective formulated in Safety Assessment Plan of Solution 39.

The methodology used can be summarised as follows:

- *For each scenario based on AIRAC1909 as described in previously, the Occupancy counts were computed by RNEST. A single definition was used for all Traffic Volumes investigated: 10 minutes of window width and a 5-minute step. E.g. the first occupancy count covered 00:00 – 00:10Z, the following one 00:05-00:15Z etc.*

- *The OCs defined above were applied to simulated traffic and OC values were derived by RNEST for all Traffic Volumes (TFVs) contained within RNEST's database, for all simulated scenarios and for all dates within AIRAC1909.*
- *A selection of TFVs (all EB, ED, LF and EG TFVs, approx. 2600 TFV in total) with their OCs were exported and analysed as a time series of values: adjacent OCs were compared in order to derive the deltas from one OC to another.*
- *The progression of the OCs was summarised and compared across the scenarios, by using the mean absolute delta for a single OC series.*

A side-by-side comparison of the aggregated statistics for the simulated scenarios show that the Network stability is comparable in all Solution scenarios to the Reference scenario without UDPP interventions.

Scenario	Minimum	1st quartile	Median	Mean	3rd quartile	Max
Baseline	0	0.4112	1.0383	1.0628	1.4887	8.6969
Scenario A	0	0.4112	1.0418	1.0630	1.4913	8.7875
Scenario B	0	0.4112	1.0383	1.0626	1.4878	8.6934
Scenario C	0	0.4112	1.0418	1.0630	1.4913	8.7875

Table 6: Mean of absolute deltas of Occupancy Counts for FTS simulation scenarios

The statistics above were derived from the full set of Traffic Volume + Date + Simulation scenario combinations. The results confirm the expectations that the deployment of UDPP does not alter the Network stability significantly, and that the effects of UDPP interventions are typically masked by the normal variability present even in today's operations."

With this information, it can be concluded that the implementation of several UDPP measures at network level will not negatively impact the stability, thus will not impact safety.

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-W2-39 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 [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 4.4.

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,
- 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.

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 timely identify and solve the imbalance	REQ-07-W2-39-SPRINTEROP-LDCB.001 REQ-07-W2-39-SPRINTEROP-NMUD.003 REQ-S39-TS-LDCB.0001 REQ-S39-TS-NMUD.0003	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-W2-39-SPRINTEROP-LDCB.003 REQ-07-W2-39-SPRINTEROP-LDCB.007 REQ-07-W2-39-SPRINTEROP-NMUD.006 REQ-S39-TS-LDCB.0002 REQ-S39-TS-NMUD.0006	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

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-W2-39 exercises (documented in the PJ07-W2-39 validation report VALR [13]) are summarized in Table 9 below.

Val Obj Id	Suc Crit Id	Success Criterion	Validation Results	Validation Objective Status
OBJ-07-W2.39-V3-VALP-SA1 **Safety**	CRT-07-W2.39-V3-VALP-SA1-001	The collaborative framework has no effect on the identification of a CCS and/or definition of a hotspot.	The identification of the CCS is not compromised with the new concept.	OK
	CRT-07-W2.39-V3-VALP-SA1-002	The DCB imbalance resolution for the arrival CCS, measured through Entry counts, in Solution scenario is equivalent to the reference scenario.	Data shows that the entry counts in the target TFV in the Solution scenarios are equivalent to the Reference scenario entry counts.	
	CRT-07-W2.39-V3-VALP-SA1-003	The DCB imbalance resolution for an arrival CCS does not increase the number of overloads, measured through Occupancy counts, within the Network.	Data shows that the occupancy counts in the observed/monitored TFVs in the Solution scenarios are equivalent to the Reference scenario occupancy counts.	

Table 9 PJ07-W2-39 exercises safety validation objectives, success criteria & Validation results

7 Acronyms and Terminology

Acronym	Definition
4D	Four Dimensional
ACP	Airport Cherry-Pick
AIM	Accident Incident Model
AMAN	Arrival Manager
ANM	ATFCM Notification Message
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider
AOC	Airline Operations Centre
AOP	Airport Operational Plan
API	Arrival Planning Information (message)
APOC	Airport Operations Centre
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATFCM	Air Traffic Flow and Capacity Management
ATFM	Air Traffic Flow Management
ATM	Air Traffic Management
AU	Airspace User
B2B	Business-to-Business
CASA	Computer-Assisted Slot Allocation (Network Manager slot allocation for regulations)
CCS	Capacity Constraint Situation
CDG	Charles de Gaulle
CDM	Collaborative Decision Making
CNS	Communication Navigation and Surveillance
CONOPS	Concept of Operations

CR	Change Request
CTOT	Calculated Take Off Time
D0	Day ‘zero’, Day of Operation
D-1	Day ‘zero minus one’, Day before Operation
DCB	Demand Capacity Balancing
dDCB	Dynamic Demand Capacity Balancing
DMAN	Departure Manager
DPI	Departure Planning Information (message)
EATMA	European ATM Architecture
ECAC	European Civil Aviation Conference
e-FPL	Extended Flight Plan
EIBT	Estimated In Block Time
EOBT	Estimated Off Block Time
EXE	Exercise
F2F	Face-to-Face
FDCI	Flight Delay Criticality Indicator
FDR	Fleet Delay Reordering
FF-ICE	Flight and Flow Information for a Collaborative Environment
FHA	Functional Hazard Analysis
FIBT	Forecasted In Block Time
FMP	Flow Management Position
FOC	Flight Operations Centre
FSFS / FPFS	First Scheduled First Served / First Planned First Served
HAZID	Hazard IDentification
HMI	Human Machine Interface
HP	Human Performance
HPAR	Human Performance Assessment Report

INTEROP	Interoperability Requirements
IRS	Interface Requirement Specification
KPA	Key Performance Area
KPI	Key Performance Indicator
L-DCB	Local Demand Capacity Balancing
MAC	Mid-Air Collision Model (AIM)
MCP	Mandatory Cherry-Pick
MPC	Most Penalising Constraint
NCP	Network Cherry-Pick
NM	Network Management
NMF	Network Manager Function
NOP	Network Operations Plan/Portal
OBJ	Objective
OI	Operational Improvement
OSED	Operational Service and Environment Definition
PFP	Preliminary Flight Plan
PSSA	Preliminary System Safety Assessment
RNEST	Research Network Strategic Tool
RTS	Real Time Simulation
SAC	Safety Criteria
SAF	Safety
SAM	Safety Assessment Methodology
SAR	Safety Assessment Report
SESAR	Single European Sky ATM Research Programme
SFP	Selective Flight Protection
SIBT	Scheduled In Block Time (initial Airline schedule)
SJU	SESAR Joint Undertaking (Agency of the European Commission)

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SPR	Safety and Performance Requirements
SRD	Safety Requirement at Design Level
SRM	Safety Reference Material
SRS	Safety Requirement at Service Level
STAM	Short-Term ATFCM Measures
SWIM	System Wide Information Model
TS	Technical Specification
TT	Target Time
TTA	Target Time of Arrival
TTOT	Target Take-Off Time
UC	Use Case
UDPP	User Driven Prioritization Process
V1, V2…	Validation Maturity Levels
VALR/P	Validation Report/Plan

Table 10: Acronyms

Term	Definition
Air Navigation Service Provider (ANSP)	Organisation responsible for the provision of traffic control and information services at airports and en-route. It includes control of air traffic at and around a controlled airport as well as local flow management.
Airport Collaborative Decision Making (A-CDM)	Operational concept, which starts with information sharing, taking capacity related decisions in a collaborative manner on the day of operations (D-0). It aims at improving the overall efficiency of airport operations by optimising the use of resources, and improving the predictability of events. It focuses especially on aircraft turnaround and pre-departure sequencing processes by using A-CDM milestones.
Airport Operations Centre (APOC)	A coordination arrangement at an airport, whereby operational stakeholders (actors) collaborate for the effective/efficient establishment and execution of an agreed operational plan, in a structured manner with agreed processes, either through physical or virtual interaction or a combination thereof. The APOC is the prime interface between the Airport and the Network Manager Operations Centre (NMOC) established in the States within, and adjacent to, the ECAC area.

Arrival Optimisation period UDPP flight Cut-off Time	Arrival Optimisation period is the local Airport (the one creating the UDPP measure) arrival anticipation period, applicable on each flight of the UDPP measure used as part of the calculation of the UDPP flight cut-off time. The UDPP flight cut-off time specifies until when the AU can set priorities/Margins on their flight. Once the flight cut-off time has been reached, the last prioritisation submitted by the AU on this flight is taken as the "final UDPP prioritisation" to elaborate the UDPP solution. UDPP flight cut-off time = COBT – TRS@ADEP – TRS@ADES TRS@ADEP: Time To Remove a flight from Sequence on departure airport (already existing in NM). TRS@ADES: Time To Remove a flight from Sequence on arrival airport (doesn't currently exist in NM). The TRS@ADES represents the Arrival Optimisation Period. The Arrival Optimisation period is defined when the "UDPP Measure" is initiated.
Airspace User (AU)	Civilian airspace users include scheduled airlines, charter companies, cargo and air freight service providers, the business and leisure aviation sectors and all forms of non-military air travel.
Baseline delay, Baseline Time	Represents the allocated delay to each flight in a constrained situation before or without the incorporation of AU constraints into the CCS resolution. It is used as a baseline of the equity in the CCS resolution and can be used to benchmark the concept to identify the concept's benefits.
Capacity Constrained Situation (CCS)	A period of time in which the Capacity of an ATFM element (Airspace, Arrival Runway, Departure Runway …) has to be controlled in relation to the demand (reduction of capacity, overload situation …) . The Capacity Constrained Situation defines the capacity as a constraint to be respected and associated with a time window to apply it (or a group of time windows, in which case the capacity constraints define the sub-periods).
Delay-Cost Curve	The function expressing the relationship between delay incurred on a flight and the cost penalty for the AU this delay represents. The delay-cost curve is unique for each flight, and it can encompass many aspects of the AU operation. Crucially, the delay-cost curve of a specific flight may be built in such way that it incorporates the costs of subsequent rotations of the same aircraft.

Demand Capacity Balancing (DCB)	The process of comparing traffic demand and available capacity in a defined timeframe, determining bottlenecks and assessing mitigation measures in order to find the optimum result in terms of minimising delays and costs. Where used in this OSED to convey a role in the proposed process, the term 'DCB' is intended to be the aggregate group including Local DCB, Airport, and Network Manager.
Fleet Delay Reordering (FDR)	The UDPP feature by which the AU can rearrange its own allocated baseline time by giving priority values on flights.
Flow Management Position (FMP)	An operational position established in appropriate air traffic control units to monitor traffic load for defined sectors (at en-route or at airport level) to ensure that traffic is safely managed by Air Traffic Controllers.
Knock-on delay or Reactionary delay	A side effect on subsequent flights due to delay given to an initial flight. The initial delays can be caused by various reasons, e.g. capacity constraints, ATC/Network constraints, airport constraints, but also airline constraints (crew, passengers …). The AU perspective on reactionary delay, in relation to the proposed concept, is to take into account all the AU fleet and aircraft rotations of the day to decrease the impact of the original delay. This is completely different from the Airport perspective where the typical approach to reactionary delay is to take into account only the impact on the local Airport platform.
Margin of Manoeuvre	For an AU, it is the maximum delay a flight can take before incurring significant cost (i.e. disruption on the delay-cost curve according to delay). It is anticipated that the "significant cost" can be defined differently by each AU, but for the purposes of this example, the cost represents a "step" that is due to factors such as crew or pilot time-out constraints, a large number of passengers who miss a connection, an airport curfew infringement etc. Each time one of the factors is met; another step in cost is incurred, which represents the end of another Margin of Manoeuvre for the AU. The Margins are typically expressed via "Time Not After" and "Time Not Before" parameters (see definitions below).
Network Manager Operations Centre (NMOC)	The Network Manager Operations Centre delivers core operational services across several domains: • Flow and Capacity Management • ATM Access Gateway and Flight Planning Operations • Information Management Domain • Crisis and Contingency Management Post-operations analysis and reporting

Network Operations Plan (NOP)	A rolling operational plan set up, maintained and shared by the Network Manager, containing expected and current traffic information, available sector capacities provided by the ANSPs and expected or actual delay information.
Prioritisation	Actions made by the AUs (using the UDPP features SFP, FDR, Slot Swap, Margins) according to the importance of their flights impacted by a UDPP measure, based on their business needs (N.B. Slot Swap is not part of this document because it is already implemented).
Protection/Protect a flight	UDPP Protection is part of the UDPP prioritisation. It is the highest priority given to a flight pushing its operation as close as possible to the planned (scheduled) off block time. To do this, UDPP applies the SFP algorithm for this flight.
Scenario	An operational situation in which Use Cases are executed.
Selective Flight Protection (SFP)	The UDPP feature by which an AU can obtain the minimum delay for a flight (Priority P) in exchange for more delay of another earlier own flight, even if the total delay for the given AU is increased.
Slot Issue Time (SIT1)	The time at which the NM issues the SAM to the AO and ATC at the aerodrome of departure.
Suspension	ATFM suspension (FLS) is an ETFMS message sent, suspending a flight, which thereafter should not get take-off clearance. NB an ATFM Suspended flight is not visible in the NOP.
Time Not After (TNA), Time Not Before (TNB)	These are the time components of the Margin of Manoeuvre. The components allow the definition of a closed (TNA and TNB together) or open-ended (TNA or TNB only) time window to be allocated by an AU to its own flight, as a constraint. This expression of AU constraint can be used to rearrange the AU sequence and/or to define a CCS resolution.
Time to Remove from Sequence (TRS)	Time needed to remove a flight from departure sequence. Its purpose is to prevent last minute modifications of the CTOT. These values are kept updated by the relevant FMPs and TWRs. They may be adjusted at any time depending on the local aerodrome traffic situation and may vary during the day. The TRS prevents a change to a later CTOT, or the allocation of a CTOT, when the flight is already in the departure sequence.
UDPP Suspended flight	UDPP Suspension is part of the UDPP prioritisation. It is the lowest priority given to a flight pushing its operation to the end of the CCS managed by UDPP (the UDPP measure). NB UDPP suspended flight is not an ATFM suspension, i.e. an FLS message.
UDPP inputs	UDPP inputs is a collective term for Protection, Margins of Manoeuvre and UDPP Priority values (see definitions above and below) that an AU may set for their flights in the UDPP measure.

UDPP max schedule anticipation	This CCS airport parameter (common to all AUs) gives the maximum early arrival delay buffer allowed by the airport to manage flights. (e.g. 5mn = 5minutes before reference flight arrival time is allowed). It's also used by the UDPP service to optimise the Arrival sequence maximising the arrival throughput.
UDPP measure UDPP NCP measure	ATFCM measures that allows the AU participation through the articulation of AU constraints for the purpose of CCS resolution. Two principal types of UDPP measure are anticipated in the concept: - "UDPP measure" based on ATFM regulation; - "UDPP NCP measure" based on Network Cherry-Pick measure. Each type of UDPP measure has its own specificities that are largely inherent from the original measure that is currently used in operations.
UDPP Priority value	A value given by the Airspace user on a flight (or a specified default value) used by the UDPP function to reorder the flights in the UDPP measure. Values can be: ***P*** for Protect, ***S*** for UDPP suspend, ***B*** for "keep baseline", or a number from 1 (highest priority) to 999 (lowest priority). See UDPP feature definitions in Appendix A2.

Table 11: Glossary of terms

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 PJ07-02 SPR-INTEROP/OSED for V2 - Part II - Safety Assessment Report, Edition 00.01.01, 15/10/2019

[8] SESAR Solution PJ07-W2-39 Validation Plan (VALP) for V3 - Part II - Edition 00.02.00, 16/09/2022

Other documents

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

[10] SESAR Solution PJ07-W2-39 SPR-INTEROP/OSED for V3 - Part I - Edition 00.07.03, 12/07/2022

[11] SESAR Solution PJ07-W2-39 SPR-INTEROP/OSED for V3 - Part IV - HPAR - Edition 00.01.02, 10/01/2023

[12] SESAR Solution PJ07-W2-39 Validation Plan (VALP) for V3 - Part I – Edition 00.02.00, 04/05/22

[13] SESAR Solution PJ07-W2-39 Validation Report (VALR) – v0.21 (draft) 03/03/2023

[14] SESAR Solution PJ07-W2-39 TS/IRS – Edition 00.04.01, 16/12/22

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

EUROPEAN PARTNERSHIP

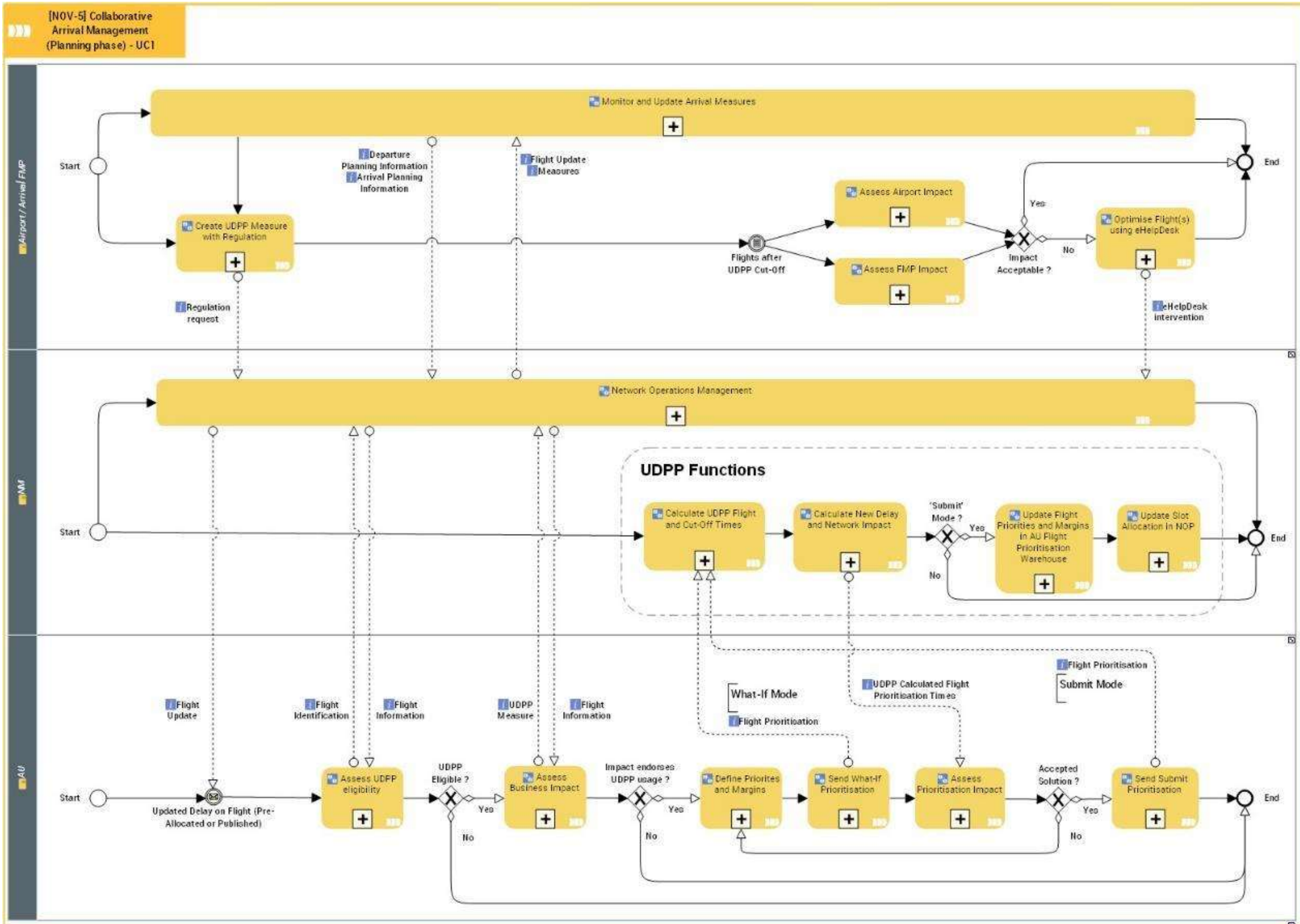
Co-funded by the European Union

Appendix A EATMA Models

Note from SPR-INTEROP/OSED [10]: No new EATMA model is needed for this use case 2 because it is the same as the use case 1, the activities are the same for both use cases. The difference resides in the particular way that some activities are implemented in detail in each use case.

EUROPEAN PARTNERSHIP

Co-funded by the European Union


[NOV-5] Collaborative Arrival Management (Planning phase) - UC1
Airport / Arrival FMP
Start
Monitor and Update Arrival Measures
Departure Planning Information
Arrival Planning Information
Flight Update Measures
Create UDPP Measure with Regulation
Regulation request
Flights after UDPP Cut-Off
Assess Airport Impact
Assess FMP Impact
Yes
No
Impact Acceptable ?
Optimise Flight(s) using eHelpDesk
eHelpDesk intervention
End
NM
Start
Network Operations Management
UDPP Functions
Calculate UDPP Flight and Cut-Off Times
Calculate New Delay and Network Impact
'Submit' Mode ?
Yes
No
Update Flight Priorities and Margins in AU Flight Prioritisation Warehouse
Update Slot Allocation in NOP
End
AU
Start
Flight Update
Updated Delay on Flight (Pre-Allocated or Published)
Flight Identification
Flight Information
Assess UDPP eligibility
UDPP Eligible ?
Yes
No
UDPP Measure
Flight Information
Assess Business Impact
Impact endorses UDPP usage ?
Yes
No
What-If Mode
Flight Prioritisation
Define Priorites and Margins
UDPP Calculated Flight Prioritisation Times
Send What-If Prioritisation
Assess Prioritisation Impact
Accepted Solution ?
Yes
No
Flight Prioritisation
Submit Mode
Send Submit Prioritisation
End

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	Impact of several UDPP measures implemented simultaneously at Network level remains to be analysed and tested	The information included in the VALR allows to ensure that there is no safety impact (see section 5.3.2) As such, this safety issue opened during PJ07-02 SAR in Wave 1 is resolved and closed
I002		

Table 13: Safety Issues log

B.3 Operational Limitations log

Ref	Operational Limitations
L001	
L002	

Table 14: Operational Limitations log

Insert project logo here

-END OF DOCUMENT-

Insert project logo here

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