INDUSTRIAL RESEARCH

sesar JOINT UNDERTAKING

SESAR Solution PJ.09-W2-44 SPR-INTEROP/OSED for V3 - Part II - Safety Assessment Report

Deliverable ID:	**D.2.1.001**
Dissemination Level:	**PU**
Project Acronym:	**DNMS**
Grant:	**874463**
Call:	**H2020-SESAR-2019-1**
Topic:	**SESAR-IR-VLD-WAVE2-07-2019**
Consortium Coordinator:	**EUROCONTROL**
Edition Date:	**29 March 2023**
Edition:	**00.01.02**
Template Edition:	**00.00.02**

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Authoring & Approval

Authors of the document

Beneficiary	Date
EUROCONTROL	12 January 2023

Reviewers internal to the project

Beneficiary	Date
EUROCONTROL	3 February 2023
ENAIRE/CRIDA	3 February 2023
DSNA	3 February 2023
NATS	3 February 2023
INDRA	3 February 2023
PANSA	3 February 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

Rejected By - Representatives of beneficiaries involved in the project

Beneficiary	Date

Document History

Edition	Date	Status	Beneficiary	Justification
00.00.01	February 2022	Initial Draft	EUROCONTROL	Initiation of the document
00.00.02	October 2022	Mature Draft	EUROCONTROL	Document updated with the design level analysis and with the HAZID outcome

00.01.00	12 January 2023	Final version for project review	EUROCONTROL & internal project reviewers	Finalization
00.01.01	07 March 2023	Final version	ENAIRE/CRIDA	Update comment from SJU
00.01.02	29 March 2023	Final version	ENAIRE / CRIDA	Changed summary of EXE 02 and 04 results. Comments arising from Maturity Gate.

DNMS

DYNAMIC AIRSPACE CONFIGURATION

This Safety Assessment Report is part of a project that has received funding from the SESAR3 Joint Undertaking under grant agreement No 874463 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.09-W2 Solution 44 (Dynamic Airspace Configuration) coordinated by EUROCONTROL.

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

No table of figures entries found.

1 Executive Summary

This document contains the Specimen Safety Assessment for a typical application of the PJ.09-W2 Solution 44 DAC. The report 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 PJ.09-W2 Solution 44 DAC Solution SPR-INTEROP/OSED.

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 PJ08-01, PJ08-02 and PJ09-02 in SESAR2020 Wave 1, contained in the corresponding SARs [3][4]. The current version of the document contains updates with the work done for the DAC concept in SESAR 2020 Wave 2.

2 Introduction

2.1 Background

The SESAR W2 Solution 44, "Dynamic Airspace Configuration (DAC)" is built upon Wave 1 results of PJ08-01 and PJ09-02.

The following documents should be taken into consideration:

- OSED PJ08 - [5] to get familiar with DAC related concepts,
- OSED PJ09 - [6] to get familiar with INAP related concepts,

2.2 General Approach to Safety Assessment

A Broader approach

The safety assessment has been conducted in accordance with the SESAR Safety Reference Material (SRM) [9] and associated Guidance [8]. The SRM is based on a twofold approach:

- a *success approach* which is concerned with the safety of the DAC concept, in the absence of failure; and
- a conventional *failure approach* which is concerned with the safety of the DAC concept, in the event of failure within the end-to-end System

These two approaches are applied to the derivation of safety properties at each of two successive stages of the development of DAC, as follows:

Safety specification at the Service Specification Level

This is defined as what the new concepts have to achieve at the Air Traffic Management (ATM) operational level in order to satisfy the requirements of the airspace users - *i.e.* it takes a "black-box" view of the new method of operations and includes what is "shared" between the users and the service providers.

From a safety perspective, the user requirements are expressed in the form of Safety Implication of the Intended Uses and the Specification is expressed in the form of Safety Requirements at Service Level (functionality & performance and integrity/reliability properties), which are derived during the V1 and V2 phases of the development lifecycle. The purpose is to check the completeness of the OSED and identify possibly additional safety validation objectives to be revealed by the safety analysis in view of their inclusion in the Validation plans.

Safety Specification at Design Level

This describes what the new DAC concept is actually like internally and includes all those system properties that are not directly required by the users but are implicitly necessary in order to fulfil the specification and thereby satisfy the user requirements. Design is essentially an internal, or "white-box", view of DAC operations. This is more generally called the Design-level Model and is expressed in terms of human and machine "actors" that deliver the functionality.

From a safety perspective, the Design is expressed in the form of Safety Requirements at Design level (sub-divided into functionality & performance and integrity/reliability properties), which are derived

during the V2 and V3 phases of the development lifecycle. The purpose here is to feed the SPR/INTEROP/OSED with a complete and correct set of safety requirements. Furthermore, if relevant, interact with the validation exercises so as to include additional safety validation objectives and obtain validation feedback regarding certain proposed safety requirements.

2.3 Scope of the Safety Assessment

The PJ.09-W2-44 DAC safety assessment makes extensive use of outcomes from previous PJ08 and PJ09 SARs [3][4].

The following parts of the safety assessment lifecycle are covered by the current issue of the Safety Assessment Report:

- **V1** - through initial identification of safety implications of the Change and the definition of Safety Criteria and/or Safety Implication of the Intended Uses

- **V2&V3** - through establishing Safety Requirements at Service level (SRSs) and the derivation of Safety Requirements at Design Level (SRDs) (based on combined safety analysis of the design and safety-related measurements, observations and debriefing of the validation exercises). The safety assessment for Safety Requirements derivation will align with the design maturity (i.e. successive inclusion of OIs). The safety assessment will be conducted to the level of granularity decided by the Project for the OSED/SPR/INTEROP and TS/IRS documents for the design of the Functional system for the Solution (encompassing people, procedures & airspace and equipment).
  The SRDs are derived during the V2&V3 phases of the development lifecycle as initial SRDs. The purpose is to feed the SESAR Solution PJ.09-W2-44 DAC SPR-INTEROP/OSED Part I with a complete and correct set of safety requirements. Furthermore, where relevant, the requirements inform the validation exercises with respect to the inclusion of related additional validation objectives for which validation feedback is required.

The PJ.09-W2-44 addresses the following OIs:

- AOM-0805 - Refine the DAC operational concept and associated algorithm

- AOM-0809-A - Initial Sector Design and Configurations Unconstrained by Predetermined Boundaries

- CM-0104-C *and* DCB-0210 - Align Integrated Network Management ATC Planning (INAP) processes, roles and measures to extend INAP operations and include DAC as part of Demand and Capacity Balancing (DCB)

- CM-0103-B, CM-0102-B - Development of new features and indicators: complexity, confidence level, what-if and what-else, uncertainty

The focus of PJ.09-W2-44 is the integration of DAC and Integrated Network Management ATC Planning (INAP) concepts, especially on the INAP timeframe where the two overlap, in a seamless way. The improvements brought by Sol 44 per concept area can be found in section 3.1 of this document or in the corresponding OSED [7].

The Safety assurance activities will be conducted in line with the SESAR 2020 Safety Policy, SESAR SRM [9] and accompanying Guidance [8].

2.4 Layout of the Document

Section 1 presents the executive summary of the document

Section 2 provides the background of the DAC 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 detailed outcome of the HAZID

3 Setting the Scene of the safety assessment

3.1 Operational concept overview

The information provided in this section is a short summary. For more details please refer to the PJ.09-W2-44 OSED [7].

The SESAR W2 Solution 44, "Dynamic Airspace Configuration (DAC)" is built upon Wave 1 results of solutions PJ08-01, PJ08-02 and PJ09-02.

The core focus of the PJ.09-W2-44 solution is the use of DAC concept into the DCB process including the Integrated Network Management ATC Planning (INAP) concept, in an integrated way, and not as two different steps. A particular emphasis will be put on the INAP timeframe where the two overlap. The INAP timeframe could be established between a few hours to a few minutes before a spot occurs, e.g.: from ~-6 hours to ~-15 min, the limits thresholds being to be adjusted according to local specificities.

The DAC Process:

The objective of the DAC process is to **identify optimized airspace configurations** (including configuration plans for transitions) for a defined airspace through the implementation of airspace design and configuration sub-processes based on the forecasted air traffic complexity, ATCo workload and ATCo availability as well as the traditional count methodologies provided by the Imbalance Prediction and Monitoring Service (Hourly Entry Counts and Occupancy). The optimized airspace configuration identified with the DAC toolbox should **meet forecasted traffic demand and reach the defined performance targets both at Local and Network levels and with minimal impact on the Business/Mission Trajectories.**

DAC proposes two process models:

- **Model A** is the "top down" DAC management model characterised by the leading role of Network Manager who is kicking off, coordinating and monitoring the DAC planning process with local actors (at national or sub-regional level depending on local organisation) assisting NM with local expertise, data and knowledge. However, the closer to the execution phase the more responsibilities are shifted from NM towards local DAC management level.
- **Model B** is the "bottom-up" DAC management model characterised by leading role of local actors (at national or sub-regional level depending on local organisation) in DAC management process in nominal case with monitoring, moderating and facilitating role of the Network Manager.

The selection of one model or the other will have an impact on the allocation of functions and responsibilities to the actors involved in DAC process.

The INAP Function

The INAP function encompasses some of the activities of the Local Traffic Manager (LTM) in tactical phase, the activities of the Extended ATC Planning(s) (EAP) and the activities linked to de-complexification managed by Planner Controller (PC) on Controller Working Positions (CPW), in a seamless and closely intertwined manner.

The EAP role has been introduced in SESAR 1. Solution 09.02 in SESAR2020 Wave 1 has investigated and validated this role, together with associated responsibilities, working methods and toolset, towards full integration with local Network Management function and ATC within INAP.

The LTM (Local Traffic Manager) replaces the Flow Manager Position (FMP) with additional responsibilities and tools, working in close collaboration with the EAP (in case they are different actors), sharing the same situation awareness, based on common information sources and extensive means of communication. CWPs are also involved in the INAP process, notably the PC, extending the PC's situation awareness beyond the scope of their Area of Interest.

It is important to note that EAP is a role, and not necessarily a dedicated actor. Depending on local management of staff, EAP and LTM roles could very well be ensured by the same person. It will depend on the ANSP the allocation of the EAP role to a specific actor and define pre-requisites to fulfil the position.

3.2 Scope of the change

PJ.09-W2-44 DAC will complete the R&D work developed within SESAR2020 Wave 1 trying to take to V3 maturity the DAC and INAP concepts developed within SESAR2020 W1 in projects PJ08-01, PJ08-02 and PJ09-02. Therefore the reference for the change is represented by the maturity of the concepts reached at the end of SESAR2020 Wave 1.

Reference (for validation) ATM&ANS systems & operations

Regarding Demand Prediction:

- Demand Prediction based on Demand Data Repository (DDR) processing;
- Imbalance Prediction based on count methodologies (Entry Count; Occupancy count) and initial complexity methodologies;

Regarding hotspot management:

- NM system provides services to collect and disseminate hotspot information but does not support other category of problems (like OptiSpot - area for opportunities/optimisation); nor does it support hotspot monitoring (to detect hotspot resolution deviation)

Regarding Local DCB roles and processes:

- STAM, VTAM;
- ASM support systems enhanced to exchange real-time airspace status updates;

- ATC systems enhanced to exchange real time (tactical) airspace status data with ASM support system;
- Exchanges between ASM support system and Airspace managers at Regional, sub regional and local level are supported by AIXM 5.1 (ADEXP, B2B etc.);

Regarding Target Time Management:

- TTA/TTO + CTOT;

Other:

- Slot swapping;
- AOP and NOP are in use;
- Network Airspace management system equipped with tools for collection of real-time airspace data.

Solution ATM&ANS systems & operations

The focus of PJ.09-W2-44 is the integration of DAC and Integrated Network Management ATC Planning (INAP) concepts, especially on the INAP timeframe (pre-tactical and tactical) where the two overlap, in a seamless way thanks to the following improvements, per concept area:

Dynamic Airspace Configuration (DAC):

- Integration with INAP and DCB;
- Integration of pre-tactical and tactical DAC;
- Implementation of optimised solutions:
  - i.e. sector configuration performance based approach defined according to a set of DAC KPA/KPI Assessment Criteria (link with What-if);
- Integration of complexity within the sector configuration optimisation process;
- Further mature of ATC procedures for all actors involved in the DAC process (SUP, ATCOs, etc.);
- Cross border for demand and capacity measures:
  - Cross border relates to being aware of the demand and sectorisation of neighbouring ATSUs as an input for coordinating capacity and demand measures in view of supporting airspace delegation to be addressed by PJ10-W2-93 and PJ32-W3;
- Full concept Integration within the Network Operations Plan (NOP) – B2B service between the locally done DCB (including demand and capacity – in Wave 1 it was only done for demand measures) and the NOP

INAP (LTM/EAP):

- Integration with DAC to extend capacity Management at tactical level;

- New functionalities: What-if/What-else for both LTM and EAP.

Note that the EAP concept will not be further developed compared to Wave 1.

ATFM Measure Design:

- New KPIs such as fuel burn/distance flown and environment impact, delay;
- New types of demand and capacity measures (e.g. Targeted CASA regulation, dynamic sector configuration, etc.);
- ATFCM measure implementation enhanced through digital communication (B2B) with regional NM;
- Digital communication with ATC included in the OSED scope (and also HP and SAF scope).
    - To check whether it was further addressed by the validation exercises.

Complexity Management:

- Complexity tool to support DAC;
- Integrate within the sector configuration optimisation process of: complexity, ATCo workload (new parameter based on psychological task model of the ATCO – developed in SESAR 1 and used in Wave 1) and ATCo availability;
- Further mature complexity algorithms.

What-If Functionality:

- Combination of DAC and DCB measures;
- Used by LTM/EAP actors.

What-Else Functionality:

- Development of what-else function to help the INAP actor propose adequate solutions, combining DAC and DCB measures (to cover strategic to tactical measures).

Note that “What-else” will not be covered in the validation exercises. “What-else” is to be developed technologically in SESAR 3 (need to perform an initial HP/SAF operational use assessment) and it will be based on AI.

Uncertainty:

Uncertainty to be presented to the DCB actor in the tool used to monitor the evolution of traffic. The following sources of uncertainty should be accounted for:

- Timeframe;
- Type of spot: optispot or hotspot;
- Trajectory prediction uncertainty, taking into account: A/c intentions, Met conditions Modelling errors, Flight technical errors;

- Quality of the information.

Based on the uncertainty data of the different sources of information presented above, the calculation is performed, accounting also for historical data. The detailed process followed for its calculation will be detailed in future versions of the OSED [7].

Spot Management:

Different categories of spots considered, characterised with Traffic Monitoring Values (TMV):

- Hotspot;
- OptiSpot;
- netSpot (through NM monitoring the network loads and the evolution of the performance target KPIs).

Note that PJ09.44 includes spots monitoring. Different monitoring parameters will be shown on the HMIs of the various concerned actors (sector capacity, occupancy traffic, complexity and workload), but only the complexity value is part of the change for Sol 44.

Regarding the two solution use cases addressing ATC:

- DCB-UC-08a: Air Traffic Control in an integrated DAC-DCB environment – hotspot
  - The only change compared to reference (i.e. Wave 1 PJ08) is in relation to the LTM-ATSU SUP coordination and Collaborative Decision Making process (possibility of interlacing DAC with DCB measures when approaching the DCB measures cut-off time). All the ATC use case activities, information flows and requirements remain unchanged compared to Wave 1 PJ 08.
- DCB-UC-08b: Air Traffic Control in an integrated DAC-DCB environment - optispot
  - Not relevant for the safety assessment (optispot have no safety implication).

Type of solution from a safety assessment perspective

As explained above, no changes to ATC are brought in by this Solution (the LTM-ATSU SUP coordination and Collaborative Decision Making process, although hosted in an ATC-related use case, could be addressed by the safety assessment together with the DAC and DCB services).

In conclusion, as the change is focused on DAC and DCB this is a **"Other-than-ATS" operational solution** which does not have direct ATS safety impact but an indirect impact via the potential safety implications of the DAC and DCB services delivered to ATS. Consequently the section 3.5 will not define Safety Criteria but Safety drivers.

3.3 Solution Operational Environment and Key Properties

Operational Environment:

Airspace:

- Fixed and FRA;
- ER & TMA (For DAC: En-Route only; For DCB/INAP: En-Route, TMAs);

- Airspace layout: current ICAO ATS airspace classifications (controlled airspace); only IFR are considered.

Traffic type: Civil & Military.

Weather: all types of weather conditions.

FABs, can contribute to DAC by permitting airspace configuration regarding flows, and disregarding boundaries (plus better sharing of human resources).

[…]

3.4 Stakeholders' expected benefits with potential Safety impact

The Solution should enable a more efficient use of the available sectors capacity due to a better airspace configuration and best DCB measures optimising the use of available airspace (i.e. optimally adapt airspace capacity to the demand). That involves an increase in the airspace throughput (**CAP2**) whilst **maintaining safety**.

The interlacing of DAC and DCB measures would enable the lowest impact on the Airspace User while **maintaining safety (FEFF1)**.

In conclusion:

Safety to be maintained despite capacity increase ➔ SVT: Safety Neutral with traffic increase – **This needs to be confirmed/validated when performing the overall PAGAR Safety computation**.

3.5 Safety Drivers

Based on the SESAR2020 SRM guidance update, in order to address the change introduced by Sol 44 impacting "Other-than-ATS" operational services (e.g. DCB service provided by NMf), a set of Safety Drivers (SD) 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 [11] and NM Airspace Data Service Specification [10]. Please note that, even though the baseline refers only to regional NM services, the services in the SDs defined in this section refer to the NM function (NMf). SDs were defined only on the services where it was identified that Sol 44 is introducing a change with safety impact.

In order to define the Other-than-ATS SDs, the following two assumptions were made:

- **Assumption 01:** the EAP role in Sol44 is participating in DCB through e.g. actions of de-complexification, very short term STAMs, DCB measures in specific sectors (in view of preventing overloads). The potential EAP role for planning in view of conflict resolution is out of scope for this solution.
- **Assumption 02**: In SESAR, it is considered that INAP DCB related activity (LTM+EAP) is not part of the ATS service provided by their ANSP, but is providing DCB service to their own ANSP and/or to other entities (aerodrome, other ANSP, etc.).

Safety Drivers:

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

SD 000: The change introduced by Sol44 to the Short Term DCB service shall not increase the number of overloads, despite the X% increase in sector(s) capacity.

This high-level SD 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 LTM, 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*):

SD 001: The Load and Capacity Monitoring service delivered to ATS, service which is enhanced with complexity at local level by Sol44, shall not increase the number of overloads, despite the increased airspace throughput (CAP2).

Note for SD 001: The share of local complexity to regional NM in order to build a consolidated view of complexity will be brought in from Sol 45. Until that is the case, complexity remains local in Sol 44.

- 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 the following functions: *ATFCM measure design*, *ATFCM measure promulgation*, *ATFCM measure implementation* and *Network cherry-pick regulations*)

SD 002: The ATFCM measure design service delivered to ATS, service which is enhanced by Sol 44 with new KPIs (such as fuel burn/distance flown and environment impact), new types of demand and capacity measures (e.g. Targeted CASA regulation, dynamic sector configuration, etc.) and new functionalities (e.g. What-if/What-else) shall not increase the number of overloads, despite the increased airspace throughput (CAP2)..

SD 003: The ATFCM measure implementation service delivered to ATS, service which is enhanced by Sol 44 through digital coordination and information sharing with regional NM and ATC, shall not increase the number of overloads, despite the increased airspace throughput (CAP2).

- In order to account for the impact on the Airspace and capacity data provision service (basic service component that includes collection, analysis, validation, upload into and maintenance of airspace, capacity and aeronautical (environment) data in the CACD; it contains the following functions: *ENV dossier, Static and dynamic NM environment data updates, Provision of AIXM airspace data files and Environment data query*)

SD 004: The Airspace and capacity data provision service delivered by regional NM shall maintain the same level of safety-related performance as per NM AIRSPACE DATA SERVICE SPECIFICATION [10], accounting for the following Sol 44 updates:

- The ENV dossier function updated with dynamic sector configurations and DMAs;

- The Static and Dynamic NM environment data update function with CACD consideration of sector capacity for the dynamic sector configuration;

- The Provision of AIXM airspace data files function enabling the exchange of the dynamic sector configurations and DMAs.

- In order to account for the impact on the Consolidated European Airspace Use Plan (eAUP) service (delivered by the Central Airspace Data Function (CADF), includes preparation and release of a consolidated daily European Airspace Use Plan (EAUP) and European Updated Airspace Use Plans (EUUPs)):

SD 005: The Consolidated European Airspace Use Plan (eAUP) service delivered to ATS, service which is merged by Sol 44 with the ATFCM daily plan (ADP) to form the EDAC plan, shall maintain the same level of safety-related performance as per NM AIRSPACE DATA SERVICE SPECIFICATION [reference].

Note for SD 005: To be clarified if the merging implies any changes to the eAUP and ADP services. It may potentially imply format changes.

Note for SD 004 and SD 005: safety-related performance might be characterised by one or several of the following attributes: correctness, accuracy, integrity, availability and reliability. The safety assessment will determine which of them are related to safety performance.

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 both 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 functionality & performance 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 Safety Drivers.

That comes to interpret, from a safety perspective, the OSED Operational Concept specification (i.e. how the DAC 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 OSED Use Cases. 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, by considering the management of Dynamic Airspace Configuration as a series of continuous processes described through the Use Cases. This shows how the SRSs contribute to meeting the Safety Drivers.

The SRS address only the aspects affected by the Change and which have a safety implication (i.e. potential contribution to un-resolved overloads).

No SRS has been derived for the Use Cases / activities with no safety implication i.e.:

- DCB-UC-00: Coordination and publication of Optimal Network DCB scenario,
- DCB-UC-01: Airspace Design,
- DCB-UC-02: Optimised configurations,

- DCB-UC-04: Spot analysis,
- DCB-UC-05 How to choose a DCB measure,
- DCB-UC-08b: Air Traffic Control in an integrated DAC-DCB environment – optispot)

Table 1 presents the consolidated list of functionality & performance Other-than-ATS Ops SRSs under normal operational conditions. The link to the Safety Drivers is shown in the last column for each SRS, via the relevant Use Case that is concerned with the change and allowed the SRS derivation.

ID	Safety Requirement at Service level (SRS) *(success approach)*	Use Case	Related Safety Driver
SRS 001	In addition to Traffic Counts (Hourly Entry Counts and Occupancy Counts), Complexity and ATCO Workload shall be displayed to the LTM/EAP actor through the Imbalance Prediction and Monitoring Service HMI in order to enable them to analyse traffic volume imbalances	DCB-UC-03: Imbalance Detection and Spot Declaration during the Tactical Phase	SD 001 SD 004
SRS 002	The hotspot resolution monitoring alert, encompassing the monitoring values (MV) revision, provided to the LTM/EAP actor shall account for complexity and workload, in addition to entry and occupancy counts	DCB-UC-06: Spot Resolution and monitoring	SD 001 SD 004
SRS 003	The LTM-ATSU SUP coordination & Collaborative Decision Making process shall account for the possibility of interlacing DAC with DCB measures when approaching the DCB measures cut-off time *Note: No other change in ATC activities compared to Wave 1 PJ 08.*	DCB-UC-08a: Air Traffic Control in an integrated DAC-DCB environment - hotspot	SD 001 SD 004
SRS 004	The LTM coordination with WOC in view of agreeing on the tactical ARES/DMA (re)allocation and subsequent EDAC publication, shall account for the possibility of interlacing DAC with DCB measures	DCB-UC-10: Change of DCB plan and its publication update	SD 005

ID	Safety Requirement at Service level (SRS) *(success approach)*	Use Case	Related Safety Driver
	when approaching the DCB measures cut-off time		
SRS 005	The What-if exclusion tool shall propose to the LTM the flights to be excluded from the regulation whilst still allowing LTM to resolve the hotspot	DCB-UC-07: What-if flight exclusion tool	SD 002 SD 003
SRS 006	The Target flow CASA regulation measure shall be proposed to LTM as a potential alternative to the baseline CASA flow regulation in view of NM impact assessment and comparative evaluation of performance against the baseline regulation	DCB-UC-09: Target flow CASA	SD 002 SD 003

Table 1: Safety Requirements at Service Level (success approach)

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 PJ08-01, PJ08-02 and PJ09-02 safety assessments:

- ABN1. NOP/ SWIM failure
- ABN2. Unforeseen airspace closure (e.g. Volcanic Ash, nuclear cloud, etc.)
- ABN3. Severe weather conditions (CBs, turbulences, icing, etc.)
- ABN4. Unplanned Large Airport closure
- ABN5. Industrial actions, e.g. strikes
- ABN6. Loss of enablers such as Traffic predictions, Confidence index
- ABN7. Major technical changes

The table below assesses, for each abnormal condition, the immediate effect on DAC operations 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 PJ09.44 was identified) additional mitigation means might be specified in terms of new SRSs.

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects
ABN1	NOP/ SWIM failure	Mechanism for sharing information and the network centric view are lost. If that lasts longer, it would impair the DCB and DAC functions	Local DAC actors will take over (using the locally available traffic prediction, last published EDAC, etc.) Coordination by phone, mail etc. Fall-back arrangements adapted to the Management of DAC will be in place for defining airspace configurations in the event of prolonged NOP/SWIM failure (as per mitigation proposed in PJ08.01 SAR)
ABN2	Unforeseen airspace closure (e.g. volcanic ash, nuclear cloud …)	**In terms of DAC:** Unplanned losses of capacity **In terms of DCB:** Source of new hotspots that might turn the existing DCB measures insufficient or inefficient. STAM measures created to deal with an overload, are not applicable anymore, and should be replaced by a regulation. However, it may be too late to apply a regulation. No new effects compared to Baseline	**In terms of DAC:** Management of DAC provides extra options - can quickly design options; **In terms of DCB:** Short term: None (ATC deals with the imbalance in the affected sectors) Longer term: Restrictive regulation
ABN3	Severe weather conditions (CBs, turbulences, icing)	**In terms of DAC:** Unplanned losses of capacity **In terms of DCB:** Specific conditions are developing locally which require adopting and coordinating a planned "axis management"	**In terms of DAC:** Management of DAC provides options for providing best performance given severe weather conditions **In terms of DCB:** NMf actors (Regional and Local) will adopt and

		scenario implementation with special and possibly earlier scenario activation. No new effects compared to Baseline.	coordinate a planned "axis management" scenario implementation
ABN4	Unplanned Large Airport closure	Unplanned losses of capacity. No new effects compared to Baseline.	DCB measures need to be re-assessed and new measures implemented, whenever applicable.
ABN5	Industrial actions, e.g. strikes	With pre-notice, expected loss of capacity This would involve decreased ATCO availability No new effects compared to Baseline	**In terms of DAC:** Management of DAC provides options for providing best performance given reduced ATC resources. **In terms of DCB:** Restrictive DCB measures.
ABN6	Loss of enablers such as Traffic predictions, Confidence index	EDAC publication is delayed. Loss of capability to generate DACs. Will affect mainly the medium term planning with impact on performance but not on safety	No mitigation necessary in the short term
ABN7	Major technical changes	Planned capacity reductions	Management of DAC provides options for providing best performance given reduced ATC resources

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

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

This section addresses the DAC 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 series of one to one meetings with the OSED Use Case experts (in replacement of a HAZID workshop).

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 [8].

The detailed outcome of the hazard identification meetings is provided in Appendix A which includes the working table used for recording and structuring the relevant information for the hazard identification and analysis.

Table 3 represents a summary of the full HAZID outcomes shown in Appendix A 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 Cases specified in OSED (see Reference [7]). 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 Reference [8]. 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).

In the table the elements highlighted in GREEN represent the change introduced by PJ09 SOL 44.

Service Hazard Description	Success SRS	Operational effect	Mitigations protecting against propagation of effects	Severity *(most probable effect)*
Inadequate airspace configuration not fully recoverable via ATFM (demand) measures		Final sector configuration or revised ATFM measures to be included in the latest published EDAC is inadequate (hotspot not resolved).	Upon detection by FMP, ATFM measures need to be implemented (STAM might be feasible, for regulations it might be late) If detected late, risk of sector overload. The risk is partially mitigated via FMP working method and supporting tools. Additional partial mitigation with PJ09.44: the possibility of interlacing DAC with DCB measures when approaching the regulations cut-off time.	MAC-SC4b IM=10
ATFM measures not designed or not implemented or implemented partially by Local ATFCM		Risk for sector overload as the **DCB process** is not respected in terms of roles/responsibilities, procedures and timeline (including hotspot identification / declaration or the associated DCB measure implementation / coordination / implementation)	In case local LTM does not identify hotspot, it might be detected at NM level (but that is not systematic) Tactical conflict management In case of no complexity available whilst maintaining occupancy and	MAC-SC4b IM=10

Co-funded by the European Union

Service Hazard Description	Success SRS	Operational effect	Mitigations protecting against propagation of effects	Severity *(most probable effect)*
			entry counts, imbalances detected as per current operations based only on Entry and Occupancy Counts. Due to reduced accuracy, some imbalances might be missed.	
Inadequate ATFM measure designed and implemented by Local ATFCM		Risk for sector overload as a DCB measure is not correctly designed (in terms of problem analysis and impact assessment)	Potentially detected by local ATFCM (INAP) Tactical conflict management Changes in relation to the use of complexity indicator in addition to occupancy and entry counts	MAC-SC4b IM=10
Inconsistency between the published EDAC and the State airspace user (WOC) ARES temporal parameters leading to sector overload		The ARES reservation published via the latest EDAC will not be fully consistent with the one agreed by WOC. Risk of ARES modification not consistent with the latest published EDAC. In case of inconsistent time ARES parameters there is a risk of overload (e.g. mission arriving earlier or leaving earlier the ARES) In the worst case for DMA*, the inconsistency concerns the DMA spatial parameters in which case the military aircraft will violate the published DMA dimensions	WOC might detect problem upon receiving ARES modifications published in EDAC. ATC still has the opportunity for ARES revision or cancellation in the execution phase in case of sector overload	MAC-SC4a IM=10

Service Hazard Description	Success SRS	Operational effect	Mitigations protecting against propagation of effects	Severity *(most probable effect)*
		*For DMAs, please see the safety assessment of PJ07.40.	The military controller and/or the pilot will tactically ensure separation from the conflicting civil traffic.	
No traffic load data provided to users		Loss (total or partial) of Network predicted imbalances (including workload and complexity indicators). Already coordinated ATFCM measures ("for implementation" status) will be implemented but with no possibility to monitor their implementation. Meanwhile no new ATFCM measures can be designed because no new hotspots can be identified. Detectable degradation of the imbalance prediction (traffic demand differs from the planned "correct" one by more than 10%) Risk for sector overload, might compromise the traffic planning & synchronization tasks (resources are allocated in priority to tactical conflict management tasks e.g. ATCO_PLN helps ATCO_EXE)	Addressed as per the current DCP (NMOC Disaster Contingency Planning). Tactical conflict management	MAC-SC4b IM=10
ATC failure to detect or resolve a pre-tactical conflict (Pre-tactical conflict = conflict that the PLN controller can observe and		The pre-tactical conflict not detected or not resolved (due to e.g. lack of PLN ATCO situation awareness in relation to planning and coordination in the configuration to	A planning or coordination error would normally be detected and recovered tactically by EXE ATCO through the tactical conflict resolution barrier.	MAC-SC4b

Service Hazard Description	Success SRS	Operational effect	Mitigations protecting against propagation of effects	Severity *(most probable effect)*
attempt to resolve before tactical intervention is needed) Note that there is no change compared to the reference scenario for this hazard		come) emerges into a tactical conflict to be managed by the EXE ATCO		
ATC incorrect planning&coordination induces a conflict (Planning&coordination includes notifying the flight (FDPS/SYSCO), coordinating transfer conditions, and handling coordination messages. However, it does not include transfer/assume functions, which are covered under ATC tactical functions. Note that there is no change compared to the reference scenario for this hazard		An additional planning conflict is induced e.g. due to PLN ATCO lack of situation awareness in relation to planning and coordination in the configuration to come (given that more sector re-configurations are possible and more frequent, the required coordination with neighbouring sectors, involved in the future sectorisation, becomes more demanding).	The conflict induced by a planning or coordination error would normally be detected and recovered tactically by EXE ATCO through the tactical conflict resolution barrier.	MAC-SC4b
ATC failure to detect or resolve a tactical conflict		Unresolved tactical conflict evolving to an imminent separation infringement (e.g. due to EXE ATCO lack of situation awareness	ATC Collision prevention (with or without STCA)	MAC-SC3

Service Hazard Description	Success SRS	Operational effect	Mitigations protecting against propagation of effects	Severity *(most probable effect)*
(Tactical conflict= any conflict that the EXE controller has to solve. These are planned conflicts - existing ones from planning, and induced - new conflicts - generated by aircraft deviations resulting from pilot, systems or ATC errors) Note that there is no change compared to the reference scenario for this hazard		about the sector configuration currently in use or due to a late transfer on frequency during the transition to the upcoming sector configuration)		
ATC incorrect trajectory management induces a tactical conflict (Trajectory management= Monitoring flight conformance with the assigned trajectory, Management of non-conformance whilst verifying separation between aircraft and conflict with restricted airspace, Manage aircraft request for trajectory		As the tactical conflict is induced by ATCO, the same actor might not be in the right position to detect & resolve it before evolving into an imminent separation infringement (that might be caused by e.g. a wrong coordination with respect to transfer of part of area of responsibility or ATCO lack of awareness about the sector configuration currently in use),	ATC Collision prevention (with or without STCA)	MAC-SC3

Service Hazard Description	Success SRS	Operational effect	Mitigations protecting against propagation of effects	Severity *(most probable effect)*
changes. The resolution of a tactical conflict might also induce a tactical conflict, as a knock-on effect) Note that there is no change compared to the reference scenario for this hazard				
Tactical sector configuration change not timely implemented or implemented partially Note that there is no change compared to the reference scenario for this hazard		Risk for sector overload (moderate overload is expected given the transitory character of this degradation, which might result from e.g. ATCO not being able at the last moment to accept the sector configuration change).	Mainly PLN ATCO is impacted, as helping the EXE ATCO will supersede his normal planning activities. The tactical conflict resolution barrier is not impacted	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 [8]).

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 [8]) is illustrated via the example for Hz 05 below:

Hz 05: No traffic load data provided to users

As Hz 05 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.

$SO_{105} = \frac{MTFoO_{relevant\_severity\_class}}{N \times IM} = \frac{1E-02}{100 \times 10} = 1E-05$ [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 [8]) as follows:

- MTFoO = 1E-2 and N=100 for Hz 01, Hz 03, Hz 04, Hz 05, Hz 06, Hz 07 and Hz 10 (MAC-SC4b)
- MTFoO = 1E-3 and N=30 for Hz 02 (MAC-SC4a)
- MTFoO=1E-4 and N=25 for Hz 08 and Hz 09 (MAC-SC3)

The consolidated list of the derived integrity/reliability SRSs (failure approach) is provided in Table 4 below. Derivation has been performed only for the hazards impacted by the change (highlighted in GREEN in the table). The remaining SRS (derived previously in the PJ08-01, PJ08-02 and PJ09-02 safety assessments) are included for completing the picture.

SRS ID	Safety Requirements at Service level *(integrity/reliability)*	Related Service Hazard	Severity & IM
SRS 101	The likelihood of inadequate airspace configuration not fully recoverable via ATFM (demand) measures shall be no more than 6e-5 per sector operational hour	Hz 01	MAC-SC4b IM=10
SRS 102	The likelihood of inconsistency between the published EDAC and the State airspace user (WOC) ARES temporal parameters leading to sector overload shall be no more than 2e-5 per sector operational hour	Hz 02	MAC-SC4a IM=10
SRS 103	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 03	MAC-SC4b IM=10
SRS 104	The likelihood of inadequate ATFM measure designed and implemented by Local ATFCM shall be no more than 6e-5 per sector operational hour	Hz 04	MAC-SC4b IM=10
SRS 105	The likelihood of No traffic load data provided to users shall be no more than 6e-5 per sector operational hour	Hz 05	MAC-SC4b IM=10

SRS 106	The likelihood of ATC failure to detect or resolve a pre-tactical conflict shall be no more than 6e-4 per sector operational hour	Hz 06	MAC-SC4b
SRS 107	The likelihood of ATC incorrect planning&coordination induces a conflict shall be no more than 6e-4 per sector operational hour	Hz 07	MAC-SC4b
SRS 108	The likelihood of ATC failure to detect or resolve a tactical conflict shall be no more than 1e-6 per sector operational hour	Hz 08	MAC-SC3
SRS 109	The likelihood of ATC incorrect trajectory management induces a tactical conflict shall be no more than 1e-6 per sector operational hour	Hz 09	MAC-SC3
SRS 110	The likelihood of Tactical sector configuration change not timely implemented or implemented partially shall be no more than 6e-4 per sector operational hour	Hz 10	MAC-SC4b

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, several workshops were held to address the specific change introduced by the PJ09.44 concept. The first one took place on the 19th of October 2020. This workshop was facilitated by SAF and HP experts from EUROCONTROL and CRIDA and it included concept and validation experts but also Flow Managers. A second set of workshops were then held throughout September and October 2022. These last set of workshops (six in total) were facilitated by SAF experts from EUROCONTROL and it included concept 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 PJ09.44 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 Design safety drivers 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

- 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 to be used in support of the design analysis where not available at the time where this safety assessment had been conducted. Alternatively the structured description of the OSED Use Cases (step-by-step) has been used as a valid alternative

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

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).

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

In the specific case of PJ09.44 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 the initial 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 5 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-S44.W2-SPRINTEROP-IPMS.0090	Uncertainty shall be presented to the DCB actors in the tool used to monitor the evolution of traffic.	Hz 01; Hz 04
REQ-S44.W2-SPRINTEROP-DCBM.0050	INAP shall be able to implement any measure or combination of measures (demand and/or capacity measure(s)) to solve a demand capacity imbalance during its timeframe of operation.	Hz 01; Hz 04
REQ-S44.W2-SPRINTEROP-WHIF.0020	The What-If service shall work in an integrated manner to achieve a seamless DCB process in which the involved actors are able to compare and assess impact and efficiency of different capacity and demand measures proposals for a specific airspace situation	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-WHIF.0030	What-If Tool shall allow at Strategic & Pre-Tactical levels the ANSP ATFCM Unit to find new sectorisation, matching the demand with acceptable level of performance.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-WHIF.0040	What-If Service shall allow automated support for imbalance detection and hotspot/optispot resolution, as far as INAP concept is concerned.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-WHIF.0060	The What-If service shall allow the end user to decide, during the different time horizons, from the Pre-Tactical to Tactical Phase (up to a range of value or discretion for each ACC) what are the measures with higher effectiveness and performance with regards to the resolution of a declared hotspot/optispot.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-WHIF.0070	The What-If service shall support the analysis and resolution to find adequate solutions to complexity situations of traffic.	Hz 01 Hz 03 Hz 04

Safety Requirement ID	Safety Requirement (functionality & performance) description	Related service hazard(s)
REQ-S44.W2-SPRINTEROP-WHIF.0100	The What-if service shall be applicable on the available capacity (predefined acceptable configurations, available configurations based on other constraints, assessment of DAC configurations before their activation on the CWP), by providing the capability of designing a configuration in terms of split, collapse, change of configuration, SAM, flexible boundaries.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-WHIF.0120	The service shall allow the What-If on the traffic demand and trajectory measures such as MCP-Ground Delay, Level-Capping, Horizontal Re-Routing (both at flight and flow levels, ground and airborne).	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-WHIF.0140	What-If service on ATFM Scenarios (Level-capping and Horizontal Rerouting)	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-WHIF.0150	The what-if service shall allow to perform What-If on the application of ATFM Regulations, simulating the impact of different regulation time windows and regulation rates.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-WHIF.0160	The What-If services shall be accessible through an HMI, with functionalities allowing their launch, as well as the presentation of their results.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-WHEL.0010	To resolve a hotspot/optispot imbalance, the What-Else Service shall allow the INAP actors to ask the system for potential alternative solutions to the ones obtained with the What-If service.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-CMPL.0010	The INAP shall be able to select the desired complexity indicator to perform the analysis of the traffic situation, independently of being or not the most appropriate for the timeframe selected.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-CMPL.0020	The INAP shall be able to filter complexity information by traffic flows and individual trajectories.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-CMPL.0030	The INAP shall be able to select specific flights associated to a time interval and airspace volume from the list of aircraft contributing to complexity to assess the individual contribution of each flight to the global complexity value.	Hz 01 Hz 03 Hz 04

Safety Requirement ID	Safety Requirement (functionality & performance) description	Related service hazard(s)
REQ-S44.W2-SPRINTEROP-CMPL.0040	The INAP shall be able to select specific traffic flows associated to a time interval and airspace volume from the list of traffic flows contributing to complexity to assess the individual contribution of each traffic flow to the global complexity value.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-CMPL.0050	The INAP shall be able to select specific flights associated to a traffic flow to assess the individual contribution of each flight to the global traffic flow complexity value.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-CMPL.0060	The INAP shall have access to an automatic identification of the flights contributing the most to complexity within a specific airspace volume and timeframe (e.g. ranked list).	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-CMPL.0070	The INAP shall have access to a detailed analysis of the complexity factors that contribute to the overall airspace complexity.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-CMPL.0080	The INAP should be able to perform Demand and/or capacity what-if analysis in support of managing complexity.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-CMPL.0090	The INAP shall be able to consider complexity assessment within the sector configuration optimisation process.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-CMPL.0100	The INAP shall be alerted when the complexity value is above the established thresholds.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-CMPL.0130	The INAP shall be able to perform capacity what-if assessments for different airspace configurations and airspace granularities in support of managing complexity.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-CMPL.0140	The INAP shall be able to propose airspace sectorisation changes for the optimisation of complexity distribution.	Hz 01 Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-CMPL.0150	The INAP shall have available all the updated information regarding airspace configurations, including airspace availability limitations due to weather or special use of airspace reservations (e.g. events) for complexity assessment purposes.	Hz 01 Hz 03 Hz 04

Safety Requirement ID	Safety Requirement (functionality & performance) description	Related service hazard(s)
REQ-S44.W2-SPRINTEROP-XBRD.0010	Cross Border airspace volumes eligible to be transferred shall be pre-defined.	Hz 01; Hz 04
REQ-S44.W2-SPRINTEROP-XBRD.0020	Rules for Cross Border sectors and delegation of airspace concerning other ATSU (same or different ANSP) shall be defined.	Hz 01; Hz 04
REQ-S44.W2-SPRINTEROP-XBRD.0040	The LTM shall be able to perform DCB within predefined Cross Border configuration using the different tools available, such as what-if and complexity.	Hz 01; Hz 04
REQ-S44.W2-SPRINTEROP-XBRD.0050	INAP shall be able to coordinate with neighbouring INAPs the proposals of Cross Border sector configurations.	Hz 01; Hz 04
REQ-S44.W2-SPRINTEROP-XBRD.0060	The Network Manager shall be aware that a Cross Border operations will take place. Where Cross Border DAC takes place, the NM shall be informed of the configuration and to whom the sectors are delegated.	Hz 01; Hz 04
REQ-S44.W2-SPRINTEROP-XBRD.0070	Local DAC actor shall be able to design the best possible - best fit - configuration, satisfying the complexity and local performance targets considering the number of opened sector and possibility to open Cross Border sectors.	Hz 01; Hz 04
REQ-S44.W2-SPRINTEROP-IER.0320	NM shall disseminate HotSpot and OptiSpot status to AU as soon as they are updated (Creation, cancellation)	Hz 03
REQ-S44.W2-SPRINTEROP-SPOT.0060	INAP shall be able to select and display for a potential hotspot/optispot, all the different parameters related to its calculation: entry counts, occupancy counts, complexity, uncertainty.	Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-IPMS.0050	INAP shall be able to access workload, demand and complexity predictions to monitor their values and know if there are some deviations or changes from initial conditions, not only for new hotspots/optispots but also for existing ones.	Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-STRA.0120	DAC tool shall support a better anticipation of imbalance through all ATM phases supported by an enhanced Predicted Workload with uncertainty assessment	Hz 03 Hz 04

Safety Requirement ID	Safety Requirement (functionality & performance) description	Related service hazard(s)
REQ-S44.W2-SPRINTEROP-STRA.0130	DAC tool shall be able to apply for the Predicted Workload Methodology different criteria according to uncertainty: Entry count, Occupancy Count, Traffic Complexity	Hz 03 Hz 04
REQ-S44.W2-SPRINTEROP-CDMP.0030	INAP shall execute the Collaborative decision making process at tactical phase by using combination of capacity and demand measures from the DCB catalogue and taking into account uncertainty, time horizon, severity and granularity.	Hz 01 Hz 04
REQ-S44.W2-SPRINTEROP-CDMP.0040	At tactical phase, the LTM shall be responsible for the CDM process	Hz 01 Hz 04

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 [12]) 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).

The safety evidence gleaned from the validation exercise is summarized at section 6.

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 PJ09.44 does not introduce any new impact on any Safety Nets other than what was already identified in the SARs of PJ09 [4] and PJ08.01 [3] in SESAR Wave 1.

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 \h [2]** 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 chapter 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 during the HAZID Workshop (held on teams over a series of meetings with the OSED Use Case owners in September 2022 - see Appendix A). 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 5.3.1). 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 (corresponding to the initial design level). 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: Inadequate airspace configuration not fully recoverable via ATFM (demand) measures

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
Local LTM accepts inadequate DAC-DCB solution (sector configurations, DCB measures, ARES allocation and activations) with regards to hotspots resolution	REQ-S44.W2-SPRINTEROP-DCBM.0050 REQ-S44.W2-SPRINTEROP-WHEL.0010 All What-if requirements except for: REQ-S44.W2-SPRINTEROP-WHIF.0010 REQ-S44.W2-SPRINTEROP-WHIF.0080 REQ-S44.W2-SPRINTEROP-WHIF.0110 All complexity-related reqs except for: REQ-S44.W2-SPRINTEROP-CMPL.0110, REQ-S44.W2-SPRINTEROP-CMPL.0120 (post-analysis)	Regarding revised sector configuration or ATFM measures: FMP will continuously monitor imbalance, identify hotspots (supported by hotspot monitoring functionality & alert) and either trigger sector re-configuration or ATFM measures. Additional partial mitigation with PJ09.44: the possibility of interlacing DAC with DCB measures when approaching the regulations cut-off time. Meanwhile if the revision error occurs late, there might be no room for certain sector re-configuration or certain ATFM measures (e.g. Regulation cut-off time is 2 hours) and the only remaining mitigations are certain STAMs or, if relevant, the tactical postponement or cancellation of reserved airspace activation upon ATC request, which could be insufficient to prevent sector overload.
Locally proposed Sector configurations (own unit or cross-border) are inadequate with regards to hotspots resolution	REQ-S44.W2-SPRINTEROP-CMPL.0090 REQ-S44.W2-SPRINTEROP-CMPL.0130 REQ-S44.W2-SPRINTEROP-CMPL.0140 REQ-S44.W2-SPRINTEROP-XBRD.0050 REQ-S44.W2-SPRINTEROP-XBRD.0070	As above

Co-funded by the European Union

Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
Incorrect CDM resulting in undetected impact on airspace volume other than the one affected by the hotspot	REQ-S44.W2-SPRINTEROP-CDMP.0030; REQ-S44.W2-SPRINTEROP-CDMP.0040	As above
Local LTM defines, in response to an optispot, an inadequate DAC-DCB solution (capacity or demand measures) creating an imbalance	REQ-S44.W2-SPRINTEROP-WHEL.0010 All What-if requirements except for: REQ-S44.W2-SPRINTEROP-WHIF.0010 REQ-S44.W2-SPRINTEROP-WHIF.0080 (equivalent to loss of what-if) REQ-S44.W2-SPRINTEROP-WHIF.0110 (performance)	As above

Table 6 Causal Analysis for Hazard 01

5.4.1.2 Hz 03: ATFM measures not designed or not implemented or implemented partially by Local ATFCM

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
Local LTM or NM fails to identify and declare hotspot (including wrong LTM/EAP evaluation of imbalance severities and/or confidence indexes in view of hotspot identification)	REQ-S44.W2-SPRINTEROP-IER.0320 REQ-S44.W2-SPRINTEROP-SPOT.0060 REQ-S44.W2-SPRINTEROP-IPMS.0050	In case local LTM does not identify hotspot, it might be detected at NM level (but that is not systematic). Mitigations from Wave 1 PJ09 thar are relevant for the scope of this Solution: REQ-S44.W2-SPRINTEROP-CMPL.0100: The INAP shall be alerted when the complexity value is above the established thresholds (previously Wave 1 PJ09 REQ-09.01-OSED-CPX.0250) REQ-S44.W2-SPRINTEROP-SAF.0040: The LTM/EAP shall have an access to the information whether complexity calculation is in progress or done (previously Wave 1 PJ09 REQ-09.01-OSED-CPX.0340) REQ-S44.W2-SPRINTEROP-SAF.0050: Training of the LTM/EAP shall consider the evaluation of imbalance severities and/or confidence indexes in view of hotspot identification (previously Wave 1 PJ09 REQ-09.01-OSED-SAF.0004)
Incorrect traffic load data provided to users Change introduced by Sol 44:	No new/changed requirements introduced by Sol 44.	A big corruption in the TMV might be detected by the Local ATFCM due to the expertise in the AoR. REQ-S44.W2-SPRINTEROP-SAF.0020: Training of the LTM/EAP shall consider the selection / modification of the TMV value (previously Wave 1 PJ09 REQ-09.01-OSED-SAF.0003)

Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
Incorrect Traffic monitoring value with regard to complexity/workload		
No complexity available whilst maintaining occupancy and entry counts	REQ-S44.W2-SPRINTEROP-IPMS.0050 REQ-S44.W2-SPRINTEROP-SPOT.0060 REQ-S44.W2-SPRINTEROP-STRA.0120 REQ-S44.W2-SPRINTEROP-STRA.0130 All complexity-related reqs except for: REQ-S44.W2-SPRINTEROP-CMPL.0110, REQ-S44.W2-SPRINTEROP-CMPL.0120 (post-analysis)	Imbalances detected as per current operations based only on Entry and Occupancy Counts. Due to reduced accuracy, some imbalances might be missed.
Wrong result in response to a “what if/else” INAP query	REQ-S44.W2-SPRINTEROP-WHEL.0010 All What-if requirements except for: REQ-S44.W2-SPRINTEROP-WHIF.0010 REQ-S44.W2-SPRINTEROP-WHIF.0080 (equivalent to loss of what-if) REQ-S44.W2-SPRINTEROP-WHIF.0110 (performance)	As the DCB measures apply to flights in the Planning phase, INAP will be able to detect via the hotspot resolution monitoring barrier and timely take appropriate action. Meanwhile, in case what-if/else is used at that moment, if the proposed solution is not correct, this might lead to not resolving the hotspot.
Undetected loss of hotspot resolution status presented to INAP	No new/changed requirements introduced by Sol 44.	The following mitigations might not be effective because potentially affected by the failure: A TMV monitoring&Alert is presented to INAP user in case a hotspot for which a DCB measure has been implemented is not resolved (as per REQ-S44.W2-SPRINTEROP-IPMS.0020, REQ-S44.W2-SPRINTEROP-IPMS.0030 and REQ-S44.W2-SPRINTEROP-IPMS.0040).

Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
		In order to allow early prevention of safety effects in case of undetected loss of functionality: REQ-S44.W2-SPRINTEROP-SAF.0010: The LTM/EAP shall be alerted in case of the loss of the Impacted hotspot resolution status functionality (previously Wave 1 PJ09 REQ-09.02-OSED-SAF.0010)
Planned traffic demand measure wrongly cancelled to address optispot	REQ-S44.W2-SPRINTEROP-WHEL.0010 All What-if requirements except for: REQ-S44.W2-SPRINTEROP-WHIF.0010 REQ-S44.W2-SPRINTEROP-WHIF.0080 (equivalent to loss of what-if) REQ-S44.W2-SPRINTEROP-WHIF.0110 (performance)	LTM will continuously monitor imbalance, identify hotspots (supported by hotspot monitoring functionality & alert) and could trigger a STAM or a sector configuration. Additional partial mitigation with PJ09.44: the possibility of interlacing DAC with DCB measures when approaching the regulations cut-off time. Meanwhile if the cancellation occurs late, there might be no room for certain sector re-configuration or certain ATFM measures with risk of sector overload.

Table 7 Causal Analysis for Hazard 03

5.4.1.3 Hz 04: Inadequate ATFM measure designed and implemented by Local ATFCM

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

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
Local LTM accepts inadequate DAC-DCB solution (sector configurations, DCB measures, ARES allocation and activations) with regards to hotspots resolution	As per Hz01	As per Hz01
Incorrect traffic load data provided to users Change introduced by Sol 44: Incorrect Traffic monitoring value with regard to complexity/workload	As per Hz03	As per Hz03
No complexity available whilst maintaining occupancy and entry counts	As per Hz03	As per Hz03
Incorrect CDM resulting in undetected impact on airspace volume other than the one affected by the hotspot	As per Hz01	As per Hz01
Wrong result in response to a “what if/else” INAP query	As per Hz03	As per Hz03
Undetected loss of hotspot resolution status presented to INAP	As per Hz03	As per Hz03
Wrong hotspot resolution status presented to INAP	No new/changed requirements introduced by Sol 44.	Gross errors might be detectable by the EAP (using their better SA wrt their sub-set sector group) and acted upon, depending on the time-frame.

Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
INAP fails to monitor Hotspot resolution (based on correct Target Deviation Indicator and Impacted hotspot resolution status) or to manage the residual imbalance by taking additional STAM	No new/changed requirements introduced by Sol 44.	Some errors might be detectable by the EAP (using their better SA wrt their sub-set sector group) and acted upon, depending on the time-frame.
Local LTM defines, in response to an optispot, an inadequate DAC-DCB solution (capacity or demand measures) creating an imbalance	As per Hz01	As per Hz01
Targeted CASA Flow Regulation inadequately designed	No new/changed requirements introduced by Sol 44	LTM will continuously monitor imbalance, identify hotspots (supported by hotspot monitoring functionality&alert) and could trigger a STAM or a sector configuration. Additional partial mitigation with PJ09.44: the possibility of interlacing DAC with DCB measures when approaching the regulations cut-off time. Meanwhile if the measure is designed late, there might be no room for certain sector re-configuration or certain ATFM measures with risk of sector overload.

Table 8 Causal Analysis for Hazard 04

5.4.2 Safety Requirements at design level addressing internal system failures

This section is intended for deriving 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).

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, no new safety requirements have been derived, in addition to the safety requirements already identified for normal and abnormal conditions or the safety requirements derived in Wave 1 PJ09 for mitigating the hazards (the IDs of the previous Wave 1 PJ09 requirements have been updated, whilst keeping in brackets the reference to the previous ID).

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 developed in different workshops 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, SAF/HP workshops 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. This is particularly true for the development of the DAC tool (e.g., based on Software and/or hardware assurance level).

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 4 of this document.

6 Demonstration of Service specification achievability

The safety-relevant validation results of the PJ09.44 exercises (documented in the PJ09.44 validation report VALR [12]) are summarized in Table 9 below, whilst indicating for each SRS that has been covered the level of safety evidence that has been obtained.

Exercise ID, Name, Objective	Exercise Safety Validation objective	Success criterion	SRS coverage	Validation results & Level of safety evidence
EXE 01: RTS led by CRIDA/ENAIRE looking at the tactical DCB processes integrating DAC and DCB. Imbalances were analysed based on complexity assessment. The exercise was based on a FRA environment over Flight Level 245 in en-route Spanish airspace Madrid ACC.	**EXE1-OBJ-PJ09W2S44-V3-VALP.016:** To investigate the impact on safety of the dynamic airspace configurations integrated with INAP concept	**EXE1-CRT-PJ09W2S44-V3-VALP-016-001** Safety is maintained compared to reference scenario, despite the traffic increase brought in by the dynamic airspace configurations integrated with INAP solution	**SRS 001** **SRS 002** **SRS 003**	Safety is maintained compared to reference scenario, despite the traffic increase brought in by the dynamic airspace configurations integrated with INAP solution *Meanwhile, it is worth mentioning that there is room for visualization improvements that allows the LTM to get the best solution efficiently and in a timely manner (to avoid confusion with all the possible sector combinations)
EXE 02: RTS led by ECTL looking simulating the full DAC process from the planning phase up to the execution phase in a seamless process. This will be achieved through the integration of ECTL's INNOVE ATFCM platform and ESCAPE ATC real time simulation platform. In addition the PANSA's CAT prototype tool, and AIRBUS WOC ASM tool are used. The initial scope has been reduced to the validation of the extension of the DAC and DCB planning process from D-1 to D-Ops (-3hours) at local and network level	Not safety relevant (planning phase Dops – 3Hrs)			
EXE 03: RTS led by DSNA looking at the what-if tool aiming to ease the choice of a (or several) DCB measure(s) (including a what if flight exclusion tool). It also aims at achieving the full integration of DAC into DCB in tactical	**EX3-OBJ-PJ09W2S44-V3-VALP.027-001** To assess whether safety standards remain the same.	**EX3- CRT-PJ09W2S44-V3-VALP-027-001** Safety is not degraded (at least, a better workload	**SRS 001** **SRS 002** **SRS 003** **SRS 005** **SRS 006**	It was demonstrated that the solution did not suppose any degradation of the operational safety, maintaining that in an adequate level. The related evidence was mainly based on measuring common situation awareness which increased;

phase and includes cross-border coordination.		distribution) and common situation awareness may be increased		better regulation impacts on capacity were observed.
EXE 04: RTS led by NATS looking to validate the application of the Dynamic Airspace Configurations (DAC) functionalities and concepts at local level within the early-mid INAP phase of the day of operation	No safety-dedicated safety validation objective, but all following ones are safety-related: **EX4-OBJ-PJ09W2S44-V3-VALP-005, -006, -007, -009, -010, -011, -014 -015**	Each validation objective investigate the ability of the user to perform DCB whilst minimizing risk of overload (i.e. safety risk), be it from a tool support perspective or from understanding the situation, finding hotspots and solving through either capacity, or demand solutions or combination of the two.	**SRS 001 SRS 002 SRS 003 SRS 004**	The exercise covered the day of operation planning-for-tactical from 4 Hrs to 2 Hrs. The answers to the validation objectives were predominantly OK or POK, showing that the support the tool gave to the user was good, the users were able to use it and for the most part were situationally aware. With respect to ARES (DMA's did not feature in the exercise), the users found the tool particularly useful in understanding the impact of closing a piece of airspace for Mil activity. Meanwhile the functionality within the tool was used more for the optimisation of ARES, i.e. when is the least impactful time to open a Special Use Area (SUA) and then dealing with the residual penetrating flights through demand measures. The conclusion is that the LTM situational awareness, capability to timely identify and resolve hotspots are sufficient for ensuring a safe DAC and DCB process. There are some comments about the amount of data shown on one of the screens, related to too many sectors to monitor, this is something that is planned to be addressed in a later stage of research. Moreover, the tool support needs to be made more efficient to reduce workload in performing tasks. Some thought needs to be made as to how situational awareness of the user can be improved.
EXE 05: RTS led by ENAV in a FRA env in Milan ACC, looking to continue SESAR 2020 Wave 1 validation activities carried out in PJ08.01 on DAC concept and in PJ09.02.03 on DCB concept, now combining the two concepts in a seamless process from the planning phase up to the execution phase, covering	**EX5-OBJ-PJ09W2S44-V3-VALP-007** To demonstrate that the actors involved in DAC sector design and configuration process are able to acquire the	**EX5-CRT-PJ09W2S44-V3-VALP-007-001**	**SRS 001 SRS 002 SRS 003**	Although Safety not assessed as such, some safety-relevant conclusions have been obtained through assessing the situation awareness of FMPs and ATCOs. The LTLLMT tool provided to LTM users the needed information to do the task with an acceptable workload and maintaining the situation awareness, hence

the gap between ATFCM and ATC activities.	due situational awareness to efficiently perform their tasks when DAC en-route ATC sector design principles are put in place.	Actors' decision-making process (when DAC en-route ATC sector design principles are put in place) results in the selection of the sector design and configuration options that best fits the pre-defined design and configuration criteria.		enabling a safe DAC and DCB process. The participant FMPs recommended to enhance the LTLM tool by including other demand measures (Level capping, Rerouting) in addition to the Ground Delay measures and by enhancing the "What-if" with new functionalities to acquire and manage additional airspace and ATC constraints impacting the user workspace and taking into account the actual airspace availability
EXE 06: RTS led by COOPANS and will use a simulation platform integrating both DAC and DCB, allowing the involved actors to detect, manage and monitor local imbalances, with the adoption of the most appropriate measures. It will supervise workload and complexity within defined airspace volumes of Zagreb/Vienna ACC, avoiding as much as possible complexity situations and/or proposing adequate solutions to complexity issues derived from the assessment performed.	**EX6-OBJ-PJ09W2S44-V3-VALP-011** Provide evidence of the ability of an automated system supporting the LTM to assess the identified imbalances based on complexity and/or entry counts and/or occupancy prediction, including the effect of capacity and / or demand measures, to solve an imbalance	**EX6-CRT-PJ09W2S44-V3-VALP-011-003** There is evidence that the level of operational safety is maintained and not negatively impacted under DAC compared to current operations	**SRS 001** **SRS 002**	According to interview and questionnaire results, LTMs agree there was no negative impact and operational safety was maintained under DAC compared to current operations. *Note (imputable to the prototype used): There were no issues related to safety, but on the other hand the system is still not mature enough. Sometimes it hindered the LTMs to have the correct information
EXE 07: RTS led by PANSA and will tackle the management of incoming traffic thanks to an optimized configuration and/or re-allocation of staff at tactical level. To this goal, a new system was developed in order to integrate traffic and airspace information, as well as ATCO availability and rostering rules. The tool was used as a decision supporting tool for the ACC SUPs and LTMs. Beyond usual ATFCM measure application, when a simple short term measure is not enough to resolve a bottleneck, the optimization of the available staff to open the most efficient configuration according to	**OBJ-PJ09W2S44-V3-VALP.026** To investigate the impact on safety of the dynamic airspace configurations integrated with INAP concept	**CRT-PJ09W2S44-V3-VALP-026-001** Safety is maintained compared to reference scenario, despite the traffic increase brought in by the dynamic airspace configurations integrated with INAP solution	**SRS 001** **SRS 002** **SRS 003**	The usage of the prototype did not induce a higher workload for the users and did not incur additional safety risks. On the contrary, as the situation awareness of the actors was increased due to the additional information, and some time savings could be observed, these elements support to increase the level of safety

traffic demand, spread over two ACCs will strive for a new modern way of managing the air traffic flows.				

Table 9. PJ09.44 exercises safety validation objectives, success criteria & Validation results

Conclusion:

The level of safety with the Solution has been assessed qualitatively in validation exercises (RTS) via debriefing with participating LTMs (and EAPs where applicable) and/or assessment of LTM & EAP situation awareness. A negative safety feeling or a degraded situation awareness of the LTM and/or EAP are interpreted as an increased potential for occurrence of sector overloads.

The EXE 02 did not provide safety evidence as its scope was focused on the day of operation planning phase: Dops-3 Hrs.

7 Acronyms and Terminology

Acronym	Definition
A/G	Air / Ground
AB	Airspace Block
ACC	Area Control Center
AI	Artificial Intelligence
ADS-B	Automatic Dependent Surveillance-Broadcast
ANSP	Air Navigation Service Provider
AMC	Airspace Management Cell
AoR	Area of Responsibility
AOP	Airport Operating Plan
APOC	Airport Operations Centre
APW	Area Proximity Warning
ARES	Airspace Reservation /Restriction
ASM	Airspace Management
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATF(C)M	Air Traffic Flow (and Capacity) Management
ATM	Air Traffic Management
ATS(U)	Air Traffic Services (Unit)
AIXM	Aeronautical Information Exchange Model
AIM MAC	Accident Incident Model Mid Air Collision
ADEXP	ATS Data Exchange Presentation
AU	Airspace Users
B2B	Business to Business
CAP	Capacity
CB	Cumulonimbus (Storm Clouds impacting safety)
CDM	Collaborative Decision Making
CDR	Conditional Route
CD/R	Conflict Detection & Resolution
CNS	Communication Navigation and Surveillance

CASA	Computer-Assisted Slot Allocation
CACD	Central Airspace and Capacity Database
CONOPS	Concept of Operations
CTOT	Calculated Take-off Time
CS	Collapsed Sector
CWP	Controller Working Position
DAC	Dynamic Airspace Configuration
DCB	Demand & Capacity Balancing
DDR	Demand Data Repository
DMA	Dynamic Mobile Area
DCP	NMOC Disaster Contingency Planning
EAP	Extended ATC Planner
EATMA	European ATM Architecture
E-ATMS	European Air Traffic Management System
EC	Executive Controller
ECAC	European Civil Aviation Conference
EAUP	European Airspace Use Plan
EUUP	European Update airspace Use Plan
EDAC	European DAC
EEG	Electroencephalogram
EOBT	Estimated OFF Block Time
ES	Elementary Sector
ER	En-Route
ENV	Environment Database NM
EXE	Executive Controller
EUROCAE	European Organisation for Civil Aviation Equipment
FAB	Functional Airspace Block
FRA	Free Route
FBT	Forecast Business Trajectory
FEFF	Flight Efficiency
FL	Flight Level
FDPS	Flight Data Processing System
FM/P	Flow Manager / Position

FOC	Flight Operations Centre
HEC	Hourly Entry Count
HMI	Human Machine Interface
HLAPB	High Level Airspace Policy Body
HP	Human Performance
Hz	Hazard
HAZID	Hazard Identification
HPAR	Human Performance Assessment Report
INAP	Integrated Network Management and Extended ATC Planning function
INTEROP	Interoperability Requirements
ICAO	International Civil Aviation Organization
IOP	Interoperability
ISA	Instantaneous-Self Assessment
IFR	Instrument Flight Rules
IM	Impact Modifier
KPA	Key Performance Area
KPI	Key Performance Indicator
LCM	Local Capacity Manager
LoA	Letter of Agreement
LTM	Local Traffic Manager
MBT	Military Business Trajectory
MIL	MILitary
MTCD	Medium Term Conflict Detection
MV	Monitoring Value
MTFoO	Max Tolerable Frequency of Occurrence
NM	Network Manager
NMf	Network Management function
NMOC	Network Manager Operations Centre
NOP	Network Operations Plan
NSA	National Supervisory Authorities
NATS	UK ANSP
NWP	Network Position
OC	Occupancy Count

OI	Operational Improvement
OSED	Operational Service and Environment Definition
PAR	Performance Assessment Report
PC / PLN	Planning Controller
PSSA	Preliminary System Safety Assessment
PRED	Predictability
RAD	Route Availability Document
RASCI	Responsible, Accountable, Support, Consulted, Informed
RBT	Reference Business Trajectory
RT	Radio Transmission
RTCA	Radio Technical Commission for Aeronautics
SD	Safety Driver
SAB	Sharable Airspace Block
SAC	Safety Criteria
SAF	Safety
SAM	Sharable Airspace Module
SAR	Safety Assessment Report
SBT	Shared Business Trajectory
SD & C	Sector Design and Configuration
SecAR	Security Assessment Report
SESAR	Single European Sky ATM Research Programme
SID	Standard Instrument Departure
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SMT	Shared Mission Trajectory
SAR	Safety Assessment Report
SVT	Safety Validation Target
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 Measure
STAR	Standard Instrument Arrival
SWIM	System Wide Information Model

STCA	Short Term Conflict Alert
TDF	Traffic Demand Forecast
TMA	Terminal Manoeuvring Area
TMV	Traffic Monitoring Volume
TS	Technical Specification
TTA / TTO	Target Time on Arrival / Target Time Over
VTAM	Virtual Telecommunications Access Method
WOC	Wing Operations Centre
xFL	Exit Flight Level

Table 10: Acronyms

Term	Definition	Source of the definition
AIR-REPORT	A report from an aircraft in flight prepared in conformity with requirements for position, and operational and/or meteorological reporting.	ICAO Annex
Airspace Block (AB)	A primary volume of airspace which has to be configured to build workable Sectors of Control defined as Configured sectors in this concept (CS).	SESAR W1 PJ08 OSED
Airspace Building Block	Elementary volume of modularised airspace (As defined by the appropriate ANSP) that are too small individually for controlling purposes, but instead form the basic constituent parts of a Controlled Airspace Block as part of an optimising process.	SWP 7.2 DOD
Airspace Configuration	Is a pre-defined and coordinated organisation of routes and their associated airspace structures, temporary airspace reservations and ATC sectorisation.	SWP 7.2 DOD
Airspace Reservation (ARES)	Airspace Reservation is a defined volume of airspace temporarily reserved for exclusive or specific use by categories of users.	European Route Network Improvement Plan (ERNIP), Part 3 - The ASM Handbook
Airspace Restriction	Airspace Restriction is a defined volume of airspace within which, variously, activities dangerous to the flight of aircraft may be conducted at specified times (a 'danger area'); or such airspace situated above the land areas or territorial waters of a State, within which the	European Route Network Improvement Plan (ERNIP), Part

	flight of aircraft is restricted in accordance with certain specified conditions (a 'restricted area'); or airspace situated above the land areas or territorial waters of a State, within which the flight of aircraft is prohibited (a 'prohibited area').	3 - The ASM Handbook
Airspace Structure	Airspace Structures are specific portions of airspace designed to accommodate the safe operation of aircraft. In the context of the FUA Concept, "Airspace Structures" include Controlled Airspace, ATS Route, including CDRs, ATC Sectors, Danger Area (D), Restricted Area (R), Prohibited Area (P), Temporary Segregated Area (TSA), Temporary Reserved Area (TRA), Cross-Border Area (CBA).	European Route Network Improvement Plan (ERNIP), Part 3 - The ASM Handbook
Business Trajectory	A 4D trajectory which expresses the business intentions of the user with or without constrains. It includes both ground and airborne segments of the aircraft operation (gate-to-gate) and is built from, and updated with, the most timely and accurate data available.	P11.01.01 Transversal consistency of BT/MT requirements (across WPs) D11.01.01-1 Definition of trajectory requirements for Step 1, including gap analysis, support to standardization report from Airspace Users perspective
Configured Sector	Configured Sector is the Result of the Sector Configuration process. This is the actual airspace a controller will be assigned to provide ATS services	SESAR W1 PJ08 OSED
Computed Take-off Time (CTOT)	An Air Traffic Flow & Capacity Management (ATFCM) departure slot, forming part of an Air Traffic Control (ATC) clearance, which is issued to a flight affected by Network Management regulations. It is defined by a time and tolerance (-5 to +10 minutes) during which period the flight is expected to take-off.	ICAO Doc 7030/4 – EUR D11.01.01-1 Definition of trajectory requirements for Step 1, including gap analysis, support to

		standardization report from Airspace Users perspective
Controlled Airspace Block	A Controlled Airspace Block (replacing the current predefined elementary sectors) is a section of modularized airspace within which a Tactical Air Traffic Controller performs his controlling functions defined as a result of dynamic airspace configuration process. Controlled Airspace Blocks are created as a result of a dynamic airspace configuration process in which each controlled block is an optimised grouping of Airspace Building Blocks under consideration of the forecast traffic pattern and ATCO availability and Safety/Performance metrics. The Controlled Airspace Block forms the elementary size of a "Hotspot Unit."	SWP 7.2 DOD
Collaborative Decision Making (CDM)	Collaborative decision-making (CDM) is defined as a process focused on how to decide on a course of action articulated between two or more community members. Through this process, ATM community members share information related to that decision and agree on and apply the decision-making approach and principles. The overall objective of the process is to improve the performance of the ATM system as a whole while balancing the needs of individual ATM community members. From a military perspective CDM is a process from which all participating parties can gain benefits through the negotiation of proposed options. The negotiation stops either at the moment when all participating parties agree with the result or when they reach a limit in their capability to accept further compromise due to defined priorities.	ICAO Doc 9971 + B4.2 (mil aspects) SESAR 2020 Concept Of Operations Edition 2017
DAC role	DAC role refers to composition of responsibilities for of carrying out of main DAC management related tasks and activities associated with DAC management processes at Local or Sub regional levels which include DAC planning, assessment, negotiation, publication and sharing, decision making and implementation.	SESAR W1 PJ08 OSED
Dynamic mobile area (DMA)	Dynamic mobile area (DMA) is an integral part of the MT described by a 4D data set, where the velocity parameter is equal to zero. DMA constitutes a defined volume of airspace that satisfies specific requirements from different Airspace Users.	SESAR 2020 Concept Of Operations Edition 2017

	There are two types of DMA that have been identified for Step 2: DMA Type 1 is a volume of airspace of defined dimensions as integral part of MT at flexible geographical locations agreed upon a CDM process, satisfying Airspace Users requirements in terms of a time and/or distance constraint parameters from a reference point as specified by AU (e.g. Aerodrome of Departure). DMA Type 2: is a volume of airspace of defined dimensions described as integral part of MT and agreed upon a CDM process, satisfying the Airspace Users requirements.	
Elementary Sector (ES)	ATC workable 3D airspace that can be controlled by ATCO for ATS provision and that cannot be split further down into workable/controllable sector(s)	SESAR W1 PJ08 OSED
Flexible boundaries (FB)	Sector boundaries that can be modified or refined to facilitate / optimise FRA trajectories. It is expected that Flexible boundaries can be facilitated through the use of: - Flexible Drawing Tool. SAM (Sharable airspace module) - smallest, non-workable volume of airspace that can be dynamically attached (belong to) to any neighbouring ES or SAB, used to marginally adapt sector boundaries, i.e. +/-10nm	SESAR W1 PJ08 OSED
Flight Intents/ Flight Intentions	The future aircraft trajectory expressed as a 4-D profile until destination (taking account of aircraft performance, weather, terrain, and ATM service constraints), calculated and “owned” by the aircraft flight management system, and agreed by the pilot.	ICAO Doc 9854
Flight Operation Centre (FOC)	Flight Operation Centre is a part (department, employee) of an Airspace user or a system used by an Airspace user providing FOC services and support like operational control, flight planning, pre-flight briefing, in-flight support and post-flight analyses in accordance to AU’s Operational Manual and Standard Operational Procedures.	P11.01.01 Transversal consistency of BT/MT requirements (across WPs) D11.01.01-1 Definition of trajectory requirements for Step 1, including

		gap analysis, support to standardization report from Airspace Users perspective
Forecast Business Trajectory	4D definition of the trajectory associated with a level of uncertainties which evolved according to the time horizon. The FBT uncertainties are characterised by Time uncertainty, Lateral uncertainty, Vertical uncertainty. The purpose is to elaborate the best predictable 4D Trajectory representation called Forecast Business Trajectory (FBT) using uncertainty modelling and including result on FBT itself. The FBT shall be built from historical data (statistical model) and various database (Airport, AO, …), then the FBT shall be refined all along the timeline based on SBT (2D + schedule or 3D + schedule or 4D profile), and trajectory elements that will be known only at a later stage of the planning process (information on 4D route, Constraints …) FBT will be complemented by prediction algorithms and simulation tools used to anticipate flight intentions which are not yet known at the considered anticipated time (SBT maturity, weather conditions, etc.)	SESAR W1 PJ08 OSED
HotSpot	The HotSpot is a 4D volume (defined in time and space) representing a potential DCB imbalance (not critical as not impairing Safety), identified by ANSP(s) and potentially NM. This imbalance is shared with partners, and ANSPs define solutions, supported by Collaborative Decision Making process and tools (either in strategical and pre-tactical phases, or in tactical phase with INAP). A hotspot situation represent a nominal, safety non critical and planned event.	OSED P13.02.03 SESAR1
Imbalance	Imbalance between Demand and Capacity (measured by the occupancy rate in a Controlled Airspace Block)	SESAR W1 PJ08 OSED
INAP Timeframe	INAP covers three main time periods, all referred to the time of occurrence of the hotspot (i.e. 0H): - **From -6H to -2H:** It is assumed that -2H is the cut-off time for CASA application, so this implies that most of the flights are still on ground,	OSED PJ.09-W2-44

	- **From -2H to -40':** This period represents the gap that INAP is filling in the DCB process, - **From -40' to -15':** In this period small adjustments are possible to optimise capacity without a safety issue. ***IMPORTANT NOTICE*** The figures provided are indicative and can slightly differ from one ACC to another, depending of the sector configurations. It should be up to INAP actors to adjust local time periods. To ease readiness of the document, 6hours and 15 minutes will commonly be used as reference in the following sections.	
Models A & B (DAC Management Process)	There are two main DAC management process models that are covered by this OSED: centralised and distributed DAC management models: Model A "Partially Distributed DAC Management Model" and Model B "Fully Distributed DAC Management Model" that are described below. Model A is the "top down" DAC management model characterised by leading role of Network Manager who is kicking off, coordinating and monitoring the DAC planning process with local actors (at national or sub-regional level depending on local organisation) assisting NM with local expertise, data and knowledge. Model B is "bottom-up" DAC management model characterised by leading role of local actors (at national or sub-regional level depending on local organisation) in DAC management process.	OSED PJ08 W1
netLoad	The Network Load (netLoad) is an indicator developed to determine the severity of areas within the network, looking at the propagation of imbalances to non-nominal and critical areas from a network point of view.	OSED PJ.09-W2-49
netSpot	The Network Spot (netSpot) is a captured geographical area that includes linked airspace clusters predicted to be in non-nominal or critical states. The netSpot represents a reference for all concerned actors and stakeholders indicating that: - a congestion is propagating at the network level moving to a non nominal or critical situations, - a global strategy will be coordinated and implemented to resolve it.	OSED PJ.09-W2-49

Network Operations Plan (NOP)	[NOP consists of]: a set of information and actions derived and reached collaboratively both relevant to, and serving as a reference for, the management of the Pan-European network in different timeframes for all ATM stakeholders, which includes, but is not limited to, targets, objectives, how to achieve them, anticipated impact. The NOP has a dynamic and rolling lifecycle starting in the strategic phase and progressively updated up to and including the execution and post-operations phases. It supports and reflects the result of the collaborative ATM planning process: at each phase, stakeholders collaborate at developing a common view of the planned network situation, allowing each of them to take informed decisions considering the network effect and the Network Manager to ensure the overall coordination of individual decisions needed to support network performance.	SWP 7.2 DOD
OptiSpot	The OptiSpot is a 4D volume (defined in time and space) representing a traffic situation where opportunity for optimization has been identified by ANSP (INAP). An ATFCM situation yet to be optimized represents a nominal, safe and planned event.	OSED PJ09 W1
Revision of the Reference Business or Mission Trajectory	The revision of the Reference Business or Mission Trajectory (RBT/RMT) is triggered at Controller or Flight crew initiative when there is the need to change the route and/or altitude constraints and/or time constraints, mainly due to hazards (traffic, weather), fine sequencing (CTA or CTO allocation) or inability for the aircraft system to meet a constraint (CTA missed).	SESAR 2020 Concept Of Operations Edition 2017
Shareable Airspace Block (SAB)	non-workable volume of airspace that can be dynamically configured (Attached) in a pre-defined way to any adjacent Elementary Sector (ES) or Airspace Block (AB) to build Configured Sectors (CS)	SESAR W1 PJ08 OSED
SAM (Sharable airspace module)	smallest, non-workable volume of airspace that can be dynamically attached (belong to) to any neighbouring ES or SAB, used to marginally adapt sector boundaries, i.e. +/- 10nm	SESAR W1 PJ08 OSED
Shared Business/Mission Trajectory	Published Business/Mission trajectory that is available for collaborative ATM planning purposes. The refinement of the SBT/SMT is an iterative process.	ATM Lexicon

Reference Business/Mission Trajectory	The business/mission trajectory which the airspace user agrees to fly and the ANSP and Airports agree to facilitate (subject to separation provision).	ATM Lexicon SESAR Integrated Dictionary
Vertical Sharable Airspace Module (VSAMS)	Non workable volumes of airspace vertically split in 1000ft segments which must be configured with a minimum number of VSAMS to create a CS.	
Wing Operations Centre	The WOC is a generic term, which gathers the operational processes and services directly related to the airspace users and linked to Mission Trajectories and other aerial activities. This definition avoids detailing the diverse organisational structures existing in Europe. It is the Military equivalent to the civil Flight Operations Centre (FOC)	P11.01.01 Transversal consistency of BT/MT requirements (across WPs) D11.01.01-1 Definition of trajectory requirements for Step 1, including gap analysis, support to standardization report from Airspace Users perspective
What-if tools	„What-If“ re-routing simulations allow selecting a single flight and perform re-route trials using flight route alternatives provided by the system, so that the delay imposed on this single flight is minimized and there is no overload on the traffic volumes crossed by the re-route flight. The system automatically provides the benefit and overload, and also automatically calculates and displays the EET and route length differences between the original flight route and the provided flight route alternatives.	SESAR W1 PJ08 OSED

Table 11: Glossary of terms

8 References

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

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

[3] SESAR Solution 08.01 SPR-INTEROP-OSED for V2 – Part II – Safety Assessment Report, Ed. 00.01.00, 5 July 2019

[4] SESAR Solution 09 SPR-INTEROP-OSED for V2 – Part II – Safety Assessment Report, Ed. 00.01.00, 10 September 2019

[5] SESAR Solution 08.01 SPR-INTEROP-OSED for V2 – Part I, Ed. 03.00.01, 8 July 2019

[6] SESAR Solution 09 SPR-INTEROP-OSED for V2 – Part I, Ed. 00.02.01, 3 June 2019

[7] SESAR Solution 09-W2-44 SPR-INTEROP/OSED for V3 – Part I, Ed. 00.01.05, September 2022

[8] Guidance to apply SESAR Safety Reference Material, Ed. 00.03.01, 14 December 2018

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

[10] NM Airspace Data Service Specification, Ed. 5.2, 13/07/2022

[11] NM Flow and Capacity Management Service Specification, Ed. 7.3, 13/07/2022

[12] SESAR Solution 44 – Intermediate VALR for V3, Ed. 00.00.02, 19 May 2022

Appendix A Risk assessment of the change at service level

This appendix presents the results of the risk assessment done at the service specification level, including service hazards identification and assessment in view of deriving additional SRS.

A.1 HAZID workshop

The following HAZID has taken place in September 2022 over a number of one to one meetings with the OSED Use Case experts via TEAMS.

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
DCB-UC-00: Coordination and publication of Optimal Network DCB scenario **DCB-UC-10:** Change of DCB plan and its publication update	Local LTM accepts inadequate DAC-DCB solution (sector configurations, DCB measures, ARES allocation and activations) with regards to hotspots resolution Newly introduced DCB measures (Targeted CASA regulations). DAC measures interlaced with DCB measures. Origin of the cause (new/changed reqs only): - REQ-S44.W2-SPRINTEROP-IPMS.0090: Uncertainty - REQ-S44.W2-SPRINTEROP-DCBM.0050: DCB measures - All What-if reqs, except for: REQ-S44.W2-SPRINTEROP-WHIF.0010, REQ-S44.W2-SPRINTEROP-WHIF.0080 (equivalent to loss of what-if), REQ-S44.W2-SPRINTEROP-WHIF.0110 (performance); - REQ-S44.W2-SPRINTEROP-WHEL.0010; - All complexity-related reqs except for: REQ-S44.W2-SPRINTEROP-CMPL.0110, REQ-S44.W2-SPRINTEROP-CMPL.0120 (post-analysis);	Human error System error (at FMP or AMC) not detected by NM during the NM-Local coordination of the modification of sectors configuration or of ATFCM measures Note: Too late change request will be rejected (requirements on tools and on procedures)	Final sector configuration or revised ATFM measures to be included in the latest published EDAC is inadequate (hotspot not resolved).	Regarding revised sector configuration or ATFM measures: FMP will continuously monitor imbalance, identify hotspots (supported by hotspot monitoring functionality&alert) and either trigger sector re-configuration or ATFM measures. Additional partial mitigation with PJ09.44: the possibility of interlacing DAC with DCB measures when approaching the regulations cut-off time. Meanwhile if the revision error occurs late, there might be no room for certain sector re-configuration or certain ATFM measures (e.g. Regulation cut-off time is 2 hours) and the only remaining mitigations are certain STAM or, if relevant, the tactical postponement or cancellation of reserved airspace activation upon ATC	Inadequate airspace configuration not fully recoverable via ATFM (demand) measures **Hz 04:** Inadequate ATFM measure designed and implemented by Local ATFCM	MAC-SC4b IM=10 MAC-SC4b IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
	- REQ-S44.W2-SPRINTEROP-XBRD.0010; REQ-S44.W2-SPRINTEROP-XBRD.0020 (off-line - mitigated via quality assurance and validation processes) - REQ-S44.W2-SPRINTEROP-XBRD.0040 - REQ-S44.W2-SPRINTEROP-XBRD.0050 - REQ-S44.W2-SPRINTEROP-XBRD.0060 (potential for incorrect FPL distribution) - REQ-S44.W2-SPRINTEROP-XBRD.0070			request, which could be insufficient to prevent sector overload.		
	Coordination outcome (counter proposals) between WOC and DAC/ASM is not consistent No new/changed requirements introduced by Sol 44.	Human error Inadequate Procedure Supporting system (data sharing or CDM)	The ARES reservation published via the latest EDAC will not be fully consistent with the one agreed by WOC. Risk of ARES modification not consistent with the latest published EDAC. In case of inconsistent time ARES parameters there is a risk of overload	WOC might detect problem upon receiving ARES modifications published in EDAC. ATC still has the opportunity for ARES revision or cancellation in	**Hz 02:** Inconsistency between the published EDAC and the State airspace user (WOC) ARES temporal parameters leading to sector overload	MAC-SC4a IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
			(e.g. mission arriving earlier or leaving earlier the ARES) In the worst case for DMA*, the inconsistency concerns the DMA spatial parameters in which case the military aircraft will violate the published DMA dimensions *For DMAs, please see the safety assessment of PJ07.40.	the execution phase in case of sector overload The military controller and/or the pilot will tactically ensure separation from the conflicting civil traffic.		
DCB-UC-02: Optimised configurations	Locally proposed Sector configurations (own unit or cross-border) are inadequate with regards to hotspots resolution Origin of the cause (new/changed reqs only): - REQ-S44.W2-SPRINTEROP-CMPL.0090 - REQ-S44.W2-SPRINTEROP-CMPL.0130 - REQ-S44.W2-SPRINTEROP-CMPL.0140	Human error System error (at FMP or AMC) not detected Note: Too late change request will be rejected (requirements on tools and on procedures)	Final sector configuration is inadequate (hotspot not resolved).	FMP will continuously monitor imbalance, identify hotspots and either trigger sector re-configuration or ATFM measures. Additional partial mitigation with PJ09.44: the possibility of interlacing DAC with DCB measures when approaching the regulations cut-off time.	Inadequate airspace configuration not fully recoverable via ATFM (demand) measures	MAC-SC4b IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
	- REQ-S44.W2-SPRINTEROP-XBRD.0050 - REQ-S44.W2-SPRINTEROP-XBRD.0070			Meanwhile if the revision error occurs late, there might be no room for certain sector re-configuration or certain ATFM measures (eg Regulation cut-off time is 2 hours) and the only remaining mitigations are certain STAM or, if relevant, the tactical postponement or cancellation of reserved airspace activation upon ATC request, which could be insufficient to prevent sector overload.		
DCB-UC-03: Imbalance Detection and Spot Declaration during the Tactical Phase	Local LTM or NM fails to identify and declare hotspot Origin of the causes (new/changed reqs only): - REQ-S44.W2-SPRINTEROP-IER.0320 - REQ-S44.W2-SPRINTEROP-SPOT.0060 - REQ-S44.W2-SPRINTEROP-IPMS.0050	LTM system error (potential malfunction of modified software) Human error (e.g. operator omission, potentially from modification of task and HMI)	If a hotspot is not identified, the monitoring of the related imbalance might not be assured correctly. At worst that would result in a **flow measure** not correctly designed or not correctly implemented leading to possible sector overload which might compromise the traffic	In case local LTM does not identify hotspot, it might be detected at NM level (but that is not systematic) Tactical conflict management In case of no complexity and workload available whilst maintaining occupancy and entry counts, imbalances detected as per current operations based only on Entry and Occupancy Counts	**Hz 03:** ATFM measures not designed or not implemented or implemented partially by Local ATFCM	MAC-SC4b IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
		Incorrect complexity or workload values	planning & synchronization tasks (resources are allocated in priority to tactical conflict management tasks e.g. ATCO_PLN helps ATCO_EXE). New: use of complexity and workload, to complement the monitoring values. LTM analysis work is more complex & demanding, however in case of wrong interpretation of additional info (complexity), it comes to a situation comparable to decision based on current occupancy counts (could over protect but never under protect).			

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
			Same effect in case of complexity & workload missing or incorrect If NM does not detect a hotspot, the effect is on performance. This is because the hotspot information is also continusouly checked by the local LTM, which has richer, more accurate local traffic data than NM has.			
	No traffic load data provided to users No new/changed requirements introduced by Sol 44.		Loss (total or partial) of Network predicted imbalances (including workload and complexity indicators). Already coordinated ATFCM measures ("for implementation" status) will be implemented but with no possibility to monitor their implementation.	Addressed as per the current DCP (NMOC Disaster Contingency Planning). Tactical conflict management	**Hz 05:** No traffic load data provided to users	MAC-SC4b IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
			Meanwhile no new ATFCM measures can be designed because no new hotspots can be identified. Detectable degradation of the imbalance prediction (traffic demand differs from the planned "correct" one by more than 10%) Risk for sector overload, might compromise the traffic planning & synchronization tasks (resources are allocated in priority to tactical conflict management tasks e.g. ATCO_PLN helps ATCO_EXE)			
	Incorrect traffic load data provided to users The only changed aspect: Incorrect Traffic monitoring value with regard to complexity/workload		Hotspot might be missed or incorrectly resolved	A big corruption in the TMV might be detected by the Local ATFCM due to the expertise in the AoR Tactical conflict management	**Hz 03:** ATFM measures not designed or not implemented or implemented	MAC-SC4b IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
	No new/changed requirements introduced by Sol 44.				partially by Local ATFCM **Hz 04:** Inadequate ATFM measure designed and implemented by Local ATFCM	MAC-SC4b IM=10
	No complexity available whilst maintaining occupancy and entry counts Origin of the causes (new/changed reqs only): - REQ-S44.W2-SPRINTEROP-IPMS.0050 (modified by workload and complexity) - REQ-S44.W2-SPRINTEROP-SPOT.0060 (modified by workload and complexity) - All complexity-related reqs except for: REQ-S44.W2-SPRINTEROP-CMPL.0110, REQ-S44.W2-SPRINTEROP-CMPL.0120 (post-analysis);		When only traffic and occupancy counts are used (no complexity): The system provides the traffic monitoring values as per the capacity increase enabled by the solution (Thanks to complexity, the load and capacity monitoring function is more accurate, which enables capacity increase (reducing safety buffers wrt to the monitoring values)). In that case ➔ potential for undetected	Imbalances detected as per current operations based only on Entry and Occupancy Counts. Due to reduced accuracy, some imbalances might be missed.	**Hz 03:** ATFM measures not designed or not implemented or implemented partially by Local ATFCM **Hz 04:** Inadequate ATFM measure designed and implemented by Local ATFCM	MAC-SC4b IM=10 MAC-SC4b IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
	- REQ-S44.W2-SPRINTEROP-STRA.0120 (modified by workload and complexity); - REQ-S44.W2-SPRINTEROP-STRA.0130 (modified by workload and complexity).		imbalance or insufficiently resolved hotspot resulting in overload (with level of traffic enabled by the increased capacity)			
	Incorrect CDM resulting in undetected impact on airspace volume other than the one affected by the hotspot Origin of the cause (new/changed reqs only): - REQ-S44.W2-SPRINTEROP-CDMP.0030; - REQ-S44.W2-SPRINTEROP-CDMP.0040		Imbalance generated in airspace volume other than the one affected by the hotspot	FMP will continuously monitor imbalance, identify hotspots (supported by hotspot monitoring functionality&alert) and either trigger sector re-configuration or ATFM measures. Additional partial mitigation with PJ09.44: the possibility of interlacing DAC with DCB measures when approaching the regulations cut-off time. Meanwhile if the revision error occurs late, there might be no room for certain sector re-configuration or certain ATFM measures (eg Regulation cut-off time is 2 hours) and the only	Inadequate airspace configuration not fully recoverable via ATFM (demand) measures **Hz 04:** Inadequate ATFM measure designed and implemented by Local ATFCM	MAC-SC4b IM=10 MAC-SC4b IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
				remaining mitigations are certain STAM or, if relevant, the tactical postponement or cancellation of reserved airspace activation upon ATC request, which could be insufficient to prevent sector overload.		
DCB-UC-04: Spot analysis **DCB-UC-05**: How to choose a DCB measure **DCB-UC-06**: Spot Resolution and monitoring	Loss of "what if/else" tool Origin of the cause (new/changed reqs only): - All What-if reqs, except for: REQ-S44.W2-SPRINTEROP-WHIF.0010, REQ-S44.W2-SPRINTEROP-WHIF.0080 (equivalent to loss of what-if), REQ-S44.W2-SPRINTEROP-WHIF.0110 (performance).	Local ATFCM System failure (potential malfunction of modified software)	Decision without the what-if will be based on less exhaustive information Non-optimal measures, no safety but only performance impact		None	No safety effect
	Wrong result in response to a "what if/else" INAP query Origin of the cause (new/changed reqs only):	Local ATFCM System error (potential malfunction of	The decision based on the wrong what if might not resolve the hotspot with risk for sector overload	As the DCB measures apply to flights in the Planning phase, INAP will be able to detect via the hotspot resolution monitoring barrier and timely	**Hz 03:** ATFM measures not designed or not implemented or implemented	MAC-SC4b IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
	- All What-if reqs, except for: REQ-S44.W2-SPRINTEROP-WHIF.0010, REQ-S44.W2-SPRINTEROP-WHIF.0080 (equivalent to loss of what-if), REQ-S44.W2-SPRINTEROP-WHIF.0110 (performance); - REQ-S44.W2-SPRINTEROP-WHEL.0010.	modified software) Regional ATFCM System error (impact assessment)		take appropriate action. Meanwhile, in case what-if/else is used at that moment, if the proposed solution is not correct, this might lead to not resolving the hotspot.	partially by Local ATFCM **Hz 04:** Inadequate ATFM measure designed and implemented by Local ATFCM	MAC-SC4b IM=10
	Detected loss of the hotspot resolution status presentation to INAP No new/changed requirements introduced by Sol 44.	Local ATFCM System error (potential malfunction of modified software)	Analysis of hotspot resolution will still be possible based on the human expertise and TMVs, provided time is available for that. The effect is on performance rather than safety.		No safety effect	
	Undetected loss of hotspot resolution status presented to INAP	Local ATFCM system error or data corruption (HMI) (potential malfunction of modified software)	Possibility for sector overload.	The following mitigation might not be effective because potentially affected by the failure: A TMV monitoring&Alert is presented to INAP user in case a hotspot for which a DCB measure has	**Hz 03:** ATFM measures not designed or not implemented or implemented partially by Local ATFCM	MAC-SC4b IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
		In order to prevent the occurrence of the un-detected event: Safety requirement for undetected: REQ-S44.W2-SPRINTEROP-SAF.0010: The LTM/EAP shall be alerted in case of the loss of the Impacted hotspot resolution status functionality (previously Wave 1 PJ09 REQ-09.02-OSED-SAF.0010)		been implemented is not resolved (as per REQ-S44.W2-SPRINTEROP-IPMS.0020, REQ-S44.W2-SPRINTEROP-IPMS.0030 and REQ-S44.W2-SPRINTEROP-IPMS.0040). Tactical Conflict Resolution Barrier	**Hz 04:** Inadequate ATFM measure designed and implemented by Local ATFCM	MAC-SC4b IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
	Wrong hotspot resolution status presented to INAP No new/changed requirements introduced by Sol 44.	Local ATFCM system error or data corruption (HMI) (potential malfunction of modified software)	That might not be detected by INAP user, resulting in sector overload.	Gross errors might be detectable by the EAP (using their better SA wrt their sub-set sector group) and acted upon, depending on the time-frame. Otherwise, tactical conflict management barrier.	**Hz 04:** Inadequate ATFM measure designed and implemented by Local ATFCM	MAC-SC4b IM=10
	INAP fails to monitor Hotspot resolution (based on correct Target Deviation Indicator and Impacted hotspot resolution status) or to manage the residual imbalance by taking additional STAM No new/changed requirements introduced by Sol 44.	Human error (fails to detect) - potential change due to modification of task and HMI Human error (define wrong monitoring threshold). Excessive workload - potential change due to	Hotspot might not be solved with the existing measures which would lead to an overload	Some errors might be detectable by the EAP (using their better SA wrt their sub-set sector group) and acted upon, depending on the time-frame. Otherwise, tactical conflict management barrier.	**Hz 04:** Inadequate ATFM measure designed and implemented by Local ATFCM	MAC-SC4b IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
		modification of task and HMI				
DCB-UC-07: What-if flight exclusion tool Note that the What-if exclusion tool is a type of STAM used before the regulation is implemented in order to reduce the number of a/c affected by the regulation Time-frame: 6h to 3h before	Loss of the what-if flight exclusion tool No new/changed requirements introduced by Sol 44.	No safety impact. Impact on performance.	No safety impact. Impact on performance.	No safety impact. Impact on performance.	N/A	N/A

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
	Incorrect/insufficient what-if exclusion tool solution proposed No new/changed requirements introduced by Sol 44.	Human error System error	**In case too many flights are excluded:** No impact on the regulated sector, as these flights will be by-passing the sector anyway. Nevertheless, the What-if exclusion tool may worsen the situation with risk of overload in the upstream (in case of an early descent) or downstream (in case of a late climb) sectors if too many flights are excluded. However this is unlikely because it is expected that the upstream/downstream ATCOs will refuse some What-if exclusions if they see their workload will be too high.	The ATCOs working the upstream/downstream sectors would not accept too many exclusions if it affects their workload (the LTM who proposes the exclusions has to always negotiate with the neighbouring sectors). Additionally, if the LTM who proposed these exclusions realises that what has been planned initially - 3 hours before - (by closely monitoring the development of the hotspots) is not good, s/he will/may change the plan.	No safety impact	

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
			In case too few a/c are excluded from the regulation: The regulation will not be optimised and hotspot will be resolved.			
DCB-UC-08a: Air Traffic Control in an integrated DAC-DCB environment – hotspot Note: This UC involves no change with the SOL 44 (compared to reference PJ09)	Late display of upcoming sectorisation including an imminent ARES activation related to it (if any) No new/changed requirements introduced by Sol 44.	Human error System error Note: ATCO might choose to display or hide the future sector configuration. **Safety Requirement**:	With regards to the imminent ARES activation: the displayed ARES will be timely visible to all the ATCO in the neighbouring sectors >> ATC (civil and military) will be able to manage tactically the situation without safety impact (i.e. ATC workload maintained at acceptable levels) With regards to next sector configuration: Lack of situation awareness in relation to planning and coordination in the configuration to come.	A planning or coordination error would normally be detected and recovered tactically through the tactical conflict resolution barrier.	None **Hz 06:** ATC failure to detect or resolve a pre-tactical conflict **Hz 07:** ATC incorrect planning&coordination induces a conflict	MAC-SC4b MAC-SC4b

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
		notification on CWP about the future sector configuration change (up to ATCO to display/hide the new sectors borders, and the flights concerned by the future sector).	Need sufficient notification time about new configuration to allow build up the new traffic situation (10 min before new DAC activation time according to OSED/UC08a)			
	Late display of upcoming sectorisation No new/changed requirements introduced by Sol 44.	Human error (ATCO or Supervisor) System error Note: ATCO might choose to display or hide the future sector configuration. **Safety Requirement**: notification on CWP about the future sector	With regards to upcoming sector configuration: Lack of situation awareness in relation to planning and coordination in the configuration to come. Need sufficient notification time about new configuration to allow build up the new	A planning or coordination error would normally be detected and recovered tactically through the tactical conflict resolution barrier.	**Hz 06:** ATC failure to detect or resolve a pre-tactical conflict **Hz 07**: ATC incorrect planning&coordination induces a conflict	MAC-SC4b MAC-SC4b

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
		configuration change (up to ATCO to display/hide the new sectors borders, and the flights concerned by the future sector).	traffic situation (10 min before new DAC activation time according to OSED/UC08a)			
	Missing planning conflicts & their resolution No new/changed requirements introduced by Sol 44.	Human error - The task is the same as per current ops (detect & solve entry conflicts through coordination, whilst accounting for sector re-configuration). **Safety requirement:** ATCO need adequate training in relation to the increased number,	Given that more sector re configurations are possible and more frequent, the required coordination with neighbouring sectors (involved in the future sectorisation) becomes more demanding.	A planning or coordination error would normally be detected and recovered tactically through the tactical conflict resolution barrier.	**Hz 06:** ATC failure to detect or resolve a pre-tactical conflict	MAC-SC4b

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
		complexity and frequency of sector re-configurations				
	Insufficient or wrong coordination with respect to transfer of part of area of responsibility No new/changed requirements introduced by Sol 44.	Human error System support failure **Safety requirement:** - ATC systems shall allow ATCO to communicate with the ATCO that are about to accept or transfer part of their area of responsibility during the sectorisation change	In the context of medium-heavy traffic, transferring a sector block from one position to the other might be complex (e.g. insufficient or wrong coordination of part of AoR). Another difficulty is in case of radical DAC configuration change. Might need requirement for stepwise configuration change (not too many changes in parallel; otherwise the Supervisor might lose his awareness and no more be able to support ATCOs when necessary) The DAC/ATFCM actor, supported by the tool, will ensure that the	ATC Collision prevention (with or without STCA)	**Hz 08:** ATC failure to detect or resolve a tactical conflict	MAC-SC3

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
			change in configuration remains feasible and safe			
	ATCO lack (loss) of awareness about the DAC configuration currently in use No new/changed requirements introduced by Sol 44.	•Too frequent changes of configuration •Change occurring at a critical time (e.g. high workload, conflict scenario) •Radical configuration change occurring •ATCO does not notice a minor configuration change	If not mitigated, risk of incorrect planning or even incorrect tactical conflict management resulting in imminent separation infringement	ATC Collision prevention (with or without STCA)	**Hz 08:** ATC failure to detect or resolve a tactical conflict **Hz 09**: ATC incorrect trajectory management induces a tactical conflict	MAC-SC3 MAC-SC3
	Delay a sector configuration change because ATCO is not prepared for it No new/changed requirements introduced by Sol 44.	Human error System support failure **Safety Requirement**: ATC systems shall request ATCO to confirm they are ready to accept	Normally ATCOs will not accept a sector re-configuration until they are ready to execute it. A delay might result in sector overload. Given the transitory character of this degradation, only moderate overload is	Tactical conflict resolution	**Hz 10:** Tactical sector configuration change not timely implemented or implemented partially (hazard existing in current ops but	MAC-SC4b IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
		the new sectorisation before activating the change (see OSED/UC13)	expected (note mainly PLN ATCO impacted, as helping the EXE ATCO will supersede his normal planning activities)		new causes due to PJ08.01)	
	Delayed implementation or display of a Sector configuration change No new/changed requirements introduced by Sol 44.	Human error (Supervisor) – no change System support failure (eg the HZ04: "Internal DAC sharing (system to ATCOs' HMI) incomplete or untimely" from Project 07.05.04: DAC Step 2 within SESAR 1 OFA 05.03.01, 05.03.03 and 03.01.03)	ATCO lack of capability to work with the new configuration (waiting for it to be displayed on CWP). Potential for sector overload Given the transitory character of this degradation, only moderate overload is expected (note mainly PLN ATCO impacted, as helping the EXE ATCO will supersede his normal planning activities)	Tactical conflict resolution	**Hz 10:** Tactical sector configuration change not timely implemented or implemented partially	MAC-SC4b IM=10
	Risk for late assuming an aircraft No new/changed requirements introduced by Sol 44.	No change (ATCO assumes upon Pilot first contact on frequency)	No change needed in the current system		No new (or modified) hazard or hazard cause	

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
	Risk for late transferring an aircraft No new/changed requirements introduced by Sol 44.	ATCO error: Late transfer on frequency (increasing compared to Baseline, in relation to the more demanding sector re configuration) **Safety Requirement**: CWP aids shall present to the controller the flight/s that need to be transferred or assumed during a DAC sectorisation change (see OSED/UC14)	Aircraft will be assumed late, whilst well advanced within the current AoR. Potential for difficulty to resolve tactical conflicts.	ATC Collision prevention (with or without STCA)	**Hz 08:** ATC failure to detect or resolve a tactical conflict (hazard existing in current ops but new causes due to PJ08.01)	MAC-SC3 MAC-SC3
	Risk for transferring to wrong frequency No new/changed requirements introduced by Sol 44.	ATCO error: transfer to wrong frequency, potentially more frequent with the	Aircraft will be assumed late (but not later compared to Baseline situation), whilst well advanced within the	ATC Collision prevention (with or without STCA)	**Hz 08:** ATC failure to detect or resolve a tactical conflict	MAC-SC3 MAC-SC3

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
		more demanding sector re configuration) **Safety Requirement:** System needs additional functionality to support ATCO in instructing the right frequency (on what frequency each aircraft currently is; on what frequency aircraft needs to be transferred; might need CPDLC) – see OSED/UC13: "- The frequency of the sector an aircraft is about to enter is shown to the ATCo X seconds	current AoR. Potential for difficulty to resolve in time tactical conflicts (same effect as per Baseline operations).		(hazards existing in current ops but new causes due to PJ08.01)	

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
		before the aircraft crosses sector boundary and upon request (if needed before)"				
DCB-UC-08b: Air Traffic Control in an integrated DAC-DCB environment - optispot	All the above failure modes apply (no need to be re-assessed here)					
	Local LTM defines, in response to an optispot, an inadequate DAC-DCB solution (capacity or demand measures) creating an imbalance Origin of the cause (new/changed reqs only): - All What-if reqs, except for: REQ-S44.W2-SPRINTEROP-WHIF.0010, REQ-S44.W2-SPRINTEROP-WHIF.0080 (equivalent to loss of what-if), REQ-S44.W2-SPRINTEROP-WHIF.0110 (performance);	LTM human error	Proposed revision of sector configuration or of ATFM measures creates imbalance	Regarding revised sector configuration or ATFM measures: FMP will continuously monitor imbalance, identify hotspots (supported by hotspot monitoring functionality&alert) and either trigger sector re-configuration or ATFM measures. Additional partial mitigation with PJ09.44: the possibility of interlacing DAC with DCB measures when	Inadequate airspace configuration not fully recoverable via ATFM (demand) measures **Hz 04:** Inadequate ATFM measure designed and implemented by Local ATFCM	MAC-SC4b IM=10 MAC-SC4b IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
	- REQ-S44.W2-SPRINTEROP-WHEL.0010.			approaching the regulations cut-off time. Meanwhile if the revision error occurs late, there might be no room for certain sector re-configuration or certain ATFM measures with risk of sector overload.		
	Planned traffic demand measure wrongly cancelled to address optispot Origin of the cause (new/changed reqs only): - All What-if reqs, except for: REQ-S44.W2-SPRINTEROP-WHIF.0010, REQ-S44.W2-SPRINTEROP-WHIF.0080 (equivalent to loss of what-if), REQ-S44.W2-SPRINTEROP-WHIF.0110 (performance); - REQ-S44.W2-SPRINTEROP-WHEL.0010.	LTM human error System error (potential malfunction of modified software)	Cancellation of planned traffic demand measure creates imbalance	FMP will continuously monitor imbalance, identify hotspots (supported by hotspot monitoring functionality&alert) and could trigger a STAM or a sector configuration. Additional partial mitigation with PJ09.44: the possibility of interlacing DAC with DCB measures when approaching the regulations cut-off time. Meanwhile if the cancellation occurs late, there might be no room for certain sector re-configuration or certain ATFM measures with risk of sector overload.	**Hz 03:** ATFM measures not designed or not implemented or implemented partially by Local ATFCM	MAC-SC4b IM=10

Use Case	E	E	Operational effect	Mitigations protecting against propagation of effects	Service hazard	Severity
DCB-UC-09: Target flow CASA	Targeted CASA Flow Regulation inadequately designed No new/changed requirements introduced by Sol 44.	LTM human error System error (potential malfunction of modified software)	Wrongly designed targeted CASA regulation not adequate for hotspot resolution	FMP will continuously monitor imbalance, identify hotspots (supported by hotspot monitoring functionality&alert) and could trigger a STAM or a sector configuration. Additional partial mitigation with PJ09.44: the possibility of interlacing DAC with DCB measures when approaching the regulations cut-off time. Meanwhile if the measure is designed late, there might be no room for certain sector re-configuration or certain ATFM measures with risk of sector overload.	**Hz 04:** Inadequate ATFM measure designed and implemented by Local ATFCM	MAC-SC4b IM=10
DCB-UC-11: Optimal ARES (DMA) allocation in DAC Pre-Tactical Level	No safety impact because hotspot will be identified and resolved at tactical level					

Table 12. Full HAZID working table

Appendix B Assumptions, Safety Issues & Limitations

B.1 Assumptions log

No specific assumption has been used.

Ref	Assumption	Validation

Table 13: Assumptions log

B.2 Safety Issues log

No specific safety issue has remained unresolved.

Ref	Safety issue	Resolution

Table 14: Safety Issues log

B.3 Operational Limitations log

No operational limitation has been specified.

Ref	Operational Limitations

Table 15: Operational Limitations log

-END OF DOCUMENT-

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