INDUSTRIAL RESEARCH

sesar
JOINT UNDERTAKING

D4.1.004 PJ07-W2-40 SPR-INTEROP/OSED for V3 - Part II - Safety Assessment Report

Deliverable ID:	D4.1.004
Dissemination Level:	PU
Project Acronym:	PJ07-W2-40
Grant:	874465
Call:	H2020-SESAR-2020-2
Topic:	Initial 4D Mission Trajectory development with integrated DMA types 1 and 2 supported by automation and dynamic civil-military CDM
Consortium Coordinator:	EUROCONTROL
Edition Date:	13.02.2022
Edition:	01.00.00
Template Edition:	00.00.04

EUROPEAN PARTNERSHIP

Co-funded by
the European Union

Authoring & Approval

Authors of the document

Beneficiary	Date
ANS CR (B4) - INTEGRA	13.02.2023

Reviewers internal to the project

Beneficiary	Date
EUROCONTROL	10.02.2023
AIRBUS SAS	10.02.2023
PANSA (B4)	10.02.2023
MEPS	10.02.2023

Reviewers external to the project

Beneficiary	Date

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

Beneficiary	Date
EUROCONTROL	13.02.2023
AIRBUS SAS	13.02.2023
PANSA (B4)	13.02.2023
MEPS	13.02.2023
ANS CR (B4) - INTEGRA	13.02.2023

Rejected By - Representatives of beneficiaries involved in the project

Beneficiary	Date

Document History

Edition	Date	Status	Beneficiary	Justification
00.00.01	15.07.2022	First draft	INTEGRA	New document
00.00.02	29.09.2022	Final draft	INTEGRA	Update after partners review

00.00.03	07.10.2022	Final draft	INTEGRA	For submission
00.00.04	10.11.2022	Final	INTEGRA	Update after SJU review
01.00.00	13.02.2023	For submission	INTEGRA	Update to Ed. 01.00.00 taking into account MG event actions – Approved by S3JU

OAUO

INITIAL 4D MISSION TRAJECTORY DEVELOPMENT WITH INTEGRATED DMA TYPES 1 AND 2 SUPPORTED BY AUTOMATION AND DYNAMIC CIVIL-MILITARY CDM

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

Abstract

This document specifies the results of the safety assessments carried out in SESAR 2020 Wave 2 by Project PJ07-Solution 40 -Initial 4D Mission Trajectory development with integrated DMA types 1 and 2 supported by automation and dynamic civil-military CDM.

This Safety Assessment Report (SAR) is contributing to the /Safety and Performance Requirements (SPR) - Interoperability (INTEROP) / Operational Service and Environment Definition (OSED) and Technical Specifications (TS)/Interface Requirement Specification (IRS) documents.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Table of Contents

List of Tables

1 Executive Summary

This document contains the Specimen Safety Assessment Report for an application of the PJ07-W2-40 Initial 4D Mission Trajectory development with integrated DMA types 1 and 2 supported by automation and dynamic civil-military CDM.

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

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 PJ07.W-2-40 Solution SPR-INTEROP/OSED and TS/IRS.

2 Introduction

2.1 Background

Solution PJ07-W2-40 validation builds upon the results delivered by SESAR 1 - P7.6.2 (Business and Mission Trajectory), P7.5.4 (Advanced Flexible Use of Airspace), SWP11.1 (WOC), and SESAR 2020 Wave1 - PJ.07-03/PJ.18-01a (Mission Trajectory Driven Processes), and PJ.08-01 (Management of Dynamic Airspace Configurations supporting DMAs type 1 and 2).

SESAR 1 relevant achievements:

- WOC - State Airspace User processes, V2 maturity [5]
- Participation of the WOC in the ARES CDM process, V2 maturity [6]
- DMA type 1 and type 2 configuration in Free Route Area operations, V2 maturity

SESAR 2020 Wave 1 relevant achievements:

- Mission Trajectory management
    - The initial V3 validation of VPA design type of ARES management in WOC, NM and ATC systems and processes. That included the evolutions of the VPA module reference as integral part of the evolved iOAT FPL syntax & concept
    - The initial V3 validation of iOAT FPL (technical mean and mechanism to describe and share MT) processing by IFPS/NM and distribution to relevant local ATM actors, including the supporting B2B services [8].
    - The feasibility of the technical capability to process the MT/iOAT FPLs in the subsequent ATFM systems of NM and ATC/FMP; i.e. ETFMS and TCM/CHMI
- Management of Dynamic Airspace Configurations (DAC) with DMA type1 and type2:
    - The V2 maturity level of DMA type 1 and 2 management in DAC and FRA operational environment [9].

2.2 General Approach to Safety Assessment

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

- a success approach which is concerned with the safety of the Solution service provision in the absence of failure within the end-to-end Solution Functional System, encompassing both Normal operation and Abnormal conditions,

- a conventional failure approach which is concerned with the safety of the Solution service provision in the event of failures within the end-to-end Solution Functional System.

These two approaches are applied to the derivation of safety properties at each of the successive lifecycle stages V2 and V3 of the Solution development (Safety Requirements at service level and at design level).

Co-funded by the European Union

From a safety assessment perspective, this safety assessment is considered as Other than ATS operational solution, meaning that the change affects the services delivered to ATS providers, other service providers or aviation undertakings (the WHAT and the HOW). The design safety driver is the specification of the changed service limited to the potential safety implication on the side of the ATS service provider or aviation undertaking (e.g. airline) using that service. Solution PJ07-W2-40 addresses the planning processes and procedures for integrated definition and development of iMT with DMA type 1 and type 2 and iSMT revision at national/sub-regional level. Therefore, the change brought by the solution does not affect directly ATS services (no direct impact on the way ATCOs and Pilots act, interact and make use of tools/equipment in view of delivering ATS), but rather focuses on the planning phase of the management of the integrated civil-military ATM demand – therefore, services delivered to civil and military AU and ANSPs prior to the execution phase.

2.3 Scope of the Safety Assessment

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

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

- V1 - through initial identification of safety implications of the Change and the definition of Safety drivers (fully covered within this document and in the Safety Plan)
- V2: e.g. safety specification at operational service level (mainly establishing Safety Requirements at Service level- SRS), safe initial design (mainly deriving Safety Requirements at initial design level -iSRD to be documented as appropriate in SPR-INTEROP/OSED and TS/IRS),
- V3: e.g. safe refined design (a second iteration of the process conducted at the safe initial design level, mainly deriving Safety Requirements at refined design level – rSRD to be documented as appropriate in SPR-INTEROP/OSED and TS/IRS).

Since the properties of the operational environment are crucial to the safety assessment, this process cannot be generic. The process is executed specifically for the operational environment defined in section 3.2 and consequently the term ‘specimen’ safety assessment should be used.

2.4 Layout of the Document

Section 1 presents the executive summary of the document

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

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

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

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

Section 6 demonstrate the achievability of safety requirements.

Section 7 lists Acronyms used in the document.

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

Appendix A describes the process of defining the Service Safety Specification for Normal and Abnormal conditions of operation

Appendix B Presents the details of Hazid workshop

Appendix C presents the consolidated list Safety Requirements at design level for Normal and Abnormal conditions of operation.

Appendix D presents the consolidated list Safety Requirements at design level for protective mitigation.

3 Setting the Scene of the safety assessment

3.1 Operational concept overview and scope of the change

PJ.07-W2-Sol.40 is further addressing Research and Development (R&D) needs related to MT with DMA type 1 and 2 management integrated military ATM demand from SESAR 2020 Wave1. MT management needs were validated partially V3 in PJ07-03, while DMA type 1 and 2 management in Dynamic Airspace Configuration (DAC) was validated V2 in PJ08.01. By achieving its objectives, the solution expects to bring benefits, mainly to the key ATM performance areas of environment (generated by gains to operational efficiency in terms of fuel, trajectory, and time efficiency), airspace capacity, flexibility, and civil-military cooperation and coordination while improving/maintaining the mission effectiveness.

The solution refines, integrates and further validates concept elements of MT, AFUA (DMA type 1 and type 2) and AASM (DAC), by addressing management of the integrated military ATM demand (iMT with DMA type 1 and type 2) at sub-regional/local level in the ATM medium to short term planning phase, specifically:

- definition and development of Early Flight Intent (EFI) with DMA type 1 and type 2
- management of iSMT with integrated DMA type 1 and type 2 with planning ATM constraint (Target Time Over - TTO).

The following improvement steps define the operational scope of the Solution subject to validation:

- AUO 0210: Participation in CDM through iSMT and Target Time (TTO) negotiation
- AOM 0304 B: Integrated management of Mission Trajectory in Trajectory Based Operations
- AOM 0208 B: Dynamic Mobile Areas (DMA) of types 1 and 2
- AUO 0216: Shared Mission Trajectory Data.

3.2 Solution Operational Environment and Key Properties

For the detail of the operational environment please refer to the part I of the SPR-INTEROP/OSED section 3.2.

3.3 Stakeholders’ expected benefits with potential Safety impact

Taking into consideration that the solution addresses the planning processes and procedures for integrated definition and development of iMT with DMA type 1 and type 2 and iSMT revision at national/sub-regional level, it can be considered as “**Other than ATS operational solution**”. The change brought by the solution does not affect directly ATS services (no direct impact on the way ATCOs and Pilots act, interact and make use of tools/equipment in view of delivering ATS), but rather focuses on the planning phase of the management of the integrated civil-military ATM demand – therefore, services delivered to civil and military AU and ANSPs prior to the execution phase.

3.4 Intended Operational use of the Service Concept

3.4.1 Intended use identified from SESAR Operational Solutions

The main impact of the PJ07-W2-40 solution is identified for the following operational nodes and functions:

- **Sub-regional / National Airspace management (ASM)**

The solution is addressing mainly the sub-regional/national Airspace Manager function of the ASM operational node together with its roles and responsibilities suited to the medium (7 to 1 days prior to execution) to short term (1 day to 1 hour prior to execution) planning phase.

By convention, the "Airspace Manager" refers only to the national function integrated in all Sub-regional ATM Network Management Functions.

The Airspace Manager (AM) is responsible for the medium to short term planning of national and potentially FAB level ASM right up to its operational implementation within European FUA (Flexible Use of Airspace) framework constraints. The AM role may in reality be filled by two actors: The Civil Airspace Manager (CAM) & The Military Airspace Manager (MAM), these actors would then have clear locally defined roles and areas of authority.

The AM task is to manage the competing airspace demands from Civil and Military operations in a pragmatic way, taking account of relevant factors. In the context of DAC, the AM ensures the configuration of airspace structures throughout a CDM process that integrates ATFCM and the military airspace user represented by WOC.

National and Sub-regional actors involved in ASM (WOC, AM) in close coordination with Local/Sub-regional and Regional ATFCM assess the impact of airspace demand and develop solutions in order to optimise network performance on regional, sub-regional, and local levels. This is an iterative and interactive process of validating, developing and refining the forecast that will evolve into a final agreed operational plan promulgated the day before the operations.

The automation of human processes and use of the ASM support tools improves the civil-military CDM process and provides additional features. What-if functionalities increase efficiency in decision making process by providing multiple solutions satisfying operational objectives in terms of demand for the airspace resource in planning and execution phases. The result is an optimised civil-military airspace configuration solution.

While offering greater flexibility to accommodate military operational requirements, NM, ANSP and Airspace Users will benefit from higher availability of CDRs – or available airspace in case of FRA –for flight planning purposes.

In the previous operating method, the ASM function managed predefined ARES configurations in with limited flexibility and dynamicity – some VPA principles may have been applied – in isolation of the trajectory information. The new Solution operating method will introduce a higher degree of flexibility in ARES allocation through the use of DMA Type 1 and connects the airspace allocation request with the development of mission trajectory.

- **Sub-regional / Local Air Traffic Flow and Capacity Management (ATFCM)**

In the scope of the Solution, the ATFCM operational node integrates the functions of flow manager, local capacity manager, and local traffic manager. The key role is to analyse and establish traffic flows and local capacity values for various airspace configurations and to establish measures enabling the balance of traffic demand with DAC accommodation capability.

Sub-regional/Local ATFCM is responsible for DCB and de-confliction of the AU demand in the context of DAC and is involved in the airspace management as a stakeholder.

ATFCM is an iterative process commencing at the long-term planning phase, being refined and detailed during the medium-term planning and short-term planning phase, with corrective actions applied even during the execution phase.

The ATFCM process integrates Local-/Sub-Regional and Regional information into a common shared Demand and Capacity picture. It is a key characteristic that none of the levels/actors work in isolation, but together in an integrated manner.

Demand planning is based on historical data and forecasts concerning traffic demand and airspace use. This planning is progressively detailed and refined with new / updated / more detailed information about flight intentions, as getting closer to operations.

In previous operating method the EFI of the MIL AU was not available and even the more mature MIL trajectories – if made available for the ATFCM function at all – did not include detailed integrated ARES information enabling a holistic CIV-MIL DCB planning. In the Solution operating method this data is available and shared between all relevant stakeholders on local, sub-regional and regional levels.

- Local DAC function

The local DAC is a function, which represents a key operational improvement in SESAR 2020 and which is used by the Solution in order to provide an appropriate operating context for the management of iMT with integrated DMA of types 1 and 2.

Local DAC fulfils a joint civil-military function at national level, which integrates ASM, ATFCM and ATS functionalities and managers so that their processes can be performed in a combined manner allowing for a cooperative management of Airspace Configurations. This function is expected to manage civil/military airspace allocation, flow and capacity management, including sector configuration management role at local/sub-regional level with following relevant responsibilities:

- Develop and deploy Dynamic airspace configurations
- Retrieve from iSMT data related to ARES (VPA, DMA, and Static) and process it in the context of airspace configuration
- Identify civil-military performance indicators to be processed for a specific airspace configuration so that to fulfil at optimal extent local/network performance targets and to fully respond to military mission requirements
- Assess impact of DAC modification on military mission requirements and advise WOC on possible ARES (VPA, DMA, Static) adaptation or modifications where suitable
- Coordinate with civil and military airspace users the implementation of priority rules for a specific airspace situation when and if the problem detected – using "What if" tool to find new ATC sectorisation, matching the demand with acceptable level of performance
- As a result of ARES modification and adaptation to DAC performance expectations such new DMAs, identifies mission trajectories subject to WOC revision in accordance with new/modified DMAs activation parameters
- Make final decision on the DAC planning at local/sub-regional level, concerning sector configuration, hotspots and DMAs

The DAC function does not exist in the previous operating method, where the ASM and ATFCM operational nodes operating with a low level of integration.
The DAC function benefits from an ASM tool, which integrates ATFCM information and provides an automated optimization of airspace structures configuration based on a 'what-if 'capability.

- **State Airspace user operations (WOC)**

The WOC function and respective technical support systems facilitate the military AU operations in planning and execution phase. The WOC function has different implementation dimensions, based on the architecture of the national military organisations. Effectively, for military AU this is a key capability that interfaces with the ATM network and facilitates the trajectory development, sharing, execution, and management.

State Airspace Users are a subgroup of Airspace Users in general, who are involved in airspace planning, reservation and management and usage of airspace on behalf of a state. The level, position and structure, which can accommodate those roles, depend entirely on the State Airspace User. One role can represent several processes in different phases of AU's activities.

The iMT concept explicitly describes WOC as a function that can be distributed amongst different entities with different roles and actors according to national military organisation and infrastructure. In the context of the Solution, WOC function is considered as a single entity responsible for all operational activities and information exchanges between all relevant nodes and stakeholders along all phase of iMT lifecycle.

Due to the shift from ASM to Trajectory management environment in ATM the actors and the roles can change and the number of processes is reduced. This is logical outcome as many of the processes performed by human actors will be delegated to system actors and thus human workload will be reduced (automation is a main SESAR Concept feature).

Relevant to the scope of the Solution is the mission planner function/role of WOC, for which the tasks integrates other relevant roles to planning (e.g. mission scheduler, AIS static data operator. In essence the task of mission planner remains the same in the new operating method as in the previous one, the responsibilities change with the full participation of WOC in the CDM for DAC.

Responsibilities include:

- To receive and analyse the mission request and to plan the request for EFI and the day of operations with the support of the mission support system
- To assess all information available relevant to mission planning, including the ATC volumes provided by the ASM tool and their impacts to the planned mission.
- To provide ASM support to missions requiring ARES/DMA
- To prepare the flight routes and to integrate the DMA into the description of mission trajectories
- To participate in CDM with the local DAC for the optimization of DMA
- To assess the impact of DMA optimization on the effectiveness of route profile and the objectives of the mission

- To decide about the final parameters for DMA allocation/change in accordance with military airspace user operational requirements.

The AU operations services address all the necessary activities to support MIL AU operations throughout the medium and short term planning (trajectory and ARES) and participation to related CDM processes.

The solution offers greater flexibility to accommodate military requirements by defining different airspace scenarios with acceptable network impact through extension or sub-division of military training areas in a flexible and dynamic manner (DMA Types 1 and 2) adjusted to match military training and operational requirements for each type of mission. Additionally, the DMA request – and subsequent allocation – is linked to specific trajectory(ies).

The solution enables the WOC to take advantage of the enhanced flexibility of the ATM system to accommodate military ATM requirements, including short notice requests/changes, in the mission planning phase more dynamically. A civil-military CDM process and supporting interoperable systems are implemented, enabling an iterative process for the refinement of mission trajectories and allocation of DMA. The solution integrates the initial MT information and requirements with DMAs of types 1 and 2 for a more holistic approach to mission planning.

In the current operating method, the WOC defines missions based on the use of static ARES with no or very limited trajectory and flight planning information associated with the ARES request. Limited CDM and stakeholder involvement is associated in the current operating method planning cycle. In the Solution operating method, the static area request is replaced by dynamically defined DMA optimised for mission specific needs and associated with a gradually maturing trajectory in an interactive and iterative process taking advantage of historical, forecast and actual (airspace and flight) demand information.

3.4.2 Other intended use outside-SESAR

- **ANSP (ATC)**

The ANSP can utilise the solution to achieve improved en-route capacity planning process and predictability as a result of improved management of traffic complexity. This is enabled by the flexibility and dynamicity of DMA types 1 and 2 and the integration of the MT into the traffic complexity assessment and mitigation process.

The solution enables for the ANSP to accommodate both civil and military ATM planning constraints and preferences/priorities into the DCB process reconciling civil and military users' needs and facilitates a more complete view of the overall DCB picture on local and sub-regional level.

- **Network Manager**

The solution enables a more effective cooperation between all the stakeholders in moving towards an optimised airspace configuration and improved efficiency of national/regional ASM-ATFCM based CDM and facilitates a more complete view of the overall DCB picture on network / regional level.

3.5 Relevant applicable standards

The applicable standards and regulations are addressed in SPR-INTEROP/OSED Part I section 3.2.6.

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 Solution.

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).

The main safety assurance activities feeding this section are the ones conducted in V2. For Solution PJ07-W2-40 the input here will be derived mainly from the SESAR 2020 Wave 1 by Project PJ08-Solution 01 (Management of Dynamic Airspace Configuration) and refined based on outcomes from the safety assurance activities done in V3.

The design safety driver for "Other than ATS solution" is the specification of the changed service limited to the potential safety implication on the side of the ATS service provider or aviation undertaking (e.g. airline) using that service.

Safety requirements at service level (SRS) are to be placed on the services of the Solution functional system that are changed or affected by the change (through change in behaviour or through new interactions introduced).

SRS for the "Other than ATS solution" might also be identified from relevant Safety Requirements at Service level (SRS) and at Design level (SRD) derived in other SESAR Operational Solutions as well as from any relevant recognized operational or technical standards and/or codes of practice (e.g. EU regulations, PANS-ATM, ICAO Annexes, equipment standards, interoperability requirements).

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– 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 set of Safety Requirements at the Service level (SRS) (functionality&performance) in this section should specify the desired safety behaviour of the change at its interface with the operational context considering normal conditions of operation.

The SRSs (functionality&performance) for normal conditions of operation are derived taking into account:

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

The SRS are derived only in relation to the potential safety implications on the side of the ATS service provider or aviation undertaking using the "Other than ATS" service.

PJ08.01 SESAR wave 1 addressed the design and validation of Dynamic Airspace Configurations (DAC) and Dynamic Mobile Areas (DMAs) of types 1 and 2 in Free Route Airspace (FRA) that enable flexible solutions that can be dynamically adapted to traffic demand to respond to different regional/local performance objectives, which may vary in time and place, up to concept maturity level V2. The scope of the PJ08.01 SAR focused on the medium to short term (including pre-tactical down to last planned/coordinated and published configuration changes) and execution phases. Therefore, some of the SRS derived in the project PJ08.01 SESAR wave 1 (formerly called Safety Objectives – SO) are also relevant within solution PJ07-W2-40.

The design characteristics/items of the Solution functional system should not be considered at this level but at the design level (in section 5.2), when the derived SRSs will enable the derivation of the Safety Requirements at Design level (SRD).

Table 1 provides the consolidated list of the SRS for normal conditions of operation that have been derived through activities described in Appendix A.3.

SRS ID	SRS for Normal conditions of operation
SRS-001	DAC shall be able to evaluate the impact of DMAs request on ATC Volumes via the set of parameters (number of impacted trajectories)
SRS-002	DAC shall be able to simulate and display new airspace configuration.
SRS-003	DAC shall be able to share the proposals of DMA's changes with WOC.
SRS-004	DAC shall be able to compare potential impact of DMAs localisation on traffic rerouting.
SRS-005	DAC shall be able to simulate and assess (against complexity parameters) the new configuration of airspace structure with DMAs.

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

4.3 Service Safety specification - Abnormal conditions of operation

The purpose of this section is to present the Safety Requirements at Service level (SRS) derived for Abnormal conditions of operation. Appendix A.4 provides more detail about the impact of the abnormal condition on the Solution.

Considering that context of PJ07-W2-40, impacting only the planning phase it has been considered that only the connectivity between WOC and DAC failure could have an impact on the operations and required and mitigation.

	Abnormal condition	Effect	Mitigation
ABN1	Connectivity between WOC and DAC failure	No sharing of information resulting in loss of communication on airspace segregations and civil traffic.	Local DAC actors will take over (using the locally available traffic prediction, last published EDAC, etc.) WOC will activate airspace segregations only after coordination.

Table 2 Relevant abnormal conditions of operation and its effect in the context of PJ07-W2-40

SRS ID	SRS for abnormal conditions of operation
SRS 006	Fall-back arrangements adapted to the management of DAC shall be in place for defining airspace configurations in the event of prolonged connectivity between WOC and DAC failure.

Table 3: List of additional SRS for Abnormal conditions of operations

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

The purpose of this section is to present the Safety Requirements at Service level (SRS) associated to Service Hazards (caused by internal failures of the Solution Functional System)The SRS provided in this section complete the safety specification of the Solution at service level, providing the adequate mitigation against the possible adverse effects that failures internal to the Solution functional system might have upon the provision of the relevant services. Two types of SRS are included here:

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

4.4.1 Service Hazards identification and analysis

The consolidated results from the hazard identification, analysis and HAZID workshop are provided in the Table 4. The details of the workshop can be found in Appendix B.

For each identified service hazard in the table are presented the following:

- the assessed operational effect (via the effect on the service provision),
- the mitigations taken into account for assessing the operational effects (protecting against effect propagation),
- the assessed severity of the most probable operational effect from hazard occurrence as per the relevant AIM-based Severity Classification Scheme(s) (SCS) from Guidance G.3 of Safety Reference Material.

Co-funded by the European Union

NOV-5	Failure mode	Example of causes & new mitigations preventing the failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
Develop Early Flight Intent (EFI) for MT with DMA type 1 and 2 (D-7-D-1)	DAC/ASM wrongly accepts DMA request in conflict with ATC Volume (does not detect a conflict)	Human error ASM tool error Inadequate / wrong DAC historical data from ATFCM	EFI consolidated with DMA in conflict with ATC volume	Detected within ATC Volumes vs DMA analysis: DAC/ASM will identify the conflict when evaluating the impact of the DMA request (NOV-5 Allocate ARES DMA type 1 and 2 (D-1- D-Ops))	None	No safety effect
	Inadequate DMA vs ATC deconfliction resulting in inadequate adaptation proposal to WOC	Human error DAC/ASM Tool error Inadequate / wrong DAC historical data from ATFCM	WOC will consider inadequate DMA adaptation proposal and updates EFI accordingly	DAC detects & corrects using the simulation of the conflict-free configuration of airspace inadequate adaptation proposal of DMA before sending it to WOC. NOV-5 Allocate ARES DMA type 1 and 2 (D-1- D-Ops)	None	No safety effect
	Adaptation proposal by DAC/AMC assigned to wrong DMA request (multiple requests received)	Human error DAC/ASM tool error	DMA request is not deconflicted	DAC detects & corrects using the simulation of the conflict-free configuration of airspace inadequate adaptation proposal of DMA before sending it to WOC. Each DMA request has a unique ID which is automatically connected to the DAC/ASM proposal and approval for all stakeholders	None	No safety effect

Co-funded by the European Union

Allocate ARES DMA type 1 and 2 (D-1- D-Ops)	DAC/ASM wrongly accepts DMA request in conflict with ATC Volume (does not detect a conflict)	Human error ASM tool error	DMA in conflict with ATC volume integrated in the DAC and published in the NOP.	DAC/ASM detects DMA request in conflict with ATC Volume while performing local impact assessment (iSMT management with planning ATM constraint (TTO) (D-1-H-Ops)	None	No safety effect
	Inadequate DMA vs ATC deconfliction resulting in inadequate adaptation proposal to WOC	Human error DAC/ASM Tool error	WOC will consider inadequate DMA adaptation proposal and inadequately updated DMA is integrated in the DAC and published in the NOP.	DAC/ASM detects DMA request in conflict with ATC Volume while performing local impact assessment (iSMT management with planning ATM constraint (TTO) (D-1-H-Ops)	None	No safety effect
	Coordination outcome (counter proposals) between WOC and DAC/ASM is not consistent	Human error Inadequate Procedure Supporting system (data sharing or CDM)	The DMA type 1 and 2 published in NOP will not be fully consistent with the one agreed by WOC.	WOC detects problem upon receiving DMA/MT modifications published in DAC. Each DMA request has a unique ID which is automatically connected to the DAC/ASM proposal and approval for all stakeholders	None	No safety effect

iSMT management with planning ATM constraint (TTO) (D-1-H-Ops)	ATFCM fails to detect a negative impact on local performance.	Human error Inadequate Procedure Supporting system	Adverse effect on local performance	DAC has a mean to analyse and to identify the imbalance and tactical measures to protect sector capacity.	Hz01: Inappropriately granted / modified DMA type 1 and 2 request leading to overload (exceeding a sector capacity)	MAC-SC4b
	ATFCM fails to detect conflicting demands	Human error Inadequate Procedure Supporting system	Adverse effect on local performance	DAC has a mean to monitor and to identify the imbalance and tactical measures to protect sector capacity.		MAC-SC4b
	Cherry-picks trajectories which are not eligible to planning ATM constraints to mitigate adverse effect on local performance targets	Human error Inadequate Procedure Supporting system	Adverse effect on local performance	DAC has a mean to monitor and to identify the imbalance and tactical measures to protect sector capacity. DAC system support identifies eligible flights and assigns TTO resolution resolving the DCB imbalance.		MAC-SC4b
	Cherry-picks trajectories which do not resolve the imbalance through TTO assignment	Human error Inadequate Procedure Supporting system	Adverse effect on local performance	DAC has a mean to monitor and to identify the imbalance and tactical measures to protect sector capacity. DAC system support identifies eligible flights and assigns TTO resolution resolving the DCB imbalance.		MAC-SC4b

	Inadequate TTO (the TTO assigned to the flight does not resolve the DCB imbalance) proposal to WOC	Human error Inadequate Procedure Supporting system	WOC will consider inadequate TTO proposal and inadequately updated DMA is integrated in the DAC and published in the NOP. Adverse effect on local performance	DAC has a mean to monitor and to identify the imbalance and tactical measures to protect sector capacity.		MAC-SC4b

Table 4: Service Hazards and Analysis

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

In Table 5 is provided the consolidated list of additional SRS (functionality and performance) mitigating against service hazard effects (protective mitigation), identified during the service hazard assessment addressed in previous section and referenced in Table 4.

SRS ID	Additional Safety Requirements at Service level *(functionality & performance)*	Mitigated Service Hazard
SRS-007	DAC shall be able to detect and correct an inadequate adaptation of the DMA proposal using the simulation of conflict-free configuration of airspace before sending it to WOC.	Hz1
SRS-008	DAC/ASM shall be able to detect the DMA request in conflict with ATC Volume while performing local impact assessment.	
SRS-009	DAC shall have a mean to analyse and to identify the imbalance and tactical measures to protect sector capacity.	
SRS-010	DAC system shall support identification of the eligible flights and assignment of TTO resolution resolving the DCB imbalance.	

Table 5 SRS (functionality and performance) to mitigate Service hazards effects

Table 6 provides the SRS addressing integrity/reliability in order to limit the frequency with which the service hazards (listed in section Service Hazards 4.4.1) could be allowed to occur.

The SRS derivation has been performed as per Guidance G.2 of Safety Reference Material and using the relevant AIM-based Risk Classification Scheme(s) from Guidance G.4 of Safety Reference Material.

SRS ID	Safety Requirements at Service level *(integrity/reliability)*	Related Service Hazard	Severity & IM
SRS-0012	The likelihood of ATFCM fails to detect a negative impact on local performance shall be no more than 3e-4.	Hz1	MAC-SC4b N:30 IM:1

Table 6: Safety Requirements at Service level - integrity/reliability

4.5 Process assurance of the Safety Specification at service level

The safety assessment was conducted according to SRM [3]. The Safety Requirements at Service level identified refer to the functionalities & performance characteristics derived from the (potential) operational use cases envisaged for the solution limited to the potential safety implication on the side of the operational users (i.e. ATS service provider).

For this reason, the current safety assessment was initiated by a preliminary safety impact assessment, including initial hazard identification, involving operational experts which are relevant for the use of the concept. This approach allowed to understand the potential safety implication of the solution.

The following safety activities were performed (Table 7) with the participation of PJ07-W2-40 solution partners including military representatives (WOC), FMP, ASM, ATM experts, human factors, and safety experts.

Safety assessment event	Scope	Deliverable receiving the outcome
HP&SAF Scoping & Change Assessment session	Definition of safety strategy and safety planning	Safety Plan
Safety metrics and indicators session	Identification of metrics and indicators to capture safety evidence.	Safety Plan
HAZID workshop Hazard identification	Safety System Requirements Initial	SAR

Table 7 Safety assessments activities conducted for PJ07-W2-40.

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 corresponding “Other than ATS” operational 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).

The safety assessment activities feeding this section are to be conducted in two iterations for accompanying the Solution progress along the lifecycle stages. The safety assessment is to be conducted at the initial design level in V2 and at the refined design level in V3.

Safety requirements at design level (SRD) 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).

5.1 Overview of activities performed

This section addresses the following activities:

- introduction of the design model (initial or refined) 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 initial or refined design model - section 5.3.3
- 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

5.2.1 Description of the Design Model

In the frame of PJ07-W2-40, given the V3 maturity level, the EATMA Operational activity models (NOV-5 diagram Operational activity model) used by the Project to specify the operational and interoperability requirements have been also used for the safety assessment at the initial design level. In addition, the safety assessment at the refined design level was supported by more detailed EATMA models like NSV-4 diagram [3].

5.2.2 Task Analysis

As the initial design level model might not enable the full description of the system behaviour, it needs to be generally complemented by a Task Analysis provided by the HP assessment. That would allow a more detailed description of the human tasks and interactions with the technical systems.

PJ07-W2-40 did not produce such a Task Analysis. However, in order to complement the Safety Assessment, several HP-relevant inputs from the HP Assessment Report [4] and from internal meetings involving the Human Performance team have been taken into account for the derivation and agreement of the Safety Requirements.

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

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

Table 8 provides the consolidated list of Safety Requirements at Design level (SRDs) (functionality and performance) for Normal and Abnormal conditions of operations derived by mapping the Safety Requirements at Service level (SRSs) for Normal and Abnormal conditions of operation documented in section 4.2 and 4.3. For each SRD is indicated the associated SRS.

Safety Requirement ID	Safety Requirement (functionality & performance)	Derived from SRS (ID)
REQ-07-W2-40-SPRINTEROP-OP01.1002	The Airspace manager shall conduct local impact assessment upon reception of the DMA type 1 and 2 requests.	SRS-001
REQ-07-W2-40-SPRINTEROP- OP03.2002	Flow manager shall be able to update ASM Sub-regional/National with latest information regarding ATC volumes.	SRS-001
REQ-07-W2-40-SPRINTEROP- OP01.1005	The Airspace designer shall be able to simulate a conflict-free configuration with DMA type 1 and 2 configuration/location agreed in CDM between Mission planner and Airspace manger.	SRS-002
REQ-07-W2-40-SPRINTEROP- OP01.1006	The Airspace manager shall be able to share the results of the simulated conflict-free airspace configuration with WOC	SRS-003
REQ-07-W2-40-SPRINTEROP- OP03.2004	Upon reception of the iSMT with DMA type 1 and 2 the Traffic manager shall analyse impact on traffic flows and ATC sectors configurations in the context of DAC	SRS-004

REQ-07-W2-40-SPRINTEROP- OP01.1007	Airspace manager shall be able to receive updates for DMA type 1 and 2 and conduct impact assessment on airspace configuration.	SRS-005

Table 8. Safety Requirements at design level (functionality and performance) satisfying SRS for Normal and Abnormal conditions.

5.3.2 Additional SRD from Static analysis of the functional system behaviour

All use cases developed for the solution were analysed and analysis did not reveal any additional safety requirements.

5.3.3 Additional SRD from Dynamic analysis of the functional system behaviour

The Project made full use of the validation exercises feed-back in order to progressively refine and complete the SPR-INTEROP/OSED requirements. Meanwhile, no additional safety requirements have been revealed.

5.3.4 Effects on Safety Nets

None of the safety nets relevant for ENR and TMA airspace make use of the planned aircraft trajectory, thus there is no foreseen impact from the initial mission trajectory iMT with integrated DMA type 1 and 2.

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, which have been identified in section 4.4.

The following Safety Requirements at Design Level (SRD) were derived from a top-down causal analysis of the Service Hazards identified in section 4.4.1, and 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.

5.4.1 Design analysis addressing internal functional system failures

The purpose of the top-down analysis was to increase the detail of risk mitigating strategy through the identification of all possible causes of the operational hazards. This way it will be possible to identify the corresponding SRDs allowing to meet the SRS of the Operational Hazard under consideration.

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

The results of the analysis the causes and identified requirements are presented in Appendix D.

Table 9 provides the consolidated list of Safety Requirements at Design level (functionality and performance) addressing internal system failures.

Safety Requirement ID	Additional Safety Requirements at Service level *(functionality & performance)*	SRS
REQ-07-W2-40-SPRINTEROP-OP01.1004	ASM solution for de-confliction If ASM solution is accepted by WOC the Airspace manager shall be able to participate in CDM with Mission Planner on optimisation of the DMA type 1 and 2 configuration/location.	SRS-007
REQ-07-W2-40-SPRINTEROP-OP01.1005	Conflict-free airspace configuration The Airspace designer shall be able to simulate a conflict-free configuration with DMA type 1 and 2 configuration/location agreed in CDM between Mission planner and Airspace manger.	SRS-007
REQ-07-W2-40-SPRINTEROP-OP03.2004	Local impact assessment (D-1 to D-Ops) Upon reception of the iSMT with DMA type 1 and 2 the Traffic manager shall analyse impact on traffic flows and ATC sectors configurations in the context of DAC.	SRS-008
REQ-07-W2-40-SPRINTEROP-OP03.2005	Planning ATM constraint (TTO) (D-1 to D-Ops) Local Traffic manager shall be able to aggregate and apply ATFCM solution to iSMT with DMA type 1 and 2	SRS-009
REQ-07-W2-40-SPRINTEROP-OP03.2006	Planning ATM constraint (TTO) (D-1 to D-Ops) Local Traffic manager shall be able to propose a target time (TTO) over DMA type 1 and 2 entry/exit point	SRS-009
REQ-07-W2-40-SPRINTEROP-OP03.2007	Planning ATM constraint (TTO) (D-1 to D-Ops) Local Traffic manager shall be able to propose a target time over (TTO) way point along flight route to iSMT with DMA type 1 and 2.	SRS-010

Table 9 SRD associated to failure conditions.

5.4.2 Safety Requirements at design level addressing internal system failures

Table 10 provides the consolidated list of Safety Requirements at Design level (integrity/reliability) addressing internal system failure derived from the Safety Requirements at Service level (integrity/reliability) documented in section 4.4 with due consideration of any potential common cause failure.

Safety Requirement ID	Safety Requirement at Design level (SRD) (Integrity/Reliability)	Derived from Cause

REQ-07-W2-40-SPRINTEROP-OP03.2002	Flow manager shall be able to update ASM Sub-regional/National with latest information regarding ATC volumes.	SRS-008
REQ-07-W2-40-SPRINTEROP-OP01.1002	REQ-07-W2-40-SPRINTEROP-OP01.1002 The Airspace manager shall conduct local impact assessment upon reception of the DMA type 1 and 2 requests.	SRS-008
REQ-07-W2-40-SPRINTEROP-OP03.2004	Upon reception of the iSMT with DMA type 1 and 2 the Traffic manager shall analyse impact on traffic flows and ATC sectors configurations in the context of DAC).	SRS-008
REQ-07-W2-40-SPRINTEROP-OP01.1005	The Airspace designer shall be able to simulate a conflict-free configuration with DMA type 1 and 2 configuration/location agreed in CDM between Mission planner and Airspace manger.	SRS-009
REQ-07-W2-40-SPRINTEROP - SF06.0001	Adequate SW assurance shall be ensured for the DAC tool functionalities addressing the impact evaluation of airspace configuration and simulations with "what-if".	SRS-009
REQ-07-W2-40-SPRINTEROP - SF06.0002	DAC shall be able to easily distinguish on the HMI the simulation environment (what-if function) and the operational environment.	SRS-009

Table 10. SRD (integrity/reliability) to mitigate the service hazards

5.5 Realism of the safe design

Safety requirements derived in this assessment target mainly two domains: equipment and human factor.

Equipment related Safety Requirements including functionality and system performance are explicit (success approach) or quantified (failure approach). The lowest quantified failure rate corresponds to the order of 3e-4, therefore well within the range of typical reliability requirement imposed on equipment in aviation.

Human factor related Safety Requirements are explicit and qualitative in either approach, therefore considered fully achievable.

Therefore, all requirements defined in this SAR are considered achievable.

5.6 Process assurance for a Safe Design

The safety assessment was conducted according to SRM. In order to identify Initial set of Safety Requirements at Design Level (SRD) a dedicated workshop with subject matters experts was conducted addressing both success approach (defining at the level of each component what it is required to fulfil in terms of functionality and performance) and failure approach (defining at the level of each component what it is required to fulfil in terms of integrity and additional functionalities). During the workshop the potential HP and safety issues were discussed and accordingly the mitigation actions were identified.

The online workshop was conducted with the participation of PJ07-W2-40 solution partners including, Subject Matter Experts (DAC and WOC representatives) concept designers and tool developers, human factors, and safety experts.

6 Demonstration of Service specification achievability

As specified in the PJ07-W2-40 Safety Plan, safety evidence for the solution was collected from the validation exercise and recorded under safety validation objective:

OBJ PJ07W2-40-V3-VALP-SAF-01: Safety impact of iMT with integrated DMA of type 1 and 2 on sub-regional/local ATM planning processes

The impact of the concept on the safety levels in the validation exercise was measured based on the number of the conflicting trajectories. The objective measurements obtained in the reference and solution runs were compared to determine the benefits in the terms of the number of conflicting trajectories.

The evidence collected from the exercise demonstrated that in the reference run, the total number of conflicts (inside and entry conflicts) is 54 (Nb of inside conflicts = 52 and Nb of entry conflicts = 2) whereas in the solution run the registered total number of conflicts was reduced to 46 (Nb of inside conflicts = 44 and Nb of entry conflicts = 2). Therefore, the number of conflicts has decreased.

In addition, the number of trajectories rerouted due to static ARES activation in the reference scenario was 121, which constitutes 41,16% of total trajectories, while in the solution scenario, the rerouted trajectories impacted by the solution is 49, that refers to only 16,67% of total trajectories. Therefore, it might be assumed that by rerouting fewer aircraft, the workload of the controllers will also be less impacted by the changes imposed by the military activities, and consequently the safety will be improved.

Co-funded by the European Union

Val. Obj. ID	SESAR Solution Validation Objective Title	SESAR Solution Success Criterion ID	SESAR Solution Success Criterion	SESAR Solution Validation Success Criterion Results	Val. SC. Status
OBJ PJ07W2-40-V3-VALP-SAF-01	Safety impact of iMT with integrated DMA of type 1 and 2 on sub-regional/local ATM planning processes	CRT-PJ07W2-40-V3-VALP-SAF01-001	The assessment results are in line with the expectation: the reference level of Safety (SAF, no target) assessed based on the number of conflicting trajectories is at least maintained: the number of trajectory conflicts does not increase when using DMA type 1 and 2 compared to the reference scenario.	In the reference scenario the total number of conflicts is 54 (Nb of inside conflicts = 52 and Nb of entry conflicts = 2), while in the solution run the registered total number of conflicts was reduced to 46 (Nb of inside conflicts = 44 and Nb of entry conflicts = 2. Based on the expert judgement the 80% of the reduction in the number of conflicts is attributed to the application of DMA type 1 and 2.	OK
		CRT-PJ07W2-40-V3-VALP-SAF01-002	The reference level of Safety (SAF, no target) assessed based on the number of conflicting trajectories is at least maintained: the number of trajectory conflicts does not increase when applying TTO/iMT compared to the reference scenario.	In the reference scenario the total number of conflicts is 54 (Nb of inside conflicts = 52 and Nb of entry conflicts = 2), while in the solution run the registered total number of conflicts was reduced to 46 (Nb of inside conflicts = 44 and Nb of entry conflicts = 2. Based on the expert judgement the 10% of the reduction in the number of conflicts is attributed to the application of TTO/iMT.	OK

Table 11 Summary of safety evidence per success criteria.

Nevertheless, the improvements brought by the solution were measured as a whole and by looking only at objective measurements it cannot be clearly distinguished how much of these benefits are brought only by the introduction of DMA type 1 and 2 (AOM-0208-B) or by applying TTO/iMT (AUO - 2010). In addition, as explained in the section due importance is also attributed to the shared mission trajectory concept (AUO-0216) and the sharing of mission trajectory profile described by a 4D dataset (AOM-0304 B).

Based on the expert judgement, the expected contribution of each of these OI steps to the fuel efficiency (see section), and therefore applicable also to safety, is as presented in the Table 12 below:

OI step	OI Steps Title	Relative benefits contribution to Safety	
AOM-0208 B	Dynamic Mobile Areas (DMA) of types 1 and 2	80% contribution	6,4 conflicts
AUO-0210	Participation in CDM through iSMT and Target Time (TTO) negotiation	10% contribution	0,8 conflicts
AUO-0216	Shared Mission Trajectory Data	5% contribution	0,4 conflicts
AOM-0304 B	Integrated management of Mission Trajectory in trajectory-based operations environment	5% contribution	0,4 conflicts
TOTAL		100%	8 conflicts

Table 12: Contribution of OI steps to level of Safety (SAF)

Additionally, the initial recommendations for further consideration have been identified for implementation of the concept.

- DMAs naming: the DMAs should be registered with unique identifier to avoid duplications that might introduce mistakes.
- Further methodology should be developed to ensure that the safety assessment of the separate elements of the concept (i.e. mission and associated DMAs) is performed in timely manner. Generic safety assessment of the mission could be created, followed by rapid safety assessment in case of updates of the mission.
- An educational campaign should be conducted with all impacted airspace users ensuring the awareness of the concept, their role, and potential changes to the operations.

7 Acronyms and Terminology

Acronym	Definition
AASM	Advanced ASM
A/C	Aircraft
ACC	Area Control Centre or Area Control
AFUA	Advanced Flexible Use of Airspace
AIP	Aeronautical Information Provider
AIS	Aeronautical Information System
AM	Airspace Manger
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider
ARES	Airspace Reservation
ASM	Airspace Management
ATC	Air Traffic Control
ATCU	Air Traffic Control Unit
ATFCM	Air Traffic Flow and Capacity Management
ATFM	Air Traffic Flow Management
ATM	Air Traffic Management
ATS	Air Traffic Services
ATSU	Air Traffic Services Unit
AU	Airspace User
AUP	Airspace Use Plan
BT	Business Trajectory
CDM	Collaborative Decision Making
CHMI	Collaboration Human Machine Interface
CMC	Civil-Military Coordination

DAC	Dynamic Airspace Configuration
DCB	Demand Capacity Balancing
dDCB	Dynamic Demand and Capacity Balancing
DMA	Dynamic Mobile Area
EAD	European AIS Database
EATMA	European ATM Architecture
EFI	Early Flight Intent
eFPL	Extended Flight Plan
EPP	Extended Projected Profile
ER ACC/APP	En-route Area Control Centre/Approach
FMP	Flow Management Position
FMS	Flight Management System
FPL	Flight Plan
HPAR	Human Performance Assessment Report
IER	Information Exchange Requirement
IFPS	Integrated Initial Flight Plan Processing System
iMT	Initial Mission Trajectory
INTEROP	Interoperability Requirements
iOAT FPL	Improved Operational Air Traffic Flight Plan
IOP	Interoperability Protocol
iRMT	Initial Reference Mission Trajectory
iSMT	Initial Shared Mission Trajectory
ISRM	Information Services Reference Model
KPA	Key Performance Area
KPI	Key Performance Indicator
MDT	Mission Development Trajectory
N/A	Not Applicable

NM	Network Manager
NMF	Network Management Function
NMOC	Network Manager Operations Centre
NOP	Network Operations Plan
NOV	NAF Operational View
OAUO	Optimized Airspace User Operations
OE	Operational Environment
OI	Operational Improvement
OSED	Operational Service and Environment Definition
PAR	Performance Assessment Report
PI	Performance Indicator
RBT	Reference Business Trajectory
REQ	Requirement
RTSA	Real Time Status of ARES
SAC	Safety Criteria
SAR	Safety Assessment Report
SESAR	Single European Sky ATM Research Programme
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SME	Subject Matter Expert
SPR	Safety and Performance Requirements
STAM	Short-Term ATFCM Measures
STAR	Standard Instrument Arrival
SWIM	System Wide Information Management
TM	Trajectory Management
TS	Technical Specification
TSA	Temporary Segregated Airspace
TTA	Target Time of Arrival

TTO	Target Time Over
UC	Use Case
VALP	Validation Plan
VALR	Validation Report
VALS	Validation Strategy
VPA	Variable Profile Area
WOC	Wing Operations Centre
WP	Work Package

Table 13: Acronyms

8 References

Safety

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

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

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

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

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

Project documentation

[1] SESAR Solution PJ07-W2-40: Validation Plan (VALP) for V3 - Part I

[2] SESAR Solution PJ07-W2-40 SPR-INTEROP/OSED for V3 - Part I

[3] SESAR Solution PJ07-W2-40 Final TS IRS for V3

[4] SESAR Solution PJ07-W2-40 SPR-INTEROP/OSED for V3 - Part IV Human Performance Assessment Report

[5] D24 - D11.1.5-2ma-WOC - Validation report for stand-alone WOC validation for Step 1 – (BMT, AFUA, iOATFPL)

[6] D27-Update Validation report for stand-alone WOC validation for Step1 (BMT, AFUA, iOATFPL)

[7] Project Number 07.05.04, Edition 00.01.01, D66 - Step 2 V2 Flexible Airspace Management, Validation Exercise VP-755 part B Validation Report (VALR)

[8] D4.2.030, Ed. 00.01.00,27 September 2019, SESAR Solution PJ.07-03 Validation Report for V3

[9] D2.1.050, edition 00.03.01, 05 July 2019, SESAR Solution 08.01 Validation Report for V2

Appendix A Defining the Service Safety Specification for Normal and Abnormal conditions of operation

A.1 SRS obtained from other operational solutions or standards

N/A

A.2 EATMA Process models or alternative description

Relevant models from TS/IRS (NSV-4 and NOV-5) were used. Please refer to SESAR Solution PJ07-W2-40 Final TS IRS for V3[3].

A.3 Derivation of SRS for Normal conditions of operation

The derivation of the functionality & performance SRS s(as part of the success approach) is performed following analysis of NOV-5 models.

The process carried out in this step is following:

- Consolidate the information outcome from above according to Use Cases and Operational services
- For each Use Case:
  - For each Operational service:
    - Check whether the identified change(s) **is (are) safety relevant** (i.e. could the change impact the efficiency of a safety barrier or the occurrence of a safety event;
    - Derive one or several SRS in order to describe the safety-relevant changes in the delivery of that operational service by the Solution.

Use case	Function/ Actor	Details	Change	SRS
Operating method: Develop early flight intent (EFI) for MT with DMA Type 1 and 2 [D-7 to D-1]				
UC-00: Definition of ATC volumes	DAC /			
	Airspace manager	Analyses the traffic demand and establishes the configuration of ATC sectors.	Same as today	
	Local flow manager	Analyses the sector load and complexity evolution and defines ATC volumes based on expert judgement method.	Same as today	
	DAC / Local flow manager	Shares the ATC volumes with WOC.	New task	
	WOC / Mission planner	Receives and confirms the receipt of ATC volumes.	New task	
UC WOC-01: Define and share Early Flight Intent (EFI) with DMA type 1 and 2	WOC / Unit	Units provide the mission schedules and operational constraints/needs	Same as today	
	WOC / Mission planner	Collects the mission schedules from units and fills in the mission trajectories data.	Same as today	
	WOC / Mission planner	Analyses the mission schedule and the constraints posed by mission requirements as well as requested by DAC. Defines the DMA of types 1 and 2 location and configuration connected to mission trajectories. Simulates the 3D (geographical location, time, altitude) configuration of DMAs versus the ATC volumes provided by DAC.	New tasks In case of non-adequate configuration of DMA with the respect to airspace volumes, the DMA could overlap with Airspace volumes. The problem will be detected and corrected by the DAC/ATFCM (FMP) through the Final Impact Assessment	

	WOC / Mission planner	Associates flexible parameters to DMAs following to the analysis of mission requirements and constraints. Associates to each DMA a priority code based on the nature of mission and the flexible parameters.	New task; no safety impact	
	WOC /Mission planner	Shares the data set of EFI with the airspace manager.	New task	
UC ASM-02: Collect and analyse EFI with DMA type 1 and 2	DAC / Airspace manager	Receives and confirms the receipt of EFI.	New tasks	
	DAC / Airspace manager	Analyses overlapping between DMAs and ATC volumes as well as the impact of DMAs on the traffic flows (checks the number of impacted trajectories).	In case of conflictual ARES/DMA with ATC volumes the problem will be detected by the DAC/ATFCM (FMP) or ASM through the Final Impact Assessment or at the latest via hotspot monitoring on D-day.	SRS-001DAC shall be able to evaluate the impact of DMAs request on ATC Volumes via the set of parameters (number of impacted trajectories)
UC ASM-03: De-conflict EFI with DMA type 1 and 2	DAC / Airspace manager	In case of overlapping, performs deconfliction by taking into account the flexible parameters associated to each DMA. In addition to deconfliction, performs an optimization of DMA 3D parameters to reduce the impact on the trajectories. Simulates the new airspace configuration with the proposed adaptations to DMAs.	New tasks, no safety impact	SRS 001 DAC shall be able to propose the optimisation using the flexible parameters to the DMA allowing deconfliction. SRS 002 DAC shall be able to simulate and display new airspace configuration
	DAC / Airspace manager	Shares the adaptation proposals to DMAs with WOC.	New task, no safety impact	SRS 003

				DAC shall be able to share the proposals of DMA's changes with WOC.
	WOC / Mission planner	Confirms the receipt of change proposals to DMA.	New tasks No safety impact	
UC WOC-04: Analyse and Update EFI with DMA type 1 and 2.	WOC / Mission planner	Checks the DAC change proposals to DMAs parameters and their impact on the missions by using the following criteria: - the predefined flexibility - training time inside DMAs - duration of transit time - flight level block suitability	New task	
Operating method: Allocate ARES DMA Type 1 and 2 [D-1 to D-Ops]				
UC WOC-05: Refine DMA type 1 and 2 versus ATC volumes	WOC / Mission planner	The mission planner accepts / rejects /makes counter-proposals to the parameters changed by the ASM solution.	New task	
	WOC / Mission planner	Shares the updates to DMA parameters with the airspace manager.	New task	
UC ASM-06: CDM for allocation of DMA type 1 and 2	DAC / Airspace manager	Receives and confirms the receipt of DMA updates.	New task, no safety impact	
	DAC / Airspace manager	Finalizes the DMA parameters in accordance with the figures provided by WOC.	New task, no safety impact	
	DAC / Airspace manager	Shares with WOC the finalized parameters of DMAs.	New task, no safety impact	

UC ASM-07: Integration of the allocated DMA type 1 and 2 into DAC and publication	WOC / Mission planner	Receives, checks the correctness of DMA parameters and confirms the receipt of allocated DMAs.	New task, no safety impact	
Operating method: iSMT sharing [D-1 to H-D]				
UC-WOC-08: Share iSMT with DMA type 1 and 2	WOC / Mission planner	Integrates the allocated DMAs into the trajectory profile definition. The resulted trajectories represent the iSMTs.	New task, no safety impact	
	WOC / Mission planner	Translates iSMT data into iOAT FPL format.	New task, no safety impact	
iSMT Management with planning ATM constraint (TTO) [D-1to H-D]				
UC-ATFCM-09: Local impact assessment of iSMT with DMA type 1 and 2 and local ATFCM solutions (TTO proposal)	DAC / Local traffic manager	Assesses the complexity of planned traffic situation in vicinity of DMAs for the time window of impact on ATC sector. Identifies the iSMTs that generate traffic rerouting.	Similar as today	SRS 004 DAC shall be able to compare potential impact of DMAs localisation on traffic rerouting.

UC-ASM-10b: TTO over entry/exit point of ARES DMA type 1 and 2;	DAC / Local traffic manager	By using an experimentation method, consisting of moving the time of activation of affecting DMAs within the pre-defined flexibility, defines a new exit time for the DMA considered as candidate to alleviate complexity of traffic. The new time over the DMA exit point represents a TTO to respective iSMT.	New task In case of conflictual DMA with ATC volumes the problem should be detected by the DAC/ATFCM (FMP) or ASM through the Final Impact Assessment or at the latest via hotspot monitoring on D-day	SRS 004 DAC shall be able to compare potential impact of DMAs localisation on traffic rerouting.
	DAC / Local traffic manager	Sends TTO proposal to WOC.	New task, no safety impact	
	WOC / Mission planner	Receives and confirms the receipt of TTO proposal and the affected iSMT.	New task, no safety impact	
UC ASM-10: CDM on local ATFCM solutions (TTO proposal) to iSMT with DMA type 1 and 2	WOC / Mission planner	Recalculates the trajectory profile and assesses the impact of changes on the entire mission.	New task, no safety impact	
	WOC / Mission planner	Following to impact assessment, takes one of the following actions: (1)TTO has no impact on the execution of the mission (no changes to allocated DMAs): sends acceptance message of TTO to local traffic manager (2) TTO has no impact on the execution of mission (changes to allocated DMAs within the pre-defined flexibility): updates the affected DMA parameters and sends to airspace manager a DMA change proposal. (3) TTO has negative impact on the execution of the mission: sends a TTO rejection message to local traffic manager	New task, no safety impact	

	DAC / Local traffic manager	Receives and confirms receipt of TTO reaction from mission planner	New task, no safety impact	
UC-WOC-11: Revise Update iSMT with local ATFCM solution	WOC / Mission planner	Updates the trajectory profile and the content of iOAT FPL.	New task, no safety impact	
UC ASM-10: CDM on local ATFCM solutions (TTO proposal) to iSMT with DMA type 1 and 2	DAC / Airspace manager	Receives, checks the updated DMA parameters and confirms to WOC the receipt of DMA change proposal	New task, no safety impact	
	DAC / Airspace manager	Simulates the new configuration of airspace structures	New task, no safety impact	SRS 005 DAC shall be able to simulate and assess (against complexity parameters) the new configuration of airspace structure with DMAs.
	DAC / Airspace manager	Sends to WOC the updated DMA parameters	New task, no safety impact	
UC-WOC-11: Revise Update iSMT with local ATFCM solution	WOC / Mission planner	Receives and confirms the receipt of DMA change acceptance	New task, no safety impact	
	WOC / Mission planner	Updates the trajectory description and iOAT FPL	New task, no safety impact	
	WOC / Mission planner	Receives from units a change request to DMA	New task, no safety impact	
	WOC / Mission planner	Analyses the impact of change on the entire mission and performs adjustments based on mission effectiveness criteria.	New task, no safety impact	
	WOC / Mission planner	Sends modifications to allocated DMAs	New task, no safety impact	

Table 14: Derivation of SRS for Normal Operations driven by EATMA Process model

A.4 Abnormal conditions

Based on the previous SESAR documentation, safety team has reviewed the following abnormal conditions. For each abnormal condition, the immediate effect on Solution operations was described and possible mitigations were identified.

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SO xx]
ABN1	ABN1. Connectivity between WOC and DAC failure	No sharing of information resulting in loss of communication on airspace segregations and civil traffic.	Local DAC actors will take over (using the locally available traffic prediction, last published EDAC, etc.) WOC will activate airspace segregations only after coordination.
ABN2	Unforeseen airspace closure (e.g. volcanic ash, nuclear cloud …)	Unplanned losses of capacity Not applicable as impacting tactical phase	No mitigation necessary in the planning phase.
ABN3	Severe weather conditions (CBs, turbulences, icing)	Unplanned losses of capacity Not applicable as impacting tactical phase	
ABN4	Unplanned Large Airport closure		
ABN5	FDPS failure		
ABN6	SDPS failure		
ABN7	Frequency management failure		
ABN8	Industrial actions, e.g. strikes	With pre-notice, expected loss of capacity The negotiation process could take into account new constraints	Flexibility offered by negotiation process might improve performance. Standard process to be followed. No new mitigation necessary.
ABN9	Loss of enablers such as Traffic predictions, Complexity predictions, Confidence index	Will affect mainly the medium-term planning with impact on performance but not on safety.	No mitigation necessary in the short term
ABN10	Major technical changes	Planned capacity reductions	Management of DAC provides options for providing best

			performance given reduced ATC resources Standard process to be followed. No new mitigation necessary.

Appendix B Risk assessment of the change at service level

B.1 HAZID workshop

On 2nd of February 2022 a SAF/HP the online workshop was held. The workshop was facilitated by SAF/HP experts aimed at the identification of the hazards introduced by the new concept. The analysis of their operational effect accounting for the available mitigations protecting against their propagation and the determination of the severity of the hazard effects. Where relevant, specific HP issues have been tackled as well.

The workshop participants:

- EUROCONTROL
- AIRBUS
- PANSA
- INTEGRA
- MEP
- SPANISH

The results of the workshop are in the main body of the report.

Appendix C Designing the Solution functional system for Normal and Abnormal conditions of operation

C.1 Deriving SRD from the SRS

SRS for Normal and Abnormal Operation (ID & content)	Safety Requirement at Design level[1] (SRD) or Assumption
SRS-001 DAC shall be able to evaluate the impact of DMAs request on ATC Volumes via the set of parameters (number of impacted trajectories)	REQ-07-W2-40-SPRINTEROP-OP01.1002 The Airspace manager shall conduct local impact assessment upon reception of the DMA type 1 and 2 requests
	REQ-07-W2-40-SPRINTEROP- OP03.2002 Flow manager shall be able to update ASM Sub-regional/National with latest information regarding ATC volumes.
SRS-002 DAC shall be able simulate and display new airspace configuration	REQ-07-W2-40-SPRINTEROP- OP01.1005 The Airspace designer shall be able to simulate a conflict-free configuration with DMA type 1 and 2 configuration/location agreed in CDM between Mission planner and Airspace manger content
SRS-003 DAC shall be able to share the proposals of DMA's changes with WOC.	REQ-07-W2-40-SPRINTEROP- OP01.1006 The Airspace manager shall be able to share the results of the simulated conflict-free airspace configuration with WOC
SRS-004 DAC shall be able to compare potential impact of DMAs localisation on traffic rerouting.	REQ-07-W2-40-SPRINTEROP- OP03.2004 Upon reception of the iSMT with DMA type 1 and 2 the Traffic manager shall analyse impact on traffic flows and ATC sectors configurations in the context of DAC
SRS-005 DAC shall be able simulate and assess (against complexity parameters) the new configuration of airspace structure with DMAs.	REQ-07-W2-40-SPRINTEROP- OP01.1007 Airspace manager shall be able to receive updates for DMA type 1 and 2 and conduct impact assessment on airspace configuration

SO006 Fall-back arrangements adapted to the management of DAC is in place for defining airspace configurations in the event of prolonged connectivity between WOC and DAC failure.	REQ-07.03-SPRINTEROP-SF06.0001 Fall-back arrangements adapted to the Management of DAC shall be in place for defining airspace configurations in the event of prolonged connectivity between WOC and DAC failure

Table 15: SRD derived by mapping SRS for normal and abnormal conditions of operation.

Appendix D Deriving SRD from the SRS (functionality&performance) for protective mitigation

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

SRS (functionality& performance) for protective mitigation (ID & content)	Safety Requirement at Design level[2] (SRD) or Assumption
SRS-007 DAC shall be able to detect and correct an inadequate adaptation of the DMA proposal using the simulation of conflict-free configuration of airspace before sending it to WOC.	REQ-07-W2-40-SPRINTEROP-OP01.1004 ASM solution for de-confliction If ASM solution is accepted by WOC the Airspace manager shall be able to participate in CDM with Mission Planner on optimisation of the DMA type 1 and 2 configuration/location.
SRS-007 DAC shall be able to detect and correct an inadequate adaptation of the DMA proposal using the simulation of conflict-free configuration of airspace before sending it to WOC.	REQ-07-W2-40-SPRINTEROP- OP01.1005 Conflict-free airspace configuration The Airspace designer shall be able to simulate a conflict-free configuration with DMA type 1 and 2 configuration/location agreed in CDM between Mission planner and Airspace manger.
SRS-008 DAC/ASM shall be able to detect the DMA request in conflict with ATC Volume while performing local impact assessment.	REQ-07-W2-40-SPRINTEROP- OP03.2004 Local impact assessment (D-1 to D-Ops) Upon reception of the iSMT with DMA type 1 and 2 the Traffic manager shall analyse impact on traffic flows and ATC sectors configurations in the context of DAC.
SRS-009 DAC shall have a mean to analyse and to identify the imbalance and tactical measures to protect sector capacity.	REQ-07-W2-40-SPRINTEROP-OP03.2005 Planning ATM constraint (TTO) (D-1 to D-Ops) Local Traffic manager shall be able to aggregate and apply ATFCM solution to iSMT with DMA type 1 and 2

Co-funded by the European Union

SRS-009 DAC shall have a mean to analyse and to identify the imbalance and tactical measures to protect sector capacity.	REQ-07-W2-40-SPRINTEROP- OP03.2006 Planning ATM constraint (TTO) (D-1 to D-Ops) Local Traffic manager shall be able to propose a target time (TTO) over DMA type 1 and 2 entry/exit point
SRS-0010 DAC system shall support identification of the eligible flights and assignment of TTO resolution resolving the DCB imbalance.	REQ-07-W2-40-SPRINTEROP- OP03.2007 Planning ATM constraint (TTO) (D-1 to D-Ops) Local Traffic manager shall be able to propose a target time over (TTO) way point along flight route to iSMT with DMA type 1 and 2.

Table 16: SRD derived by mapping SRS (functionality&performance) for degraded conditions.

D.1.1 Top-down analysis of the design

Table 17 provides the causes of a service hazard and the associated mitigations preventing the service hazard to occur.

Cause ID	Origin of the cause	Detailed description	Mitigation/Safety Requirement
Cause 1 DAC/ASM wrongly accepts DMA request in conflict with ATC Volume (does not detect a conflict)	Inadequate / wrong DAC historical data from ATFCM	The system provides wrong / inadequate historical data, therefore the DAC/ASM is not able to detect the conflict.	REQ-07-W2-40-SPRINTEROP-OP03.2002 Flow manager shall be able to update ASM Sub-regional/National with latest information regarding ATC volumes
Cause 2 Upon receiving an updated DMA request the DAC impact assessment fails to detect the ATFCM impact	Supporting system failure	The supporting system does not provide correct assessment of the impact on traffic flown (the displayed impacted traffic flows are not corrected)	REQ-07-W2-40-SPRINTEROP-OP01.1002 The Airspace manager shall conduct local impact assessment upon reception of the DMA type 1 and 2 requests. REQ-07-W2-40-SPRINTEROP-OP03.2004 Upon reception of the iSMT with DMA type 1 and 2 the Traffic manager shall analyse impact on traffic flows and ATC sectors configurations in the context of DAC). REQ-07-W2-40-SPRINTEROP-OP01.1005 The Airspace designer shall be able to simulate a conflict-free configuration with DMA type 1 and 2 configuration/location agreed in CDM between Mission planner and Airspace manger.

Co-funded by the European Union

			REQ-07.03-SPRINTEROP-SF06.0002 Adequate SW assurance shall be ensured for the DAC tool functionalities addressing the impact evaluation of airspace configuration and simulations with "what-if".
Cause 3 ATFCM fails to detect conflicting demands	Human error	The supporting system does not assist adequately the user in decision making. The decision making is not adequate.	REQ-07-W2-40-SPRINTEROP-OP01.1002 The Airspace manager shall conduct local impact assessment upon reception of the DMA type 1 and 2 requests. REQ-07-W2-40-SPRINTEROP-OP03.2004 Upon reception of the iSMT with DMA type 1 and 2 the Traffic manager shall analyse impact on traffic flows and ATC sectors configurations in the context of DAC). REQ-07-W2-40-SPRINTEROP-OP01.1005 The Airspace designer shall be able to simulate a conflict-free configuration with DMA type 1 and 2 configuration/location agreed in CDM between Mission planner and Airspace manger. REQ-07.03-SPRINTEROP-SF06.0002 Adequate SW assurance shall be ensured for the DAC tool functionalities addressing the impact evaluation of airspace configuration and simulations with "what-if".
Cause 4 Cherry-picks trajectories which are not eligible to planning ATM constraints to mitigate adverse effect on local performance targets	Human error Supporting system	The supporting system does not assist adequately the user in decision making -Confusion between simulation and operational environment (when performing "what-if") HMI leaves room for confusion (e.g. operator mistakenly plays a "what-if" in the ops environment with the risk of introducing	REQ-07-W2-40-SPRINTEROP-OP01.1002 The Airspace manager shall conduct local impact assessment upon reception of the DMA type 1 and 2 requests. REQ-07-W2-40-SPRINTEROP-OP03.2004 Upon reception of the iSMT with DMA type 1 and 2 the Traffic manager shall analyse impact on traffic flows and ATC sectors configurations in the context of DAC). REQ-07-W2-40-SPRINTEROP-OP01.1005 The Airspace designer shall be able to simulate a conflict-free configuration with DMA type 1 and 2 configuration/location agreed in CDM

		an undesired change to the airspace).	between Mission planner and Airspace manger. REQ-07.03-SPRINTEROP-SF06.0002 Adequate SW assurance shall be ensured for the DAC tool functionalities addressing the impact evaluation of airspace configuration and simulations with "what-if". REQ-07.03-SPRINTEROP-SF06.0003 DAC shall be able to easily distinguish on the HMI the simulation environment (what-if function) and the operational environment.

Table 17. Service hazard causes and associated preventive mitigations (SRD)

D.1.2 Bottom-up analysis of the design

The bottom-up analysis of the failure modes of the functional system elements / element-to-element interfaces and of their effects, was conducted for Hazard 1.

Functional system element	Failure mode	Effects	Mitigation/Safety Requirement	Service hazard
Airspace manager sub-regional/ National	Failure of the impact assessment supporting system	The DAC ASM not able to simulate and assess the impact on ATC volumes DMAs are not implemented / negotiation process is suspended	ASS07-W2-40- SF06.0001 Fall-back arrangements adapted to the Management of DAC shall be in place for defining airspace configurations in the event of prolonged connectivity between WOC and DAC failure	*Hz1*

Table 18. Common cause failures for Hazard 1