INDUSTRIAL RESEARCH

sesar JOINT UNDERTAKING

SESAR Solution PJ10-W2-93 SPR-INTEROP/OSED for V3 - Part II - Safety Assessment Report

Deliverable ID:	**D3.2.030**
Dissemination Level:	**PU**
Project Acronym:	**PROSA**
Grant:	**87446**
Call:	**H2020-SESAR-2019-1**
Topic:	**PJ.10-W2 Separation Management and Controller Tools**
Consortium Coordinator:	**DFS**
Edition Date:	**26th May 2023**
Edition:	**01.00.01**
Template Edition:	**00.00.04**

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Authoring & Approval

Authors of the document

Beneficiary	Date
ENAV	11/01/2022

Reviewers internal to the project

Beneficiary	Date
DFS	20/12/2022
Skyguide	13/12/2022
COOPANS	05/12/2022
PANSA	20/01/2023
ENAIRE	20/12/2022

Reviewers external to the project

Beneficiary	Date

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

Beneficiary	Date
DFS	08.02.2023
Eurocontrol	09.02.2023
Skyguide	10.02.2023
ENAIRE	13.02.2023
Thales Airsys	10.02.2023
Indra	09.02.2023
Frequentis	10.02.2023
ENAV	10.02.2023
Naviair	13.02.2023
NATS	13.02.2023
DSNA	13.02.2023
Leonardo	13.02.2023
Hungarocontrol	13.02.2023

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Rejected By - Representatives of beneficiaries involved in the project

Beneficiary	Date
none	

Document History

Edition	Date	Status	Beneficiary	Justification
00.00.01	11/01/2022	Draft	ENAV	Creation of the document
00.00.02	24/01/2022	Draft	ENAV	Document updated
00.00.03	02/02/2022	Draft	DFS ENAV	Document updated considering comments received after internal review
00.00.04	14/02/2022	Draft	ENAV	Document aligned with new template
00.00.05	18/02/2022	Updated Version	ENAV	Editorial changes and general updates
00.00.06	21/12/2022	Updated Version	ENAV Skyguide COOPANS PANSA ENAIRE	Document updated with exercises results
00.01.00	**06/02/2023**	**Final Version**	**ENAV**	**Sent out for approvals**
00.01.01	**13/02/2023**	**Final**	**ENAV**	**Final version for submission to the SJU**
01.00.00	**24.02.2023**	**Approved**	**ENAV**	**Approved by the SJU**
01.00.01	**26/05/2023**	**Final version after maturity gate**	**ENAV**	**Final version**

EUROPEAN PARTNERSHIP

Co-funded by the European Union

PJ.10-W2 PROSA

DELEGATION OF ATM SERVICES PROVISION AMONG ATSUS

This SPR-INTEROP/OSED Part II is part of a project that has received funding from the SESAR Joint Undertaking under grant agreement No 874464 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 PJ10 Solution 93 (Delegation of ATM services provision among ATSUs).

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. The assessment presented in this document is complemented by the one performed at technological level within the SESAR PJ.10-W2 Technological Solutions 93A, 93B and 93C and presented in the TS/IRS Part II – SAR.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Table of Contents

EUROPEAN PARTNERSHIP
Co-funded by the European Union

List of Tables

EUROPEAN PARTNERSHIP
Co-funded by the European Union

EUROPEAN PARTNERSHIP

Co-funded by the European Union

List of Figures

EUROPEAN PARTNERSHIP

Co-funded by the European Union

1 Executive Summary

This document contains the Specimen Safety Assessment for a typical application of the PJ.10-W2-93 Delegation of ATM services provision among ATSUs. The report presents the assurance that the Safety Requirements for the V3 phase are complete, correct and realistic, thereby providing all material to adequately inform the PJ.10-W2-93 V3 Solution OSED/SPR/INTEROP [15] and SESAR PJ.10-W2 Technological Solutions 93A, 93B and 93C TS-IRS Part I [17] and II [10].

EUROPEAN PARTNERSHIP

Co-funded by the European Union

2 Introduction

2.1 Background

The V3 maturity phase of SESAR Solution PJ.10-W2-93 is built as a follow-up of the work carried out within SESAR 2020 Wave 2 PJ.10-W2-93 at V2 level, and continues the research initiated in SESAR 2020 Wave 1 by PJ.15-09 and PJ.16-03 in the operational and technical aspects, respectively, for the delegation of ATM services provision concept.

On the operational side, PJ.15-09 “Delegation of airspace and contingency” explored an initial set of potential use cases for the delegation of ATM services provision among ATSUS in case of nominal and abnormal conditions (i.e., contingency). This solution was launched after the TRL-2 maturity gate of “Enabling rationalisation of infrastructure using virtual centre-based technology” to cover the operational gap.

Considering the initial set of use cases developed within PJ.15-09, PJ.10-W2-93 validated at V2 level the operational concept, operational requirements and operational procedures defined for the delegation of ATM services provision among ATSUs at night and during abnormal conditions (i.e., ATSU contingency).

On the technological side, the virtual centre technology supporting the delegation of ATM services provision was originally explored in SESAR 1 – B04.04, which focused on the demonstration of the technical feasibility.

In SESAR 2020 Wave 1, PJ.16-03 “Enabling rationalisation of infrastructure using virtual centre based technology” continued the work performed in SESAR 1 and matured up to TRL-6 some of the services used in support of Virtual Centre.

In SESAR 2020 Wave 2, PJ.10-W2-93 further explored the use of both existing (PJ.16-03) and new services, involving different ATSUs and ADSPs from different vendors.

2.2 General Approach to Safety Assessment

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

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

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

According to the SESAR Safety guidance, from a safety assessment perspective, solution 93 is an ATS operational solution because, as for the definition provided by the guidance, change affects mainly the ATS services delivered to the airframe, the WHAT (services and their characteristics) and/or the HOW

EUROPEAN PARTNERSHIP

Co-funded by the European Union

(the way ATCOs and Pilots act, interact and make use of tools/equipment in view of delivering ATS). The design safety drivers are the Safety Criteria (SAC).

2.3 Scope of the Safety Assessment

Under V3, Safety Assessment requires the analysis of the refined System. The safety assessment will derive:

- The Safety Requirements at ATS Service level (SRS) in view of mitigating the relevant risks inherent to aviation in both normal and abnormal conditions of operation and also in failure cases with the mitigation of system generated hazards;
- The Safety Requirements at Design level (SRD) that are design characteristics/items of the Solution functional system to ensure that the system operates as specified and is able to achieve the SAC.

  The set of SRD to be documented refer to:

  - Safety Requirements at initial design level (iSRD) in V2;
  - Safety Requirements at refined designed level (rSRD) in V3.

The current version of the Safety Assessment Report covers the following exercises:

1. EXE-2 led by ENAIRE aimed at validating the operational aspects linked to the delegation of ATM services provision for the following use cases:
   - Delegation of ATM services provision at night
   - Delegation of ATM services provision at fixed time
   - Delegation of ATM services provision on-demand
2. EXE-3 led by SkyGuide aimed at validating the operational and technical aspects, including the validation of new services, linked to the delegation of ATM services provision for the following use cases:
   - Delegation of ATM services provision at night
   - Delegation of ATM services provision in case of contingency
3. EXE-4 led by ENAV aimed at validating the operational and technical aspects linked to the delegation of ATM services provision for the following use cases:
   - Delegation of ATM services provision at night
   - Delegation of ATM services provision at fixed time
   - Delegation of ATM services provision on-demand
   - Delegation of ATM services provision in case of contingency

EUROPEAN PARTNERSHIP

Co-funded by the European Union

- Delegation of ATM services provision between Civil and Military ATSUs

4. EXE-5 led by COOPANS validate the operational and technical aspects linked to the delegation of ATM services provision for the following use case:
    - Delegation of ATM services provision on-demand
    - Delegation of ATM services provision in case of contingency
5. EXE-6 led by PANSA aimed at validating the operational aspects linked to the delegation of ATM services provision for the following use case:
    - Delegation of ATM services provision at night
    - Delegation of ATM services provision on-demand
    - Delegation of ATM services provision in case of contingency.

2.4 Layout of the Document

Section 1 presents the executive summary of the document

Section 2 provides a high-level description of the change and background of the concept, the principles of the safety assessment in SESAR and the scope of this safety assessment

Section 3 provides a description of the solution operational environment and key properties, and the definition of Safety Criteria (SAC)

Section 4 addresses the safety specification at ATS service level, through the derivation of Safety Requirements at ATS service level (SRS)

Section 5 addresses the safe design of the solution functional system, through the derivation of Safety Requirements at design level (SRD)

Section 6 addresses the Safety criteria achievability

Section 7 is dedicated to acronyms and specific terminology employed in this Safety Assessment Report

Section 8 lists the documents referred to in this Safety Assessment Report

Appendix A presents the outcomes of the preliminary safety impact assessment and Safety Criteria determination

Appendix B presents the derivation of the SRS (functionality and performance) in order to mitigate the hazards inherent to aviation under normal conditions of operation

Appendix C presents the results of the risk analysis

Appendix D presents the risk analysis done at the level of the ATS service specification, including operational hazards identification and analysis in view of deriving additional SRS.

Appendix E addresses the designing the Solution functional system for normal conditions

Appendix F addressed the designing the Solution Functional system for Abnormal conditions of operation

Appendix G presents the detailed risk evaluation and mitigation of the operational hazards performed at the level of the design of the Solution functional system.

Appendix H presents the demonstration of Safety Criteria achievability

Appendix I includes the assumptions, Safety Issues & Limitations

EUROPEAN PARTNERSHIP

Co-funded by the European Union

3 Setting the Scene of the safety assessment

3.1 Operational concept overview and scope of the change

PJ.10-W2-Solution 93 is exploring operational concepts of the delegation of ATM services provision amongst ATSUs. Delegations can be done either in normal conditions in order to improve the efficiency of ATM or it can be done in abnormal, i.e., contingency, conditions in order to improve resilience and minimise the impact a failure.

The delegation of ATM services provision concept applies when one ATSU delegates a portion of its airspace, or the entire airspace, to another ATSU based on a particular condition. The Solution will investigate Use Cases for the Delegation of ATM and Contingency in conjunction with the Virtual Centre Technology where the ATM Data Service Provider (ADSP) is geographically separated from the Virtual Centre ATSU providing ATS to a region of airspace.

Based on the new operational opportunities offered by the Virtual Centre concept, a preliminary set of Delegation and Contingency Uses Cases have been selected, with the aim to further investigate and develop dynamic airspace configuration and advanced ATFCM[1] capabilities. These will allow a completely new architecture to provide Air Traffic Services. These Use Cases will consider the operational procedures and resource management to support static and dynamic delegation of ATS, and will be identified before defining the Operational Requirements for different ATSU and ADSP configurations.

This agility will lead to greater opportunities to provide Air Traffic Services, both from a technical and operational context, leading to flexible use of resources, which in turn leads to improved overall Performance.

This solution considers potential improvements in ATM by developing detailed Use Cases for the Delegation of ATM services provision between ATSUs in normal conditions and in the event of a Contingency.

The solution changes impact on several aspects (e.g. roles and responsibilities; operating methods; technical systems). Details are provided in OSED Part I [15][15]~~[12]~~, Human Performance Assessment Plan [12][12]~~[9]~~, Human Performance Assessment Report [13][13]~~[10]~~ and TS-IRS **Error! Reference source not found.Error! Reference source not found.**~~[14]~~.

3.2 Solution Operational Environment and Key Properties

[1] ATFCM aspects of delegation of ATM services among ATSU will be researched in detail by PJ.32-W3

EUROPEAN PARTNERSHIP

Co-funded by the European Union

The Operational Environment relevant for the solution 10-93 for V3 is reported in detail in the OSED/SPR/INTEROP Part I [15][15]~~[12]~~. This sub-section describes the key properties of the Operational Environment that are relevant to the PJ.10-W2-93 safety assessment.

3.2.1 Airspace

En-Route Airspace specified and known. Delegated Airspace configuration not changed: ATS routes, free route Sector, ATC Sectors, OLDI process delegation, LoA, datalink. ATS Environment and Radar maps specified, updated and known.

ATS Environment and Radar maps must be specified, updated and known by receiving unit.

3.2.2 Airspace Users – Flight Rules

It is expected that the airspace users will operate according to Instrument Flight Rules (IFR). The application of the operating concept does not imply any changes to the AUs.

3.2.3 Traffic Levels and complexity

Different traffic level (Low to High) and complexity is considered within the solution.

3.2.4 Aircraft ATM capabilities

The Aircraft ATM capabilities are not relevant to the solution concepts in PJ.10-W2-93.

3.2.5 Terrain Features – Obstacles

The definition of characteristics of terrain features and obstacles are not relevant to the solution concepts in PJ.10-W2-93.

3.2.6 CNS Aids

All the data needed for the ATCO have to be available (e.g. surveillance data and flight plans). VCS should be considered, especially when the delegation process involves different ANSPs, in order to avoid any kind of frequency issues.

3.2.7 Operational working method and Separation Minima

Working method of the different actors need to be clearly defined, as specific coordination procedures to allow delegation process need to be released.

Same radar separation and operational Standard in the delegated ATSU shall be applied in the same category of airspace in order to make the delegation process transparent to the AUs.

Relevant information regarding flights should be in the system (updated trajectory, status, clearance, CPDLC capability, etc.) before the handover.

In case of contingency (e.g. loss of ATSU, loss of ADSP), adequate procedures shall be in place

EUROPEAN PARTNERSHIP

Co-funded by the European Union

3.2.8 ATCO Training and Licensing

ATCO training is needed as well as licensed and available skilled ATCOs in the receiving units. In order to be able to provide ATM services for a delegated piece of airspace, the ATCOs of the receiving ATSU need to hold the appropriate licences for the airspace they are intended to take the responsibility for. If the receiving ATSU cannot provide appropriately licensed ATCOs, ATM services cannot be provided for a delegating ATSU.

In addition, ATCOs recurrent training is needed in order to guarantee an optimal maintenance of competence by reinforcing and broadening the knowledge necessary to perform effectively in their role.

3.3 Stakeholders' expected benefits with potential Safety impact

During the SAF&HP Scoping and Change Assessment Workshop, input to HP and Safety issues and benefits have been collected from participants to workshop through a workgroup activity. Details of this activity are reported in the **Error! Reference source not found.Error! Reference source not found.**~~Appendix A~~ of V2 SAP [6].

Further details about the benefits that the solution is intended to bring are also reported in the OSED/SPR/INTEROP Part I BIM Section [15][15]~~[12]~~.

3.4 Safety Criteria

Safety Criteria (SAC) define the acceptable level of safety (i.e. accident and incident risk level) to be achieved by the Solution under assessment, considering its impact on the ATM/ANS functional system and its operation.

The SAC setting is driven by the analysis of the impact of the Change on the relevant AIM models (models identified at §**Error! Reference source not found.Error! Reference source not found.**~~4.2.1~~ of SAP) and it needs to be consistent with the SESAR safety validation targets defined by PJ 19.04.

For PJ.10-W2-93 the Safety Validation Target is: *Safety needs to be maintained*.

In order to perform the safety assessment, the level of safety is to be defined in terms of risk associated to the hazardous situations and defining how the system contributes to them. As stated in §4.2.1, a pre-condition for performing the safety assessment for the introduction of a new concept is to understand the impact it would have in the overall ATM risk picture. Quantification of this risk is to be done based on the AIM.

Steps done to prepare the Safety Criteria:

- Identification of the accident incident type impacted by the change, after defined hazards inherent to aviation (see §4.2.1);
- Identification of safety barriers and precursors of the relevant accident incident model impacted by the change (see below);
- Definition of the Safety Criteria at the level of safety barriers (see below).

The main barriers of model MAC-ER considered within solution PJ.10-W2-93 are:

- Traffic Planning and Coordination (B10)

  This barrier involves the actions of the planner in coordination with the executive ATCo to prevent conflicts at the entry to a sector and de-conflict aircraft on leaving a sector. It normally involves the setting of appropriate entry and exit conditions for each aircraft. This barrier also deals with the coordination between planners in adjacent sectors and also between the planner and the exec on the same sector. Finally it deals with the traffic synchronisation aspects which are especially important in TMA operations and in the boundaries of TMA and Enroute.

- Tactical Conflict Management

  This is the "normal" Tactical Conflict Management task of the executive ATCo. It is the detection of conflicts (risks of infringement of separation norms), solution and communication of that solution to the aircraft involved. This barrier includes:

  - Management of planned conflict (conflict detected by the ATC),
  - Management of ATC induced conflict (conflict induced by the ATCO when solving another conflict or when dealing with a situation of bad weather / restricted area activation),
  - Management of crew/aircraft induced conflict (conflict induced by a failure of the pilot or the aircraft)

The main precursors (conditions, events, sequences that precede and lead up to Mid Air Collision) of MAC-ER AIM are the following:

- Pre-Tactical Conflict
- ATC Induced pre-tactical conflict
- Induced tactical conflict
- Planned tactical conflict
- Imminent infringement

Barrier	Precursor	Positive impact	Negative Impact	Sum up of impact	Safety Criteria
Traffic Planning & Coordination	Planning Conflicts	Planner/ ATCO prevents potential conflicts from becoming	No negative impact	No negative impact. Minimized potential tactical	With the introduction of PJ.10-W2-93 concept, the number of planning conflicts shall not increase.

		tactical conflicts thereby reducing tactical intervention.		conflict situations	
	ATC induced tactical conflict		No negative impact	No negative impact. Minimized potential losses of separation.	With the introduction of PJ.10-W2-93 concept, the number of ATC induced conflicts shall not increase.
Tactical conflict Management	Imminent Infringement	ATCOs monitoring for potential conflicts, detect and resolve them, minimising losses of separation	No negative impact	No negative impact. Minimized potential losses of separation.	With the introduction of PJ.10-W2-93 concept, the number of imminent infringements shall not increase, according to the AoR.

Table 11111. Summarised SAC in terms of barriers

The following Safety Criteria have been defined:

SAC#01: With the introduction of PJ.10-W2-93 concept, the number of planning conflicts shall not increase.

The AIM precursor considered is “Planning Conflicts” (MF5.1).

SAC#02: With the introduction of PJ.10-W2-93 concept, the number of ATC induced conflicts shall not increase.

The AIM precursor considered is “ATC induced conflict” (MF7.1).

SAC#03: With the introduction of PJ.10-W2-93 concept, the number of imminent infringements shall not increase, according to the AoR.

The AIM precursor considered is “Imminent Infringement” (MF5.9).

EUROPEAN PARTNERSHIP

Co-funded by the European Union

4 Safety specification at ATS service level

4.1 Overview of activities performed

This section addresses the following activities:

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

4.2 Mitigation of Risks Inherent to Aviation – Normal conditions

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

Based on the hazards inherent to aviation identified in Appendix A.1, and following **Guidance E.3** of **SESAR Safety Reference Material, Error! Reference source not found.Error! Reference source not found.**~~Table 1~~ identifies the ATS operational services potentially impacted by the Change provided in the relevant operational environment to address and mitigate the hazards inherent to aviation.

ID	ATS Operational Service	Hazards inherent to aviation
ATS-01	Maintain separation between aircrafts.	Ha#1 Ha#2 Ha#3 Ha#4
ATS-02	Prevent an unauthorized entry into restricted airspace.	Ha#2
ATS-03	Handle request from aircraft; Manage Trajectory.	Ha#1 Ha#4

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Table 22222: ATS Operational services potentially impacted and Hazards inherent to aviation

Error! Reference source not found.Error! Reference source not found.Table 3 provides the consolidated list of the SRS for normal conditions of operation that have been derived in Appendix B.

SRS ID	SRS for Normal conditions of operation	Related SAC
SRS-001	The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	SAC#01 SAC#02 SAC#03
SRS-002	The decision for delegation abortion by the Supervisor in the Receiving ATSU shall be taken timely.	SAC#01 SAC#02 SAC#03
SRS-003	The delegating ATSU and the receiving ATSU as well as other concerned parties shall mutually agree upon operational procedures of the delegated airspace.	SAC#01 SAC#02 SAC#03
SRS-004	All relevant third parties shall be informed about an aborted delegation.	SAC#01 SAC#02 SAC#03
SRS-005	The receiving ATCO team shall have the complete traffic situational awareness for the delegated sector following the traffic exchange with the delegating ATCO team.	SAC#01 SAC#02 SAC#03
SRS-006	One ATCO shall be in control of the delegated sector during all phases of the delegation procedure.	SAC#01 SAC#02 SAC#03
SRS-007	The operational Supervisor of the receiving ATSU shall inform all relevant third parties about the successful completion of the delegation.	SAC#01 SAC#02 SAC#03

Table 33333: List of SRS (functionality and performance) for normal conditions of operation

4.2.2 Additional SRS related to adjacent airspace or neighbouring ATM Systems

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SRS ID	SRS for compatibility	Related SAC
SRS-008	Special procedures as defined by delegation contracts regulating the initiation, execution and termination of the delegation shall be in place with the ATSU(s) adjacent to sectors subject delegation.	SAC#01 SAC#02 SAC#03
SRS-009	The operational Supervisor of the delegating ATSU shall inform operational Supervisor(s) of adjacent ATSU(s) when the delegation procedure is triggered.	SAC#01 SAC#02 SAC#03

Table 44444: Additional SRS (functionality and performance) for Compatibility

4.3 Mitigation of Risks Inherent to Aviation - Abnormal conditions

4.3.1 Identification of Abnormal Conditions

The purpose of this section is to identify any abnormal conditions related to PJ.10-W2-93 concept that might be encountered relatively infrequently.

Such conditions cover:

- Technical Issues (e.g. Partial/Full loss of ATM System because of Cyber Attack, Electrical problem / flooding's, Critical infrastructure failure)
- Staff Issues (e.g. ATC STAFF Capacity) Too many aircraft for the control area/sector; too many to do the delegation
- Other significant, but infrequent events in the operational environment (e.g. Terrorist Attack).

Only in the contingency situations strictly related to the ATS provision, the delegation procedures can be seen as mitigation protecting against the propagation of effects. In fact, even if during the delegation safety will still be degraded (e.g. transferring ATSU has not radar and can't give a proper handover), the delegation will improve the situation. This kind of contingency measures are only executed in the event of a disruption of services, which may result in a partial outage of a specific ATS unit. In case of complete, catastrophic outage of a specific ATS unit, or if no immediate contingency delegation can be provided, the Supervisor of the failing ATSU instructs the ATCO teams of the failing unit to clear-the-sky.

For further information, please refer to Appendix C of this document.

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

Table below provides the consolidated view of the SRS for abnormal conditions of operation derived in Appendix C.

SRS ID	Description	Related SAC

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SRS-010	All procedures concerning involved parties in contingency delegation mode shall have a well-defined contingency plan including legal operational procedures and definition of responsibility for the service provision.	SAC#01 SAC#02 SAC#03
SRS-011	The operational Supervisor of the failing ATSU shall be responsible to decide if the ATSU has a contingency case	SAC#01 SAC#02 SAC#03
SRS-012	The operational Supervisor of the failing ATSU shall be responsible to decide if a contingency delegation is initiated.	SAC#01 SAC#02 SAC#03
SRS-013	The operational Supervisor of the failing ATSU of the failing ATSU shall request contingency delegation at an aiding ATSU.	SAC#01 SAC#02 SAC#03
SRS-014	The operational Supervisor of the aiding ATSU shall decide if contingency delegation can be provided.	SAC#01 SAC#02 SAC#03
SRS-015	The receiving ATSU shall have opportunity to monitor the traffic load in the receiving sector(s) in order to prevent overload situations.	SAC#01 SAC#02 SAC#03

Table 55555: List of additional SRS for Abnormal conditions of operation

4.4 Mitigation of System-generated Risks (failure conditions)

4.4.1 Operational Hazards Identification and Analysis

The list of Operational Hazards is based on Wave 1 PJ.16-03 SAR Appendix D – Hazards Consequences. The list was reviewed during off-line consultation with domain safety experts.

ID	Operational Hazard Description	Operational Effects	Mitigation of effects propagation	Severity *(most probable effect)*
OH 01	Loss of Service prevents controller from	Near Mid Air Collision	ATC collision prevention	MAC-SC2a

	managing one or many aircraft for receiving ATSU	(MF3a)	B3B4	
OH 02	Loss of Service prevents controller from managing one or many aircraft for both delegating and receiving ATSUs	Near Mid Air Collision (MF3a)	ATC collision prevention B3B4	MAC-SC2a
OH 03	Loss of Service results in "Service Loss (one/two workstation/s) for receiving ATSU", i.e. data and or functions not available or not behaving correctly preventing the controller to have access to all functionality required to safely manage traffic.	Imminent Infringement (MF5.9)	ATC Collision Prevention B3B4	MAC-SC3
OH 04	Loss of Service results in "Service Loss (one/two workstation/s) for both delegating and receiving ATSUs", i.e. data and or functions not available or not behaving correctly preventing the controller to have access to all functionality required to safely manage traffic.	Imminent Infringement (MF5.9)	ATC Collision Prevention B3B4	MAC-SC3

OH 05	Loss of Service results in"Detected corruption for receiving/ both delegating and receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic	Imminent Collision (MF4)	ATC Collision Prevention B3B4	MAC-SC2b
OH 06	Loss of Service results in "Undetected Corruption for receiving/ both delegating and receiving ATSU" preventing controller from managing safe separation of traffic	Near Mid Air Collision (MF3a)	ATC collision prevention B3B4	MAC-SC2a

Table 66666: Operational Hazards and Analysis

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

Table 7 provides the consolidated list of additional SRS (functionality and performance) associated to failure conditions.

SRS ID	Additional Safety Requirements at ATS Service level *(functionality & performance)*	Mitigated Operational Hazard
SRS 016	The delegation procedures shall be fully safety assessed and approved by the safety authorities of the parties involved in delegation	OH 01 OH 02 OH 03 OH 04 OH 05 OH 06

SRS 017	The receiving ATSU shall implement processes and procedures to manage failures of delegated ATM services after their successful delegation.	OH 01 OH 02 OH 03 OH 04 OH 05 OH 06

Table 77777: Additional SRS (functionality and performance) to mitigate operational hazards

Table 10 provides the SRS addressing integrity/reliability in order to limit the frequency with which the operational hazards (listed in section 4.4.1) could be allowed to occur.

The SRS derivation has been done 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**.

The formula used for the computation of the SRS is the following:

$$SRS = \frac{MTFoO_{relevant\_severy\_class}}{N \times IM}$$

where:

- $MTFoO_{relevant\_severy\_class}$ stands for the Maximum Tolerable Frequency of Occurrence being the maximum probability of the hazard's effect;
- N is the overall number of operational hazards for a given severity class at a given barrier:
- IM is the Impact Modification factor to take account of additional information regarding the operational effect of the hazard, in particular related to the number of aircraft exposed to the operational hazard.

Severity Class	*Hazardous situation*	*Operational Effect*	*MTFoO [per fh]*
MAC-SC1	A situation where an aircraft comes into physical contact with another aircraft in the air.	Accident - Mid air collision (MF3)	1e-9
MAC-SC2a	A situation where an imminent collision was not mitigated by an airborne collision avoidance but for which geometry has prevented physical contact.	Near Mid Air Collision (MF3a)	1e-6
MAC-SC2b	A situation where airborne collision avoidance prevents near collision	Imminent Collision	1e-5

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Severity Class	*Hazardous situation*	*Operational Effect*	*MTFoO [per fh]*
		(MF4)	
MAC-SC3	A situation where an imminent collision was prevented by ATC Collision prevention	Imminent Infringement (MF5-8)	1e-4
MAC-SC4a	A situation where an imminent infringement coming from a crew/aircraft induced conflict was prevented by tactical conflict management	Tactical Conflict (crew/aircraft induced) (MF6.1)	1e-3
MAC-SC4b	A situation where an imminent infringement coming from a planned conflict was prevented by tactical conflict management	Tactical Conflict (planned) (MF5.1)	1e-2

Table 88888 SESAR Risk Classification Scheme (TMA and En-Route)

Severity Class	*Number of operational hazards per Severity Class per Accident Type*				
	MAC (ER&TMA)	*RWY Coll.*	*CFIT*	*TWY Coll.*	*WK-FA*
SC1	1	1	5	1	1
SC2	n/a	n/a	10	n/a	n/a
SC2a	5	5	n/a	5	5
SC2b	10	10	n/a	10	5
SC3	25	20	n/a	20	n/a
SC3a	n/a	n/a	50	n/a	5
SC3b	n/a	n/a	50	n/a	5
SC4	n/a	30	n/a	30	5
SC4a	30	n/a	n/a	n/a	n/a
SC4b	100	n/a	n/a	n/a	n/a

Table 99999: Maximum Hazard Numbers per Severity Class

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SRS ID	Safety Requirements at ATS Service level *(integrity/reliability)*	Related Operational Hazard	Severity & IM
SRS-018	The frequency of occurrence of Loss of Service preventing controller from managing one or many aircraft for receiving ATSU shall not be more than 1,2 1e-6 [sector operating hours].	OH 01	MAC-SC2a
SRS-019	The frequency of occurrence of Loss of Service preventing controller from managing one or many aircraft for both delegating and receiving ATSU shall not be more than 1,2 1e-6 [sector operating hours].	OH 02	MAC-SC2a
SRS-020	The frequency of occurrence of Service Loss (one/two workstation/s) for receiving ATSU" shall be no greater than 2,4 1e-6 [sector operating hours]	OH 03	MAC-SC3
SRS-021	The frequency of occurrence of Service Loss (one/two workstation/s) for both delegating and receiving ATSU" shall be no greater than 2,4 1e-6 [sector operating hours]	OH 04	MAC-SC3
SRS-022	The frequency of occurrence of Loss of Service resulting in "Detected corruption for receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic shall be no greater than 6,0 1e-7 [sector operating hours]	OH 05	MAC-SC2b
SRS-023	The frequency of occurrence of Loss of Service resulting in "Detected corruption for both delegating and receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic shall be no greater than 6,0 1e-7 [sector operating hours]	OH 05	MAC-SC2b
SRS-024	The frequency of occurrence of Loss of Service resulting in "Undetected corruption for receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic shall be no greater than 1,2 1e-7 [sector operating hours]	OH 06	MAC-SC2a
SRS-025	The frequency of occurrence of Loss of Service resulting in "Undetected corruption for both delegating and receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic shall be no greater than 1,2 1e-7 [sector operating hours]	OH 06	MAC-SC2a

Table 1010101~~10~~: Safety Requirements at Service level - integrity/reliability

4.5 Process assurance of the Safety Specification at ATS Service level

A safety team encompassing controllers, engineers, Safety and Human Performance specialists have supported this safety assessment. In addition to the activities conducted at OSED level, the first step was the validation of the SPR level model, then the initial SRS and SRD derived at V2 have been analysed and refined with the derivation process detailed in the dedicated Appendixes of this document. In addition to the SAF/HP workshop, several meetings were organised to consolidate the list of safety requirements.

Safety Requirements at Service level	Process description	Personnel involved
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-002 The decision for delegation abortion by the Supervisor in the Receiving ATSU shall be taken timely.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-003 The delegating ATSU and the receiving ATSU as well as other concerned parties shall mutually agree upon operational procedures of the delegated airspace.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-004 All relevant third parties shall be informed about an aborted delegation.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-005 The receiving ATCO team shall have the complete traffic situational awareness for the delegated sector following the traffic exchange with the delegating ATCO team.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SRS-006 One ATCO shall be in control of the delegated sector during all phases of the delegation procedure.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-007 The operational Supervisor of the receiving ATSU shall inform all relevant third parties about the successful completion of the delegation.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-008 Special procedures as defined by delegation contracts regulating the initiation, execution and termination of the delegation shall be in place with the ATSU(s) adjacent to sectors subject delegation.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-009 The operational Supervisor of the delegating ATSU shall inform operational Supervisor(s) of adjacent ATSU(s) when the delegation procedure is triggered.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-010 All procedures concerning involved parties in contingency delegation mode shall have a well-defined contingency plan including legal operational procedures and definition of responsibility for the service provision.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-011 The operational Supervisor of the failing ATSU shall be	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to	**Safety experts** **ATCOs** **Operational experts**

Co-funded by the European Union

responsible to decide if the ATSU has a contingency case	address properly safety aspects)	
SRS-012 The operational Supervisor of the failing ATSU shall be responsible to decide if a contingency delegation is initiated.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-013 The operational Supervisor of the failing ATSU of the failing ATSU shall request contingency delegation at an aiding ATSU.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-014 The operational Supervisor of the aiding ATSU shall decide if contingency delegation can be provided.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-015 The receiving ATSU shall have opportunity to monitor the traffic load in the receiving sector(s) in order to prevent overload situations.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-016 The delegation procedures shall be fully safety assessed and approved by the safety authorities of the parties involved in delegation	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-017 The receiving ATSU shall implement processes and procedures to manage failures of delegated ATM services after their successful delegation.	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**

SRS-018 The frequency of occurrence of Loss of Service preventing controller from managing one or many aircraft for receiving ATSU shall not be more than 1,2 1e-6 [sector operating hours].	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-019 The frequency of occurrence of Loss of Service preventing controller from managing one or many aircraft for both delegating and receiving ATSU shall not be more than 1,2 1e-6 [sector operating hours].	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-020 The frequency of occurrence of Service Loss (one/two workstation/s) for receiving ATSU" shall be no greater than 2,4 1e-6 [sector operating hours]	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-021 The frequency of occurrence of Service Loss (one/two workstation/s) for both delegating and receiving ATSU" shall be no greater than 2,4 1e-6 [sector operating hours]	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-022 The frequency of occurrence of Loss of Service resulting in "Detected corruption for receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic shall be no greater than 6,0 1e-7 [sector operating hours]	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-023	Workshops (concept description, preparing "the	**Safety experts**

The frequency of occurrence of Loss of Service resulting in "Detected corruption for both delegating and receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic shall be no greater than 6,0 1e-7 [sector operating hours]	road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**ATCOs** **Operational experts**
SRS-024 The frequency of occurrence of Loss of Service resulting in "Undetected corruption for receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic shall be no greater than 1,2 1e-7 [sector operating hours]	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**
SRS-025 The frequency of occurrence of Loss of Service resulting in "Undetected corruption for both delegating and receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic shall be no greater than 1,2 1e-7 [sector operating hours]	Workshops (concept description, preparing "the road" of Safety Assessment, preparing validation exercise to address properly safety aspects)	**Safety experts** **ATCOs** **Operational experts**

Table 1111111~~11~~ Consolidated list of PJ.10-W2-93 Safety Requirements at ATS service level

EUROPEAN PARTNERSHIP

Co-funded by the European Union

5 Safe Design of the Solution functional system

5.1 Overview of activities performed

This section addresses the following activities:

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

5.2 Design model of the Solution functional system

5.2.1 Description of the Design Model

This section presents the System Functionality & Flow Models (NSV-4 EATMA diagram) developed in the context of the solution. It describes the main tasks and machine functions in accordance with the delegation process for a Y architecture. For further details, please refer to OSED Part I [15][15]~~[12]~~ and TS/IRS **Error! Reference source not found.Error! Reference source not found.**~~[14]~~ documents.

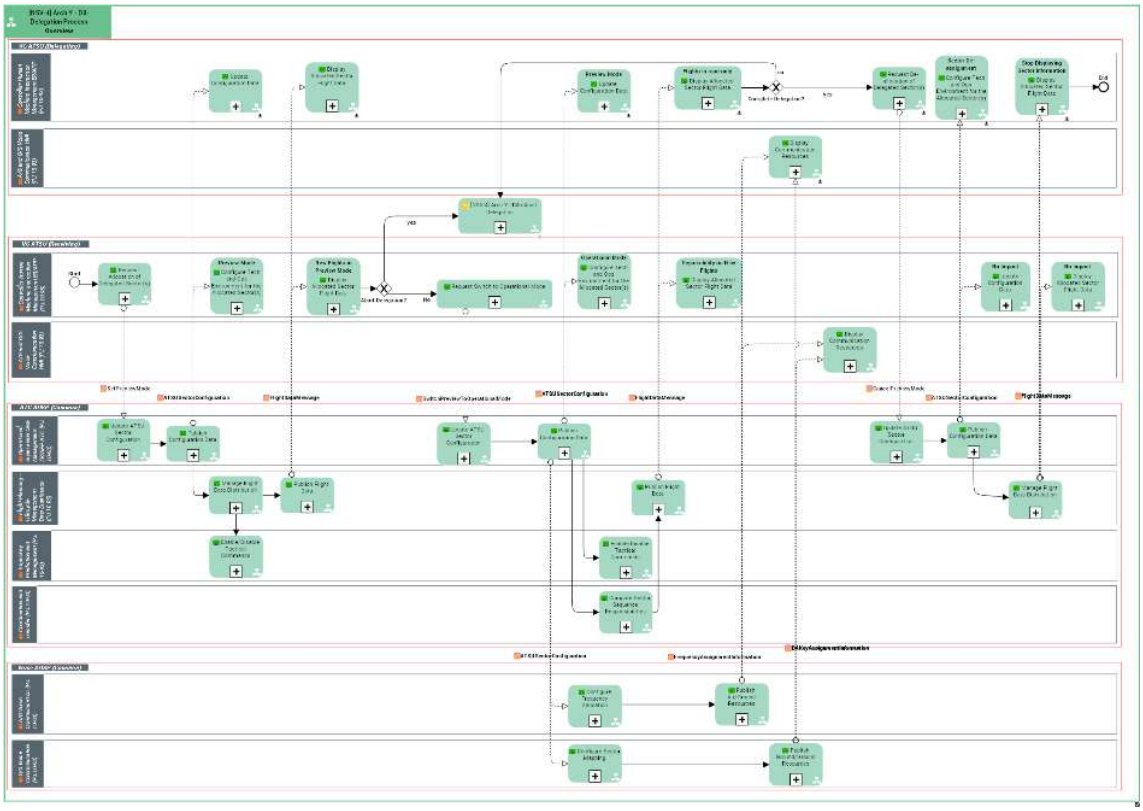

Figure 11111. [NSV-4] Arch Y - D0-Delegation Process Overview

Function	Description
Compute Sector Sequence Responsibilities	Compute the sectors/units that will either control the flight, or need to be coordinated or informed.
Configure Frequency Allocation	Reconfiguration of frequency assignment(s) of the VCS position(s).
Configure Sector Mapping	Reconfiguration of the sector mapping of the VCS position(s).
Configure Tech and Ops Environment for the Allocated Sector(s)	Initialisation of the HMI with environment and operational data relative to the sector(s) allocated to the position.
Display Allocated Sector Flight Data	After sector reconfiguration and impacts in sector control sequence, update the concerned flights of the position.
Display Communication Resources	Display frequency and sector mapping of the VCS position.
Enable/Disable Tactical Commands	Enable, or disable, the processing of controller commands that have been input when the position is respectively set in operation or in

	preview mode. This function, when implemented, may as well be directly allocated to the CHMI FB.
Manage Flight Data Distribution	Determine how, and according to which criteria, flight distribution is to be performed for each position/Controller.
Publish Air/Ground Resources	Publication of new frequency assignments to the VCS positions.
Publish Configuration Data	Publishes configuration data to relevant subscribers.
Publish Flight Data	Distribution of Flight Plan Data to the relevant subscribers.
Publish Ground/Ground Resources	Publication of a new sector mapping configuration to the VCS positions.
Request Allocation of Delegated Sector(s)	Following a delegation agreement, request for setting the allocation of the delegated sector on the working position.
Request Delegation Abortion	Request for triggering the abortion of a delegation process that has been initiated but cannot be completed.
Request Switch to Operational Mode	Trigger for switching working position(s) from preview mode to operational mode.
Update ATSU Sector Configuration	Updates the ATSU sector configuration with requested new configuration.
Update Configuration Data	Following reception of a configuration change, analyse the impact on the working position and process the changes if any required.

Table 1212121212. NSV-4 Functions

5.2.2 Task Analysis

A task analysis has not been produced in the framework of the HP assessment.

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

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

Table below provides the list of Safety Requirements at Design level (functionality and performance) for Normal conditions of operations derived by mapping the SRS for Normal conditions of operations (documented in section 4.2) onto the related elements of the Design Model.

Safety Requirement ID [Design Model Element]	Safety Requirement (functionality & performance)	Derived from SRS (ID)

SRD-001 [Preview Mode]	The receiving ATCO team(s) shall be able to preview traffic of the sector to be delegated on their CWP.	SRS-001
SRD-002 [Preview Mode]	The receiving ATSU shall activate the preview mode for the sectors to be delegated.	SRS-001
SRD-003 [Preview Mode]	The frequency of the delegated sector should be activated automatically to Rx at the Executive CWP of the receiving ATSU when the receiving ATSU activates the preview mode for this sector.	SRS-001
SRD-004 [Operational Mode]	The delegation of ATS provision shall be supported by the CWP (ATS and Voice).	SRS-001 SRS-005 SRS-006
SRD-005 [Operational Mode]	The receiving ATCO team(s) shall contact the delegating ATCO team(s) and exchange the traffic situation of the sector to be delegated when starting the Exchange Traffic Situation phase.	SRS-001 SRS-005
SRD-006 [Preview/Operational Mode]	The receiving ATSU shall request to switch the CWPs at the receiving ATCO team from Preview Mode to Operational mode.	SRS-001
SRD-007 [Request Delegation/ Request Allocation of delegated sectors]	The ATCOs of the receiving ATSU shall have the appropriate endorsement(s) to operate the sector or sector configurations to be delegated.	SRS-001
SRD-008 [Operational Mode]	The delegation process shall not be performed at the moment the receiving ATSU is considered at full capacity.	SRS-001
SRD-009 [Abort Delegation]	The operational Supervisor of receiving ATSU shall be supported by the system to abort the ongoing delegation.	SRS-001 SRS-002 SRS-004 SRS-007 SRS-009

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SRD-010 [Operational Mode]	A receiving ATSU shall be appropriately equipped and staffed in order to provide ATS in the pre-defined airspace of the delegating ATSU.	SRS-001 SRS-005
SRD-011 [Operational Mode]	The receiving ATCO team shall coordinate about proceeding to the next phase of the Delegation Procedure at the end of the Delegation Preparation phase.	SRS-001
SRD-012 [Operational Mode]	The delegating ATCO team shall use the WEST checklist for a systematic approach of the traffic handover to the receiving ATCO team.	SRS-001
SRD-013 [Operational Mode]	The delegating ATCO team shall be able to identify the flights that need to be handed over.	SRS-001
SRD-014 [Operational Mode]	The receiving ATCO team shall read-back and acknowledge all flights being pointed out by the delegating ATCO team.	SRS-001
SRD-015 [Traffic Exchange/Operational Mode]	The ATCO team(s) of the receiving ATSU shall coordinate internally to agree on entering the Enter Operational Mode phase after exchanging traffic with the ATCO team of the delegating ATSU.	SRS-001
SRD-016 [Preview/Operational Mode]	The delegating and receiving ATCO teams shall coordinate and acknowledge the point when the preview mode is switched to operational mode at the receiving ATSU.	SRS-001
SRD-017 [Operational Mode]	The ATCO of the receiving ATSU shall be able to identify which sector is in operational mode	SRS-001 SRS-005
SRD-018 [Preview/Operational Mode]	The receiving Executive should have a radio check of the frequency of the delegated sector before switching to operational mode.	SRS-001
SRD-019 [Preview/Operational Mode]	The delegating ATCO team shall switch the frequency of the delegated sector from Tx/Rx to Rx when switching from operational mode to preview mode in the delegating ATSU.	SRS-001
SRD-020 [Preview/Operational Mode]	The frequency of the delegated sector should be switched automatically from Tx/Rx to Rx at the Executive CWP of the delegating ATSU when switching from	SRS-001

	operational mode to preview mode in the delegating ATSU.	
SRD-021 [Preview/Operational Mode]	The frequency of the delegated sector should be switched automatically from Rx to Tx/Rx at the Executive CWP of the receiving ATSU when switching from preview mode to operational mode for this sector in the receiving ATSU.	SRS-001
SRD-022 [Preview Mode]	The delegating ATSU shall terminate the preview mode for the delegated sector after a time defined in the delegation agreement.	SRS-001 SRS-003 SRS-008
SRD-023 [Preview Mode]	The Executive ATCO of the delegating ATSU shall disable the frequency of the delegated sector when the preview mode is terminated.	SRS-001
SRD-024 [Preview Mode]	The frequency of the delegated sector should automatically be disabled when the preview mode is terminated at the delegating ATSU.	SRS-001
SRD-025 [Preview Mode]	The ATCO of the receiving ATSU shall be able to identify the termination of the preview mode at the delegating ATSU when the preview mode is supported by the system.	SRS-001
SRD-026 [all phases of the delegation]	ATSEP of the ATSU shall be able to control systems running at the ATSU, including network connection to ADSP at all times.	SRS-001

Table 1313131~~13~~. Safety Requirements at design level (functionality and performance) satisfying SRS for Normal conditions of operation

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

The Use Cases reported in section 3.3 of PJ.10-W2-93 SPR/INTEROP/OSED V3 [15][15]~~[12]~~ have been considered in the framework of V3 PJ.10-W2-93.

From the analysis of the NOV-5 / NSV-4 diagrams developed in the framework of the solution, the SRD presented in section 5.3.3 have been derived. No additional SRDs considered after static analysis.

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

From the execution of Validation exercise EXE3, one additional SRD has been derived:

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SRD-027: The delegating and receiving ATCOs shall be supported by appropriate automation and HMI functions to fully exchange relevant information and safely handover the responsibility.

Further information is provided in the Appendix E.3 of this document.

5.3.4 Effects on Safety Nets – Normal conditions of operation

No impact on safety nets has been evaluated.

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

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

Table 14 provides the list of Safety Requirements at Design level for Abnormal conditions of operations.

Safety Requirement ID [Design Model Element]	Safety Requirement (functionality & performance) for abnormal operation	Derived from SRS (ID)
SRD-028 [Operational Mode]	The existing safety level shall not be impacted negatively in case of contingency delegation.	SRS 010 SRS 011 SRS 012 SRS 013 SRS 014 SRS 015
SRD-029 [Operational Mode]	A delegation agreement shall define the constraints and performance boundaries when delegated ATM services are operated in degraded mode.	

Table 1414141414. Safety Requirements at design level (functionality and performance) satisfying SRS for Abnormal conditions

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

No additional Safety Requirements (Functionality and Performance) for abnormal conditions of operation have been found. The SRD derived in 5.4.1 used already a dynamic approach, by mapping the requirements to the SRS (Functionality and Performance) which were derived based on the OSED Use Cases and the analysis of the NOV-5 / NSV-4 diagrams developed in the framework of the solution. In addition, the safety-related results obtained from the execution of the Real Time Simulations confirmed the requirement already derived (the SRD reported in 5.3.3 are valid also for abnormal conditions of operation).

5.5 Safety Requirements at Design level addressing Internal Functional System Failures

5.5.1 Design analysis addressing internal functional system failures

A top-down analysis has been conducted in order to:

- Ensure identification of a complete list of Solution functional system failures that could cause each operational hazard
- Ensure identification of the required Mitigation means preventing causes to occur or preventing their effect to propagate towards each operational hazard
- Contribute to demonstrate the feasibility and effectiveness of the contingency procedures associated to the degraded modes of operation in which the functional system might enter as a result of certain failure modes
- Determine potential common cause failures and ensure their mitigation through dedicated SRD or design choice.

Further information is reported in Appendix G.

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

This section provides the consolidated list of initial Safety Requirements at Design level associated to internal system failures. Only mitigating requirements have been derived within this assessment. No Quantitative SRD (integrity/ reliability) have been derived in this safety assessment and they will need to be done by the industry in the validation stages prior to implementation (i.e. V4 onwards).

However, some reliability requirements have been considered within the technological safety assessment performed within solutions PJ.10-W2-93A-93B and 93C. For more information, please refer to TS/IRS Part I [17] and II [10].

Safety Requirement ID	Safety Requirement at Design level (SRD) (functionality & performance)	Derived from SRS (ID) or Common cause failure
SRD-030	Recurrent Training shall be provided to ATCOs in order to guarantee an optimal maintenance of competence for airspaces associated with a delegation agreement.	**SRS 016** **SRS 017**
SRD-031	The ATSEPs of the delegating and receiving ATSU and the ATSEPs of the ADSP shall be regularly trained to operate their technical systems.	**SRS 018** **SRS 019**
SRD-032	The ATSEPs of the delegating and receiving ATSU and the ATSEPs of the ADSP shall be licensed for the technical systems they are operating.	**SRS 020** **SRS 021**
SRD-033	In case of contingency, coordination and synchronization messages shall be exchanged between ATSUs.	**SRS 022** **SRS 023**
SRD-034	A delegation agreement shall clearly define how failures of delegated ATM services need to be handled after their successful delegation.	**SRS 024** **SRS 025**
SRD-035	The operational Supervisor and/or the ATSEP shall be able to make the system input to abort a delegation.	
SRD-036	An ATSU shall have the capability to manage unexpected events and problems that occur during and after a delegation.	

Table 1515151~~15~~. SRD (functionality & performance) to mitigate the operational hazards

5.6 Realism of the safe design

Considering the development and results of validation exercises executed at V3 and the safety assessment performed, it can be stated that safety assumptions are correct and coherent with the described scenarios, and that the SRD are testable and possible to satisfy. All of this of course depending on the correct implementation of the identified Recommendations (VALR).

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, etc.

5.7 Process assurance for a Safe Design

A safety team encompassing controllers, engineers, Safety and Human Performance specialists have supported this safety assessment. The safety requirements have been derived in normal, abnormal and failure conditions being in line with the SRM process. In addition to the SAF/HP meeting related to the exercises, several meetings were organised to consolidate the list of safety requirements. The

EUROPEAN PARTNERSHIP

Co-funded by the European Union

following table provides the traceability between SAR safety requirements (SRD) and SPR/INTEROP-OSED requirements with category Safety

SRD ID	SPR/INTEROP-OSED requirements ID	Requirement Text
SRD-001	REQ-PJ.10-W2.93-SPRINTEROP-0014	The receiving ATCO team(s) shall be able to preview traffic of the sector to be delegated on their CWP.
SRD-002	REQ-PJ.10-W2.93-SPRINTEROP-0088	The receiving ATSU shall activate the preview mode for the sectors to be delegated.
SRD-0003	REQ-PJ.10-W2.93-SPRINTEROP-0089	The frequency of the delegated sector should be activated automatically to Rx at the Executive CWP of the receiving ATSU when the receiving ATSU activates the preview mode for this sector.
SRD-004	REQ-PJ.10-W2.93-SPRINTEROP-0006	The delegation of ATS provision shall be supported by the CWP (ATS and Voice).
SRD-005	REQ-PJ.10-W2.93-SPRINTEROP-0022	The receiving ATCO team(s) shall contact the delegating ATCO team(s) and exchange the traffic situation of the sector to be delegated when starting the Exchange Traffic Situation phase.
SRD-006	REQ-PJ.10-W2.93-SPRINTEROP-0025	The receiving ATSU shall request to switch the CWPs at the receiving ATCO team from Preview Mode to Operational mode.
SRD-007	REQ-PJ.10-W2.93-SPRINTEROP-0012	The ATCOs of the receiving ATSU shall have the appropriate endorsement(s) to operate the sector or sector configurations to be delegated.
SRD-008	REQ-PJ.10-W2.93-SPRINTEROP-SAF.0006	The delegation process shall not be performed at the moment the receiving ATSU is considered at full capacity.
SRD-009	REQ-PJ.10-W2.93-SPRINTEROP-0056	The operational Supervisor of receiving ATSU shall be supported by the system to abort the ongoing delegation.
SRD-010	REQ-PJ.10-W2.93-SPRINTEROP-0005	A receiving ATSU shall be appropriately equipped and staffed in order to provide ATS in the pre-defined airspace of the delegating ATSU.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SRD-011	REQ-PJ.10-W2.93-SPRINTEROP-0018	The receiving ATCO team shall coordinate about proceeding to the next phase of the Delegation Procedure at the end of the Delegation Preparation phase.
SRD-012	REQ-PJ.10-W2.93-SPRINTEROP-0092	The delegating ATCO team shall use the WEST checklist for a systematic approach of the traffic handover to the receiving ATCO team.
SRD-013	REQ-PJ.10-W2.93-SPRINTEROP-0093	The delegating ATCO team shall be able to identify the flights that need to be handed over.
SRD-014	REQ-PJ.10-W2.93-SPRINTEROP-0094	The receiving ATCO team shall read-back and acknowledge all flights being pointed out by the delegating ATCO team.
SRD-015	REQ-PJ.10-W2.93-SPRINTEROP-0024	The ATCO team(s) of the receiving ATSU shall coordinate internally to agree on entering the Enter Operational Mode phase after exchanging traffic with the ATCO team of the delegating ATSU.
SRD-016	REQ-PJ.10-W2.93-SPRINTEROP-0096	The delegating and receiving ATCO teams shall coordinate and acknowledge the point when the preview mode is switched to operational mode at the receiving ATSU.
SRD-017	REQ-PJ.10-W2.93-SPRINTEROP-0097	The ATCO of the receiving ATSU shall be able to identify which sector is in operational mode
SRD-018	REQ-PJ.10-W2.93-SPRINTEROP-0100	The receiving Executive should have a radio check of the frequency of the delegated sector before switching to operational mode.
SRD-019	REQ-PJ.10-W2.93-SPRINTEROP-0101	The delegating ATCO team shall switch the frequency of the delegated sector from Tx/Rx to Rx when switching from operational mode to preview mode in the delegating ATSU.
SRD-020	REQ-PJ.10-W2.93-SPRINTEROP-0102	The frequency of the delegated sector should be switched automatically from Tx/Rx to Rx at the Executive CWP of the delegating ATSU when switching from

		operational mode to preview mode in the delegating ATSU.
SRD-021	REQ-PJ.10-W2.93-SPRINTEROP-0103	The frequency of the delegated sector should be switched automatically from Rx to Tx/Rx at the Executive CWP of the receiving ATSU when switching from preview mode to operational mode for this sector in the receiving ATSU.
SRD-022	REQ-PJ.10-W2.93-SPRINTEROP-0107	The delegating ATSU shall terminate the preview mode for the delegated sector after a time defined in the delegation agreement.
SRD-023	REQ-PJ.10-W2.93-SPRINTEROP-0108	The Executive ATCO of the delegating ATSU shall disable the frequency of the delegated sector when the preview mode is terminated.
SRD-024	REQ-PJ.10-W2.93-SPRINTEROP-0109	The frequency of the delegated sector should automatically be disabled when the preview mode is terminated at the delegating ATSU.
SRD-025	REQ-PJ.10-W2.93-SPRINTEROP-0110	The ATCO of the receiving ATSU shall be able to identify the termination of the preview mode at the delegating ATSU when the preview mode is supported by the system.
SRD-026	REQ-PJ.10-W2.93-SPRINTEROP-0046	ATSEP of the ATSU shall be able to control systems running at the ATSU, including network connection to ADSP at all times.
SRD-027	REQ-PJ.10-W2.93-SPRINTEROP-0112	The delegating and receiving ATCOs shall be supported by appropriate automation and HMI functions to fully exchange relevant information and safely handover the responsibility.
SRD-028	REQ-PJ.10-W2.93-SPRINTEROP-SAF.0004	The existing safety level shall not be impacted negatively in case of contingency delegation.
SRD-029	REQ-PJ.10-W2.93-SPRINTEROP-0072	A delegation agreement shall define the constraints and performance boundaries when delegated ATM services are operated in degraded mode.

SRD-030	REQ-PJ.10-W2.93-SPRINTEROP-0037	Recurrent Training shall be provided to ATCOs in order to guarantee an optimal maintenance of competence for airspaces associated with a delegation agreement.
SRD-031	REQ-PJ.10-W2.93-SPRINTEROP-0068	The ATSEPs of the delegating and receiving ATSU and the ATSEPs of the ADSP shall be regularly trained to operate their technical systems.
SRD-032	REQ-PJ.10-W2.93-SPRINTEROP-0070	The ATSEPs of the delegating and receiving ATSU and the ATSEPs of the ADSP shall be licensed for the technical systems they are operating.
SRD-033	REQ-PJ.10-W2.93-SPRINTEROP-0042	In case of contingency, coordination and synchronization messages shall be exchanged between ATSUs.
SRD-034	REQ-PJ.10-W2.93-SPRINTEROP-0073	A delegation agreement shall clearly define how failures of delegated ATM services need to be handled after their successful delegation.

Table 1616161616. Safety Requirements Traceability

6 SAfety Criteria achievability

As specified in the Safety Plan, safety evidence will be collected from the validation exercises planned as per the Validation Plan. Safety Validation Objectives are defined in the Validation Plan and the safety-related outcomes of the validation exercises will feed the Safety Criteria and will be traced back to the safety validation objectives. Decision for deriving (or not) Safety Requirements will be taken from these results.

Driven by the SACs defined in section 3.4, the following safety-related validation objectives and associated success criteria have been identified:

Safety Validation Objective	Associated Success Criteria and related SAC	
OBJ-PJ.10-W2-93-V3-VALP-014 To assess the impact in terms of Safety of the ATM services provision delegation concept in nominal conditions	**CRT-PJ.10-W2-93-V3-VALP-014-001** The level of safety remains at an acceptable level according to ATCo's expert judgment before, during and after the delegation of ATM services provision in nominal conditions. **SAC#01** **SAC#02** **SAC#03**	**CRT-PJ.10-W2-93-V3-VALP-014-002** Impact remains acceptable according to ATCo expert judgment in terms of the management and provision of aircraft separation before, during and after the delegation of ATM services provision in nominal conditions are identified. **SAC#01** **SAC#02** **SAC#03**
OBJ-PJ.10-W2-93-V3-VALP-015 To assess the impact in terms of Safety of the ATM services provision delegation concept in abnormal conditions	**CRT-PJ.10-W2-93-V3-VALP-015-001** The level of safety remains at an acceptable level according to ATCo's expert judgment before, during and after the delegation of ATM services provision in abnormal conditions. **SAC#01** **SAC#02** **SAC#03**	**CRT-PJ.10-W2-93-V3-VALP-015-002** Impact remains acceptable according to ATCo's expert judgment in terms of the management and provision of aircraft separation before, during and after the delegation of ATM services provision in abnormal conditions are identified. **SAC#01** **SAC#02** **SAC#03**

Table 1717171717. Safety validation objectives and related Safety Criteria

An overview of the safety results of the V3 exercises is presented in Appendix H.

7 Acronyms and Terminology

Term	Definition
ACC	Area Control Centre
ADSP	ATM Data Service Provider
AIM	Accident Incident Model
ANSP	Air Navigation Service Provider
AoR	Area of Responsibility
APP	Approach
ARES	Airspace Reservation
AU	Airspace Users
ATCO	Air Traffic Controller
ATSEP	Air traffic safety electronics personnel
ATSU	Air Traffic Services Unit
AU	Airspace User
CNS	Communication Navigation Surveillance
CPDLC	Controller-pilot data link communications
Ha	Hazard inherent to aviation
HMI	Human Machine Interface
HP	Human Performance
IFR	Instrument Flight Rules
INAP	Integrated Network Management and Extended ATC Planning
LoA	Letter of Agreement
MAC-ER	Mid Air Collision En-Route
OE	Operational Environment
OH	Operational Hazard

EUROPEAN PARTNERSHIP

Co-funded by the European Union

OLDI	On-Line Data Interchange
OSED	Operational Service Environment Description
SAC	Safety Criteria
SAP	Safety Assessment Plan
SAR	Safety Assessment Report
SPR	Safety Performance Requirements
SRD	Safety Requirements at ATS Design level
SRM	SESAR Safety Reference Methodology
SRS	Safety Requirements at ATS Service level
TRA	Temporary Reserved Area
TSA	Temporary Segregated Area
UC	Use Case
VALP	Validation Plan
VALR	Validation Report
VCS	Voice Communication System

Table 1818181818: Acronyms and Terminology

EUROPEAN PARTNERSHIP

Co-funded by the European Union

8 References

Safety

[1] SESAR 2020 Safety Policy

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

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

[4] STELLAR Slideboard, Safety (complementary guidance)

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

[6] SESAR2020 PJ.10-W2-93 V2 Validation Plan Part II – Safety Assessment Plan

[7] SESAR2020 PJ.10-W2-93 V3 Validation Plan Part II – Safety Assessment Plan

[8] SESAR2020 PJ.32 Validation Plan Part II – Safety Assessment Plan

[9] SESAR2020 PJ.32 SPR-INTEROP/OSED Part II – Safety Assessment Report

[10] SESAR 2020 PJ.10-W2-93A Final TS/IRS TRL6 (and 93B, 93C TRL4) - Part II - Safety Assessment Report

Human Performance

[11] SESAR Human Performance Assessment Process V1 to V3- including VLDs - latest edition accessible in STELLAR Program Library

[12] SESAR2020 PJ.10-W2-93 V3 Validation Plan Part IV – Human Performance Assessment Plan

[13] SESAR2020 PJ.10-W2-93 V3 OSED Part IV – Human Performance Assessment Report

General

[14] SESAR 2020 PJ19 Validation Targets (2020)

[15] SESAR2020 PJ.10-W2-93 V3 SPR-INTEROP/OSED Part I

[16] SESAR 2020 PJ.10-W2-93 V3 Validation Plan Part I

[17] SESAR 2020 PJ.10-W2-93A Final TS/IRS TRL6 (and 93B, 93C TRL4)

[18] SESAR2020 PJ.32 SPR-INTEROP/OSED Part I

[19]SESAR 2020 PJ.10-W2-93 V3 Validation Report

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix A Preliminary safety impact assessment

A.1 Relevant Hazards Inherent to Aviation

A pre-condition for performing the safety assessment for the introduction of a new Concept is to understand the impact it would have in the overall ATM risk picture. The SRM Guidance D and E provides a set of Accident Incident Models (AIM - one per each type of accident) which represent an integrated risk picture with respect to ATM contribution to aviation accidents.

In order to determine which AIM models are relevant for the PJ10 Solution 93, this section presents the relevant aviation hazards that have been identified within the HP&SAF scoping & change assessment session (using SRM Guidance F.2.2). The relevant hazards inherent to aviation with the corresponding ATM-related accident types and AIM models are presented in the Table below.

Hazards inherent to aviation	ATM-related accident type & AIM model
Ha#1: situation in which the intended trajectories of two or more aircraft are in conflict	Mid-Air Collision (MAC) En Route and associated AIM models
Ha#2: incursion in ARES (infringement by non-participating IFR traffic)	
Ha#3: ARES borders excursion by traffic using it	
Ha#4: encounters with adverse weather	

Table 191919~~19~~. Hazards inherent to aviation relevant for the Solution

Considering these hazards, relevant Accident Incident Model to be considered is **Mid-Air Collision-En route (MAC-ER)**.

A.2 Functional system-generated hazards (preliminary)

Based on the preliminary hazard identification conducted in the frame of the HP&SAF scoping & change assessment session, the table 2 lists the operational hazards that could be generated by the reference functional system.

Functional system-generated hazards (preliminary)	Impacted (new/modified) & justification
Hs 01: A situation where an imminent infringement coming from a planned conflict was prevented by tactical conflict management Tactical Conflict (planned)	Starting from this preliminary hazards, operational hazards have been identified. Please refer to section 4.4.1 and Annex D of this document.
Hs 02: A situation where an imminent collision was prevented by ATC Collision prevention	

Table 202020202~~0~~. Functional system-generated hazards applicable to the Solution (preliminary list)

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

This appendix presents the derivation of the SRS (functionality and performance) in order to mitigate the hazards inherent to aviation under normal conditions of operation.

B.1 EATMA Process models or alternative description

In PJ.10-W2-93 there are the process models shown below. They address the delegation process in both normal and contingency situation.

The following models support identified SRS on success approach. Figure 2 describes for the transfer of responsibility for the provision of ATM services in a volume of airspace between two ATSUs: the delegating ATSU and the receiving ATSU. The procedure is intended to be as generic as possible and to imitate as far as possible the common, everyday procedure used by a sector team when handing over responsibility for a sector(s) at the end of their shift to an incoming sector team. Therefore, the delegation procedure is applicable to all kinds of delegations, e.g. regular delegation at night-time, ATFCM-based delegation providing capacity-on-demand or even contingency cases. The procedure is a sequence of tasks performed by the delegating and receiving ATSU operational staff and, where necessary, technical staff. Figure 3 describes an overview of the contingency procedure. The Contingency Lifecyle starts with an unexpected severe event that causes the failure of an ATSU. Both procedures are detailed in the OSED Part I [15][15]~~[12]~~.

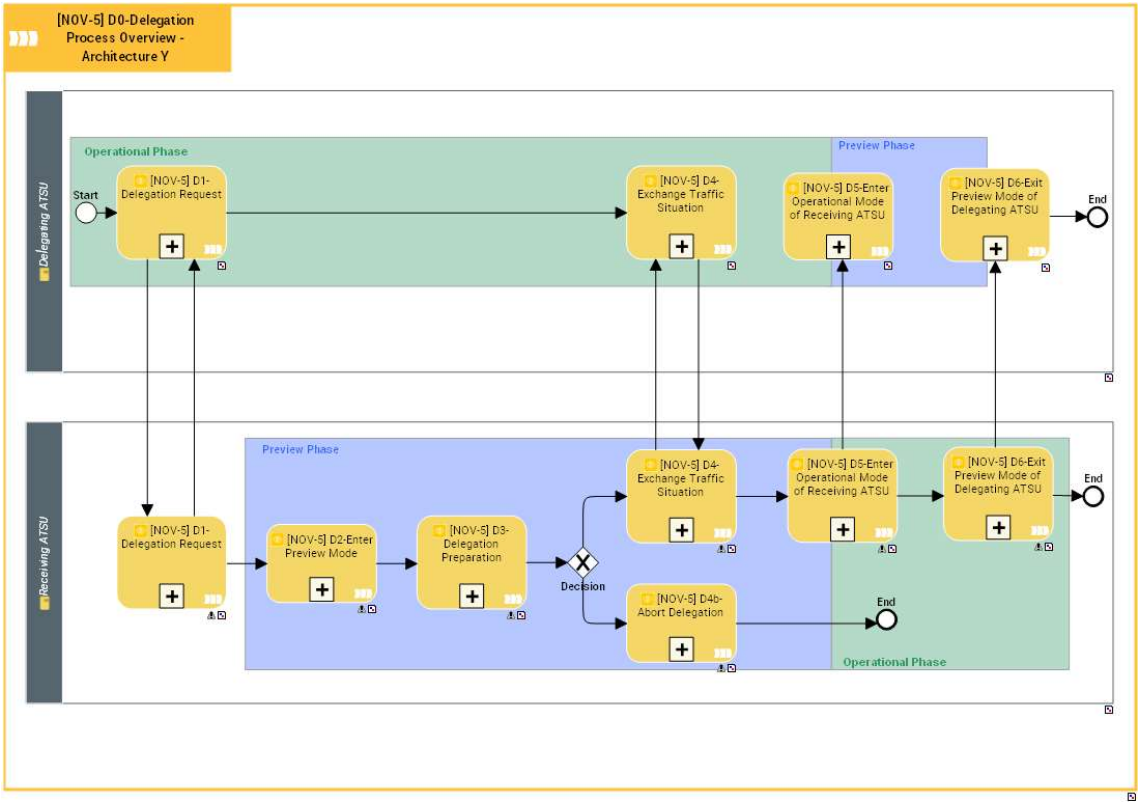

Figure ~~22222~~: Delegation Overview Process

EUROPEAN PARTNERSHIP
Co-funded by the European Union

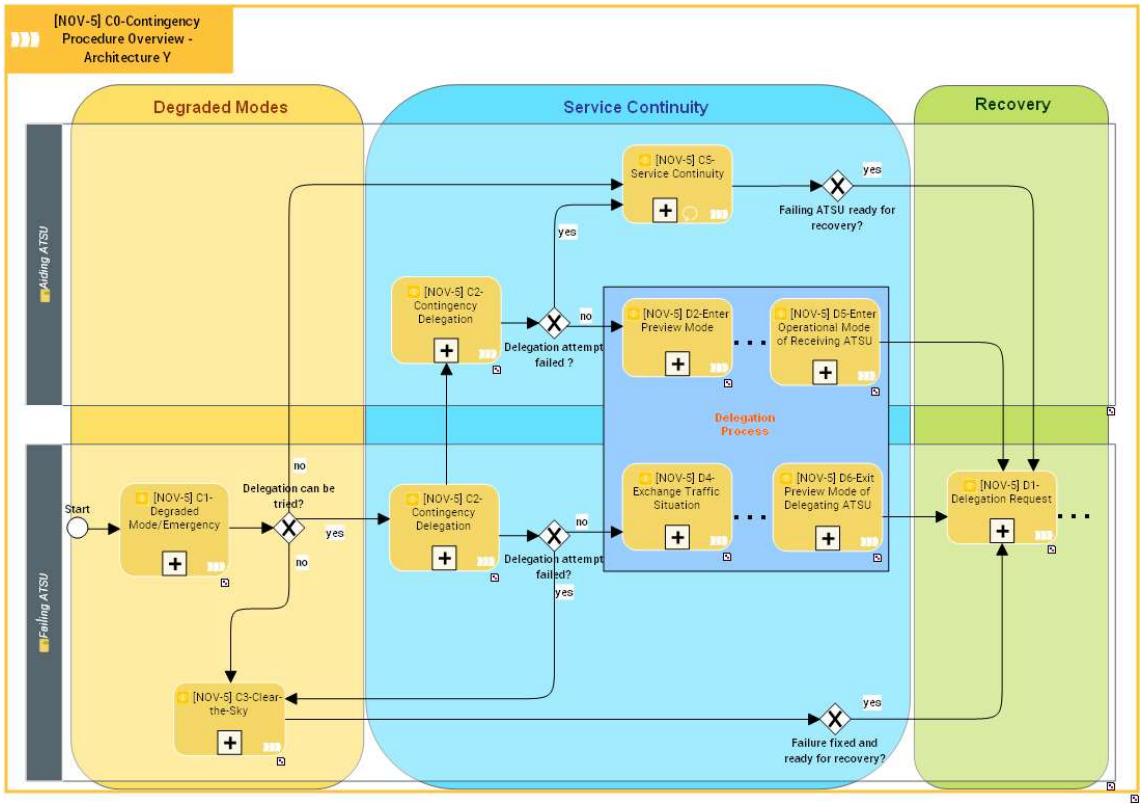

Figure 33333. Contingency Procedure

Finally, the eventuality of a problem in the receiving ATSU which cannot be resolved quickly (e.g. unavailability of radio communication or failure of the CWP) with the consecutive abortion of the delegation procedure has to be taken into account. In this case, either the receiving Executive or Planner ATCO informs the Supervisor of the receiving ATSU that a problem has occurred during the preparation of the CWPs. The receiving Supervisor then consults experts to decide if the problem can be fixed quickly and the delegation can be continued or if the delegation needs to be aborted. In the latter case the receiving Supervisor forwards this information about the abort to the delegating Supervisor who subsequently informs the ATCO team of the delegating ATSU about the abort of the delegation procedure.

On the receiving ATSU side, the Supervisor requests the switch of the CWPs from the Preview Mode back to the previous mode for the affected sector. This request is processed by the ADSP and redistributed to the CWPs.

The procedure ends here. The consequences of aborting the delegation procedure depends on the use case and is elaborated with more detail in more specific contexts.

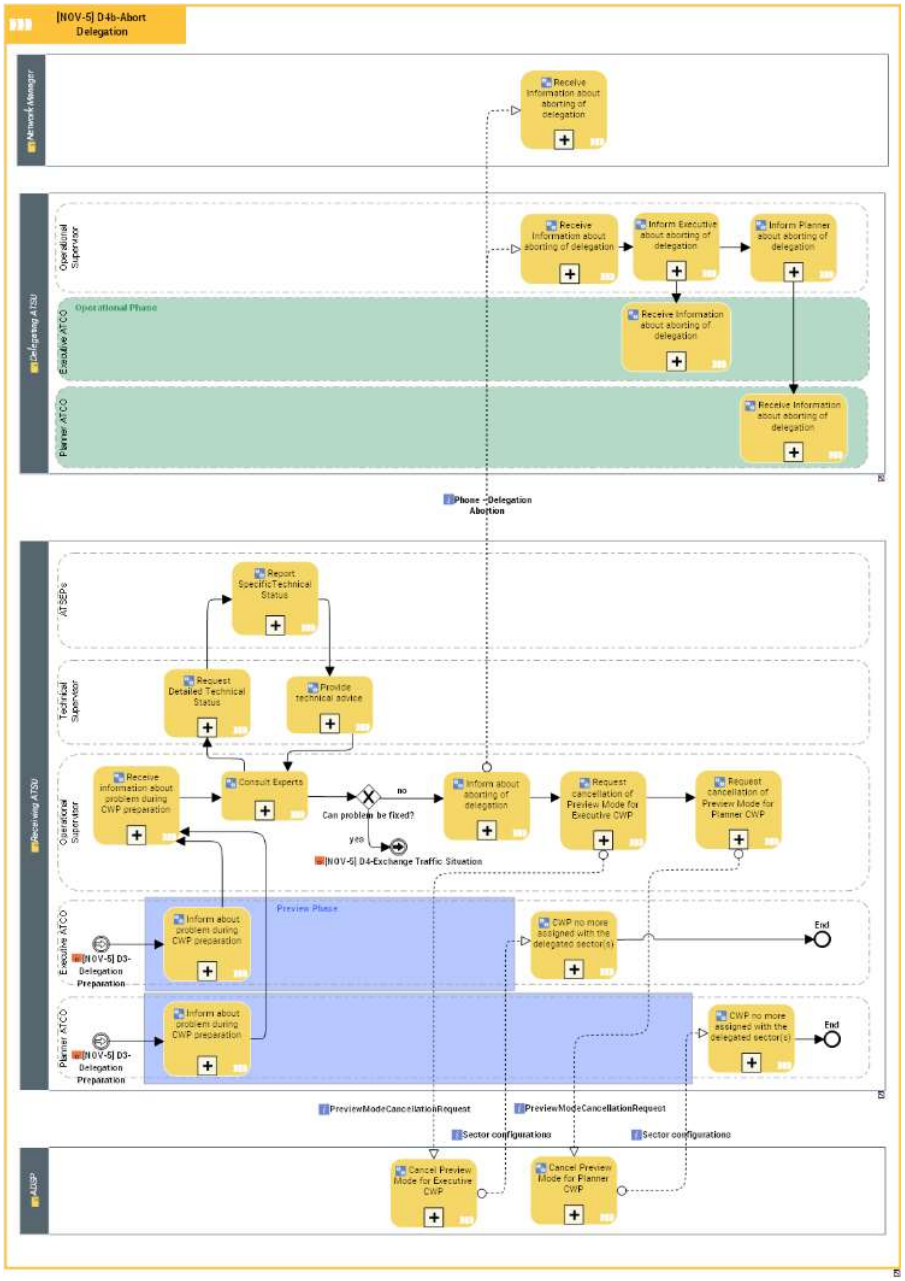

Figure 44444. [NOV-5] D4b-Abort Delegation

B.2 Derivation of SRS for Normal Operations

EUROPEAN PARTNERSHIP

Co-funded by the European Union

ATS Operational Service	EATMA Use Case-Activity or Flow	Derived SRS	Related SAC# (AIM Barrier or Precursor)
Maintain separation between aircrafts. Prevent an unauthorized entry into restricted airspace. Manage Trajectory.	Delegation Request / Operational Mode	**SRS-001** The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SAC#01** "Planning Conflicts" (MF5.1). **SAC#02** "ATC induced conflict" (MF7.1). **SAC#03** "Imminent Infringement" (MF5.9).
Maintain separation between aircrafts.	Abort Delegation	**SRS-002** The decision for delegation abortion by the Receiving ATSU (SUP) shall be taken timely.	**SAC#01** "Planning Conflicts" (MF5.1). **SAC#02** "ATC induced conflict" (MF7.1). **SAC#03** "Imminent Infringement" (MF5.9).
Maintain separation between aircrafts. Prevent an unauthorized entry into restricted airspace. Manage Trajectory.	Delegation Process Overview	**SRS-003** The delegating ATSU and the receiving ATSU as well as other concerned parties shall mutually agree upon operational procedures of the delegated airspace.	**SAC#01** "Planning Conflicts" (MF5.1). **SAC#02** "ATC induced conflict" (MF7.1). **SAC#03** "Imminent Infringement" (MF5.9).

EUROPEAN PARTNERSHIP

Co-funded by the European Union

ATS Operational Service	EATMA Use Case-Activity or Flow	Derived SRS	Related SAC# (AIM Barrier or Precursor)
Maintain separation between aircrafts.	Abort Delegation	**SRS-004** All relevant third parties shall be informed about an aborted delegation.	**SAC#01** "Planning Conflicts" (MF5.1). **SAC#02** "ATC induced conflict" (MF7.1). **SAC#03** "Imminent Infringement" (MF5.9).
Maintain separation between aircrafts. Prevent an unauthorized entry into restricted airspace. Manage Trajectory.	Exchange traffic	**SRS-005** The receiving ATCO team shall have the complete traffic situational awareness for the delegated sector following the traffic exchange with the delegating ATCO team.	**SAC#01** "Planning Conflicts" (MF5.1). **SAC#02** "ATC induced conflict" (MF7.1). **SAC#03** "Imminent Infringement" (MF5.9).
Maintain separation between aircrafts. Prevent an unauthorized entry into restricted airspace. Manage Trajectory.	Delegation Process Overview	**SRS-006** One ATCO shall be in control of the delegated sector during all phases of the delegation procedure.	**SAC#01** "Planning Conflicts" (MF5.1). **SAC#02** "ATC induced conflict" (MF7.1). **SAC#03** "Imminent Infringement" (MF5.9).
Maintain separation	Delegation Process Overview	**SRS-007** The operational Supervisor of the receiving ATSU shall inform all relevant third parties	**SAC#01**

Co-funded by the European Union

ATS Operational Service	EATMA Use Case-Activity or Flow	Derived SRS	Related SAC# (AIM Barrier or Precursor)
between aircrafts. Prevent an unauthorized entry into restricted airspace. Manage Trajectory.		about the successful completion of the delegation.	"Planning Conflicts" (MF5.1). **SAC#02** "ATC induced conflict" (MF7.1). **SAC#03** "Imminent Infringement" (MF5.9).
Maintain separation between aircrafts. Prevent an unauthorized entry into restricted airspace. Manage Trajectory.	Delegation Process Overview	**SRS-008** Special procedures as defined by delegation contracts regulating the initiation, execution and termination of the delegation shall be in place with the ATSU(s) adjacent to sectors subject delegation.	**SAC#01** "Planning Conflicts" (MF5.1). **SAC#02** "ATC induced conflict" (MF7.1). **SAC#03** "Imminent Infringement" (MF5.9).
Maintain separation between aircrafts. Prevent an unauthorized entry into restricted airspace. Manage Trajectory.	Delegation Request	**SRS-009** The operational Supervisor of the delegating ATSU shall inform operational Supervisor(s) of adjacent ATSU(s) when the delegation procedure is triggered.	**SAC#01** "Planning Conflicts" (MF5.1). **SAC#02** "ATC induced conflict" (MF7.1). **SAC#03** "Imminent Infringement" (MF5.9).

Table 2121212121: Derivation of SRS for Normal Operations driven by EATMA Process models

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

Section 4.3.1 reports the abnormal conditions related to PJ.10-W2-93 concept and covering Technical issues, Staff issues and Other significant but infrequent events.

The ATSU Contingency use case is related to a severe failure taking place at the ATSU premises at a random point in time. In these cases, ATM services provision needs to be delegated to another ATSU or several ATSUs in order to provide ATM services to the airspace users.

During the execution of EXE3 and EXE4 some contingency situations have been tested:

- EXE3: Technical issue impacting the simulator platform and the VCS-b led to a few simulations runs having to be delayed or restarted. During some simulation runs, for a reduced number of flights, there was no automatic correlation between system track and the flight plan. This had no immediate operational effect: the concerned flights were manually correlated at a spare CWP.
- EXE4: Transmission frequency failure at Brindisi ACC. During a simulation run, a VCS failure occurred at Brindisi ACC where the Supervisor, once understood the problem was local and having a coordination with Roma ACC, proceeded with the contingency delegation. Later, after solving the problem and restoring all the operating functionalities, the Brindisi supervisor contacted the Rome supervisor and a recovery delegation was performed.

It has to be highlighted that while the occurrence of contingency situation (e.g. radar outage) prevents the controller to have access to all functionality required to safely manage traffic, the possibility to delegate the traffic to another fully operating unit can be considered as a mitigation protecting against propagation of effects. In fact, even if during the delegation safety will still be degraded, e.g. transferring ATSU has not radar and can't give a proper handover, the delegation will improve the situation. Delegation procedures can be seen as mitigation if the contingency situations strictly related to the ATS provision. If no immediate Contingency Delegation can be provided by aiding units or if the Contingency event does not allow to coordinate with aiding ATSUs, the Supervisor of the failing ATSU instructs the ATCO teams of the failing unit to clear-the-sky.

The potential operational effects of the abnormal conditions and the potential mitigation of these effects are presented in the following table:

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SRS xxx]
ABN 1	**Terrorist attack**	Closure of Airspace. Increase of ATCOs Workload. Increase of pilots workload.	Coordination between civil and military.
		ATCOs Workload increased to	Civil/military coordination.

Co-funded by the European Union

		coordinate response civil/military. Sovereignty issues.	Revert delegation.
		Increase of ATCOs Workload. Increase of potential conflicts.	The agreement between the two ATSUs shall define the procedure in case of hijack/contingency situations.
ABN 2	**Total/Partial loss of an ATSU (not able to delegate/revert to "normal operations"):** • **Full loss of ATM System because of Cyber Attack** • **Electrical problem / flooding's** • **Critical infrastructure failure**	One ATSU is no longer capable of managing the delegated area (partial loss).	The provision of ATS should go back to the other ATSU (partial loss). / The Supervisor shall be responsible to decide if the ATSU has a contingency case / The Supervisor shall be responsible to decide if a contingency delegation is initiated. / All procedures concerning involved parties in contingency delegation mode shall have a well-defined contingency plan including legal operational procedures and definition of responsibility for the service provision.
		Decreased ATSU capacity.	Capacity reduction in affected ATC sectors. / All procedures concerning involved parties in contingency delegation mode shall have a well-defined contingency plan including legal operational procedures and definition of

Co-funded by the European Union

			responsibility for the service provision.
		In case of failure of ATSU, contingency procedures will be planned. If ATSU1 won't be able to cover ATSU2, it will be closed (partial loss).	ATSU1 will take back the delegation. / All procedures concerning involved parties in contingency delegation mode shall have a well-defined contingency plan including legal operational procedures and definition of responsibility for the service provision.
		In case of full loss of ATM System because of Cyber Attack, there should be a lack of services.	Redundant System. / All procedures concerning involved parties in contingency delegation mode shall have a well-defined contingency plan including legal operational procedures and definition of responsibility for the service provision.
		In case of Critical infrastructure failure, there should be a lack of services.	Redundant infrastructure ready to ensure services in a minimum time. / The Supervisor of the aiding ATSU shall decide if contingency delegation can be provided.
ABN 3	**ATC STAFF Capacity**	Lack of resources.	The receiving ATSUs shall have sufficient human resources to handle an additional airspace. / Revert Delegation or Clear-

			the-sky procedure if no immediate contingency delegation can be provided.

Table 2222222222: Risk analysis for Abnormal conditions of operation

EUROPEAN PARTNERSHIP

Co-funded by the European Union

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

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

D.1 Hazard Identification

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
Delegation of ATM services provision at night Delegation of ATM services provision at fixed time Delegation of ATM services provision on-demand	ATCOs fail to detect and resolve potential conflicts before they result in losses of separation Lack of training / Lack of familiarity with the sector results in a lack of capacity to manage the sector and/or an emergency	Tactical Conflict (planned) (MF5.1)	Tactical Conflict Management B5-9	Hs 01: A situation where an imminent infringement coming from a planned conflict was prevented by tactical conflict management MAC-SC4b

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
Delegation of ATM services provision at night Delegation of ATM services provision at fixed time Delegation of ATM services provision on-demand	ATCOs fail to detect and resolve potential conflicts before they result in losses of separation Lack of training / Lack of familiarity with the sector results in a lack of capacity to manage the sector and/or an emergency	Imminent Infringement (MF5.9)	ATC collision prevention B3B4	Hs 02: A situation where an imminent collision was prevented by ATC Collision prevention MAC-SC2b
Delegation of ATM services provision in case of contingency	ADSP Failure Infrastructure failure	Near Mid Air Collision (MF3a)	ATC collision prevention B3B4	OH 01 Loss of Service prevents controller from managing one or many aircraft for receiving ATSU MAC-SC2a
Delegation of ATM services provision in case of contingency	ADSP Failure Infrastructure failure	Near Mid Air Collision (MF3a)	ATC collision prevention B3B4	OH 02 Loss of Service prevents controller from managing one or many aircraft for both delegating and receiving ATSUs MAC-SC2a

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
Delegation of ATM services provision in case of contingency	ADSP Failure Infrastructure failure Maintenance Error Technical Personnel Error / Lack of training	Imminent Infringement (MF5.9)	ATC Collision Prevention B3B4	OH 03 Loss of Service results in "Service Loss (one/two workstation/s) for receiving ATSU", i.e. data and or functions not available or not behaving correctly preventing the controller to have access to all functionality required to safely manage traffic. MAC-SC3
Delegation of ATM services provision in case of contingency	ADSP Failure Infrastructure failure Maintenance Error Technical Personnel Error / Lack of training	Imminent Infringement (MF5.9)	ATC Collision Prevention B3B4	OH 04 Loss of Service results in "Service Loss (one/two workstation/s) for both delegating and receiving ATSUs", i.e. data and or functions not available or not behaving correctly preventing the controller to have access to all functionality required to safely manage traffic. MAC-SC3

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
Delegation of ATM services provision in case of contingency	Data corrupted	Imminent Collision (MF4)	ATC Collision Prevention B3B4	OH 05 Loss of Service results in"Detected corruption for receiving/both delegating and receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic MAC-SC2b
Delegation of ATM services provision in case of contingency	Data corrupted	Near Mid Air Collision (MF3a)	ATC collision prevention B3B4	OH 06 Loss of Service results in "Undetected Corruption for receiving/ both delegating and receiving ATSU" preventing controller from managing safe separation of traffic MAC-SC2a
Delegation of ATM services provision in case of civil military	Telephone switching dormant failure	MIL ATSU will not be able to coordinate with receiving ATSU once the delegation is implemented	As per PJ32 OSED UC04 description, SR#: Prior to initiate a delegation request involving an ARES the delegating ATSU shall inform the military party (Military SPV) about the delegation request in order for the military party to verify the switch to the envisaged telephone contacts for communication with the receiving ATSU.	OH 07 Lack of phone coordination regarding ARES between MIL control and receiving ATCO

Table 2323232323. Full HAZID working table

Appendix E Designing the Solution functional system for normal conditions

E.1 Deriving SRD from the SRS

Table below shows the Safety Requirements at Design level (SRD) (functionality and performance) for normal conditions of operation derived from the Safety Requirements at ATS Service level (SRS) for normal conditions of operation derived in section 004.2.

SRS for Normal Operation (ID & content)	Safety Requirement at Design level[2] (SRD) or Assumption	Maps onto
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-001** The receiving ATCO team(s) shall be able to preview traffic of the sector to be delegated on their CWP.	[Preview Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-002** The receiving ATSU shall activate the preview mode for the sectors to be delegated.	[Preview Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-003** The frequency of the delegated sector should be activated automatically to Rx at the Executive CWP of the receiving ATSU when the receiving ATSU activates the preview mode for this sector.	[Preview Mode]

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

SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload. SRS-005 The receiving ATCO team shall have the complete traffic situational awareness for the delegated sector following the traffic exchange with the delegating ATCO team. SRS-006 One ATCO shall be in control of the delegated sector during all phases of the delegation procedure.	**SRD-004** The delegation of ATS provision shall be supported by the CWP (ATS and Voice).	[Operational Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload. SRS-005 The receiving ATCO team shall have the complete traffic situational awareness for the delegated sector following the traffic exchange with the delegating ATCO team.	**SRD-005** The receiving ATCO team(s) shall contact the delegating ATCO team(s) and exchange the traffic situation of the sector to be delegated when starting the Exchange Traffic Situation phase.	[Operational Mode]

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-006** The receiving ATSU shall request to switch the CWPs at the receiving ATCO team from Preview Mode to Operational mode.	[Preview/Operational Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-007** The ATCOs of the receiving ATSU shall have the appropriate endorsement(s) to operate the sector or sector configurations to be delegated.	[Request Delegation/ Request Allocation of delegated sectors]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-008** The delegation process shall not be performed at the moment the receiving ATSU is considered at full capacity.	[Operational Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload. SRS-002 The decision for delegation abortion by the Supervisor in the Receiving ATSU shall be taken timely. SRS-004 All relevant third parties shall be informed about an aborted delegation. SRS-007 The operational Supervisor of the receiving ATSU shall inform all relevant third	**SRD-009** The operational Supervisor of receiving ATSU shall be supported by the system to abort the ongoing delegation.	[Abort Delegation]

parties about the successful completion of the delegation. SRS-009 The operational Supervisor of the delegating ATSU shall inform operational Supervisor(s) of adjacent ATSU(s) when the delegation procedure is triggered.		
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload. SRS-005 The receiving ATCO team shall have the complete traffic situational awareness for the delegated sector following the traffic exchange with the delegating ATCO team.	**SRD-010** A receiving ATSU shall be appropriately equipped and staffed in order to provide ATS in the pre-defined airspace of the delegating ATSU.	[Operational Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-011** The receiving ATCO team shall coordinate about proceeding to the next phase of the Delegation Procedure at the end of the Delegation Preparation phase.	[Operational Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-012** The delegating ATCO team shall use the WEST checklist for a systematic approach of the traffic handover to the receiving ATCO team.	[Operational Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable	**SRD-013** The delegating ATCO team shall be able to identify the flights that need to be handed over.	[Operational Mode]

level of safety and ATCO workload.		
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-014** The receiving ATCO team shall read-back and acknowledge all flights being pointed out by the delegating ATCO team.	[Operational Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-015** The ATCO team(s) of the receiving ATSU shall coordinate internally to agree on entering the Enter Operational Mode phase after exchanging traffic with the ATCO team of the delegating ATSU.	[Traffic Exchange/Operational Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-016** The delegating and receiving ATCO teams shall coordinate and acknowledge the point when the preview mode is switched to operational mode at the receiving ATSU.	[Preview/Operational Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload. SRS-005 The receiving ATCO team shall have the complete traffic situational awareness for the delegated sector following the traffic exchange with the delegating ATCO team.	**SRD-017** The ATCO of the receiving ATSU shall be able to identify which sector is in operational mode	[Operational Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable	**SRD-018** The receiving Executive should have a radio check of the frequency of	[Preview/Operational Mode]

level of safety and ATCO workload.	the delegated sector before switching to operational mode.	
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-019** The delegating ATCO team shall switch the frequency of the delegated sector from Tx/Rx to Rx when switching from operational mode to preview mode in the delegating ATSU.	[Preview/Operational Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-020** The frequency of the delegated sector should be switched automatically from Tx/Rx to Rx at the Executive CWP of the delegating ATSU when switching from operational mode to preview mode in the delegating ATSU.	[Preview/Operational Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-021** The frequency of the delegated sector should be switched automatically from Rx to Tx/Rx at the Executive CWP of the receiving ATSU when switching from preview mode to operational mode for this sector in the receiving ATSU.	[Preview Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload. SRS-003 The delegating ATSU and the receiving ATSU as well as other concerned parties shall mutually agree upon operational procedures of the delegated airspace. SRS-008	**SRD-022** The delegating ATSU shall terminate the preview mode for the delegated sector after a time defined in the delegation agreement.	[Preview Mode]

Special procedures as defined by delegation contracts regulating the initiation, execution and termination of the delegation shall be in place with the ATSU(s) adjacent to sectors subject delegation.		
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-023** The Executive ATCO of the delegating ATSU shall disable the frequency of the delegated sector when the preview mode is terminated.	[Preview Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-024** The frequency of the delegated sector should automatically be disabled when the preview mode is terminated at the delegating ATSU.	[Preview Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-025** The ATCO of the receiving ATSU shall be able to identify the termination of the preview mode at the delegating ATSU when the preview mode is supported by the system.	[Preview Mode]
SRS-001 The execution of delegation shall be managed by operational procedures that maintain an acceptable level of safety and ATCO workload.	**SRD-026** ATSEP of the ATSU shall be able to control systems running at the ATSU, including network connection to ADSP at all times.	[all phases of the delegation]

Table 2424242424: SRD derived by mapping SRS for normal conditions of operation to Design Model Elements

E.2 Static analysis of the solution functional system behaviour

From the analysis of the NOV-5 / NSV-4 diagrams developed in the framework of the solution, the SRD presented in section 5.3.3 have been derived. No additional SRDs considered after static analysis.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

E.3 Dynamic analysis of the Solution functional system behaviour

From the execution of Validation exercise EXE3, one additional SRD has been derived:

SRD-027: The delegating and receiving ATCOs shall be supported by appropriate automation and HMI functions to fully exchange relevant information and safely handover the responsibility.

Also, from all the exercises it has been strongly highlighted the importance of:

- having a full set of supporting tools. ATSUs involved in the delegation should identify a minimum equipment/ tools list for safe delegation of airspace. The impact of the unavailability of any of the identified items should be included in the letter of agreement between the two ATSUs (e.g., unavailability of certain tools will not allow a delegation).
- training for controllers. They should be also trained to handle high traffic density in case of delegation of ATM services provision in both nominal and emergency situations. In the latter situation, controllers situational awareness might be lost and the level of workload would increase therefore and it might get difficult to maintain the safety level".

EUROPEAN PARTNERSHIP

Co-funded by the European Union

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

F.1 Deriving SRD from SRS

Table below shows the Safety Requirements at Design level (SRD) (functionality and performance) for abnormal conditions of operation derived from the Safety Requirements at ATS Service level (SRS) for abnormal conditions of operation derived in section 004.3.

Ref	SRS for Abnormal Operation	Derived SR 0xx and/or A 0xx	Map on to
1	**SRS 010** All procedures concerning involved parties in contingency delegation mode shall have a well-defined contingency plan including legal operational procedures and definition of responsibility for the service provision.	**SRD 028** In case of contingency delegation, the existing safety level shall not be impacted. **SRD 029** A delegation agreement shall define the constraints and performance boundaries when delegated ATM services are operated in degraded mode.	[Operational Mode]
2	**SRS 011** The operational Supervisor of the failing ATSU shall be responsible to decide if the ATSU has a contingency case		
3	**SRS 012** The operational Supervisor of the failing ATSU shall be responsible to decide if a contingency delegation is initiated.		
4	**SRS 013** The operational Supervisor of the failing ATSU of the		

	failing ATSU shall request contingency delegation at an aiding ATSU.		
5	**SRS 014** The operational Supervisor of the aiding ATSU shall decide if contingency delegation can be provided.		
6	**SRS 015** The receiving ATSU shall have opportunity to monitor the traffic load in the receiving sector(s) in order to prevent overload situations.		

Table 2525252525: SRD derived by mapping SRS for Abnormal conditions of operation onto Design Model elements

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

From the analysis of the NOV-5 / NSV-4 diagrams developed in the framework of the solution, the SRD presented in section 5.4.1 has been derived. The safety-related results obtained from the execution of the Real Time Simulation confirmed the requirement already derived (the SRD reported in E.3 are valid also for abnormal conditions of operation). No additional SRDs considered after static/dynamic analysis.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

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

This appendix provides the several causes for each of the identified hazards in Appendix D.

Note that within this safety assessment only mitigating requirements have been derived without considering Quantitative SRD (integrity/ reliability) that will need to be done by the industry in the validation stages prior to implementation (i.e. V4 onwards).

However, some reliability requirements have been defined within the technological safety assessment performed within solutions PJ.10-W2-93A-93B and 93C. For more information, please refer to TS/IRS Part I [17] and II [10].

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

G.1.1 Causal analysis

Causal Analysis

A top-down identification of internal system failures leading to hazards has been conducted, identifying each of these causes and linking them to the possible hazards they could lead to, which are identified and listed in section 4.4.1. The table below lists the causes identified and relates them to these hazards.

Causes	Hazard Description	Hazard Identification
ATCOs fail to detect and resolve potential conflicts before they result in losses of separation	A situation where an imminent infringement coming from a planned conflict was prevented by tactical conflict management	Hs 01
Lack of training / Lack of familiarity with the sector results in a lack of capacity to manage the sector and/or an emergency	A situation where an imminent collision was prevented by ATC Collision prevention	Hs 02

Causes	Hazard Description	Hazard Identification
ADSP Failure Infrastructure failure	Loss of Service prevents controller from managing one or many aircraft for receivingATSU	OH 01
ADSP Failure Infrastructure failure	Loss of Service prevents controller from managing one or many aircraft for both delegating and receiving ATSUs	OH 02
ADSP Failure Infrastructure failure Maintenance Error Technical Personnel Error / Lack of training	Loss of Service results in "Service Loss (one/two workstation/s) for receiving ATSU", i.e. data and or functions not available or not behaving correctly preventing the controller to have access to all functionality required to safely manage traffic.	OH 03
ADSP Failure Infrastructure failure Maintenance Error Technical Personnel Error	Loss of Service results in "Service Loss (one/two workstation/s) for both delegating and receiving ATSUs", i.e. data and or functions not available or not behaving correctly preventing the controller to have access to all functionality required to safely manage traffic.	OH 04
Data corrupted	Loss of Service results in"Detected corruption for for receiving/ both delegating and receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic	OH 05
Data corrupted	Loss of Service results in "Undetected Corruption for for receiving/ both delegating and receiving ATSU" preventing controller from managing safe separation of traffic	OH 06

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Causes	Hazard Description	Hazard Identification
Telephone switching dormant failure	Lack of phone coordination regarding ARES between MIL control and receiving ATCO	OH 07

Table 2626262626. List of causes, generating hazards

Common Cause Analysis

Hazard Identification	Causes	Consequences (Common cause analysis)	
OH 01	ADSP Failure Infrastructure failure	Near Mid Air Collision (MF3a)	Increase of controllers' workload; Decrease of controllers' situational awareness
OH 02	ADSP Failure Infrastructure failure		
OH 06	Data corrupted		
OH 03	ADSP Failure Infrastructure failure Maintenance Error Technical Personnel Error / Lack of training	Imminent Infringement (MF5.9)	
Hs 02	ATCOs fail to detect and resolve potential conflicts before they result in losses of separation Lack of training / Lack of familiarity with the sector results in a lack of capacity to manage the		

Hazard Identification	Causes	Consequences (Common cause analysis)	
	sector and/or an emergency		
OH 04	ADSP Failure Infrastructure failure Maintenance Error Technical Personnel Error		
OH 05	Data corrupted	Imminent Collision (MF4)	
Hs 01	ATCOs fail to detect and resolve potential conflicts before they result in losses of separation Lack of training / Lack of familiarity with the sector results in a lack of capacity to manage the sector and/or an emergency	Tactical Conflict (planned) (MF5.1)	
OH 07	Telephone switching dormant failure	MIL ATSU will not be able to coordinate with receiving ATSU once the delegation is implemented	

Table 2727272727. List of consequences in Common Cause Analysis

Formalization of Mitigations

Hazard Identification	Hazard Description	Causes	Consequences (Common cause analysis)		Mitigations
OH 01	Loss of Service prevents controller from managing one or many aircraft for receivingATSU	ADSP Failure Infrastructure failure	Near Mid Air Collision (MF3a)	Increase of controllers' workload; Decrease of controllers' situational awareness	Operating methods (procedures) covers all operations (normal and abnormal conditions); Training for ATCOs covers all operations (normal and abnormal conditions); Training for ATSEP Recurrent Training for all the technical and operational staff Systems redundancy License for ATSEPs of the ADSP for the technical systems they are operating Coordination and synchronization messages exchange between ATSUs Delegation abortion
OH 02	Loss of Service prevents controller from managing one or many aircraft for both delegating and receivingATSUs	ADSP Failure Infrastructure failure			
OH 06	Loss of Service results in "Undetected Corruption for receiving/ both delegating and receivingATSU" preventing controller from managing safe separation of traffic	Data corrupted			
OH 03	Loss of Service results in "Service Loss (one/two workstation/s) for receivingATSU", i.e. data and or functions not available or not behaving correctly preventing the controller to have access to all functionality required to	ADSP Failure Infrastructure failure Maintenance Error Technical Personnel Error / Lack of training	Imminent Infringement (MF5.9)		

Hazard Identification	Hazard Description	Causes	Consequences (Common cause analysis)		Mitigations
	safely manage traffic.				
OH 04	Loss of Service results in "Service Loss (one/two workstation/s) for both delegating and receivingATSUs", i.e. data and or functions not available or not behaving correctly preventing the controller to have access to all functionality required to safely manage traffic.	ADSP Failure Infrastructure failure Maintenance Error Technical Personnel Error / Lack of training			
Hs 02	A situation where an imminent collision was prevented by ATC Collision prevention	ATCOs fail to detect and resolve potential conflicts before they result in losses of separation Lack of training / Lack of familiarity with the sector results in a lack of capacity to manage the sector and/or			

Hazard Identification	Hazard Description	Causes	Consequences (Common cause analysis)		Mitigations
		an emergency			
OH 05	Loss of Service results in"Detected corruption for receiving/ both delegating and receivingATSU" preventing the controller to have access to all functionality required to safely manage traffic	Data corrupted	Imminent Collision (MF4)		
Hs 01	A situation where an imminent infringement coming from a planned conflict was prevented by tactical conflict management	ATCOs fail to detect and resolve potential conflicts before they result in losses of separation Lack of training / Lack of familiarity with the sector results in a lack of capacity to manage the sector and/or an emergency	Tactical Conflict (planned) (MF5.1)		

Co-funded by the European Union

Hazard Identification	Hazard Description	Causes	Consequences (Common cause analysis)		Mitigations
OH 07	Lack of phone coordination regarding ARES between MIL control and receiving ATCO	Telephone switching dormant failure	MIL ATSU will not be able to coordinate with receiving ATSU once the delegation is implemented		As per PJ32 OSED UC04 description, SR#: Prior to initiate a delegation request involving an ARES the delegating ATSU shall inform the military party (Military SPV) about the delegation request in order for the military party to verify the switch to the envisaged telephone contacts for communication with the receiving ATSU.

Table 2828282828. List of mitigations to reduce likelihood of hazards

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

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

SRS (functionality&performance) for protective mitigation (ID & content)	Safety Requirement at Design level[3] (SRD) or Assumption	Maps onto
SRS-016 The delegation procedures shall be fully safety assessed and approved by the safety authorities of the parties involved in delegation **SRS-017** The receiving ATSU shall implement processes and procedures to manage	**SRD-030** Recurrent Training shall be provided to ATCOs in order to guarantee an optimal maintenance of competence for airspaces associated with a delegation agreement. **SRD-031** The ATSEPs of the delegating and receiving ATSU and the ATSEPs of the ADSP shall be regularly trained to operate their technical systems.	Operational Mode

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

failures of delegated ATM services after their successful delegation. **SRS-018** The frequency of occurrence of Loss of Service preventing controller from managing one or many aircraft for receiving ATSU shall not be more than 1,2 1e-6 [sector operating hours]. **SRS-019** The frequency of occurrence of Loss of Service preventing controller from managing one or many aircraft for both delegating and receiving ATSU shall not be more than 1,2 1e-6 [sector operating hours]. **SRS-020** The frequency of occurrence of Service Loss (one/two workstation/s) for receiving ATSU" shall be no greater than 2,4 1e-6 [sector operating hours] **SRS-021**	**SRD-032** The ATSEPs of the delegating and receiving ATSU and the ATSEPs of the ADSP shall be licensed for the technical systems they are operating. **SRD-033** In case of contingency, coordination and synchronization messages shall be exchanged between ATSUs.	

The frequency of occurrence of Service Loss (one/two workstation/s) for both delegating and receiving ATSU" shall be no greater than 2,4 1e-6 [sector operating hours] **SRS-022** The frequency of occurrence of Loss of Service resulting in "Detected corruption for receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic shall be no greater than 6,0 1e-7 [sector operating hours] **SRS-023** The frequency of occurrence of Loss of Service resulting in "Detected corruption for both delegating and receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic shall be no greater than 6,0 1e-7 [sector operating hours] **SRS-024** The frequency of occurrence of Loss of Service resulting in	**SRD-034** A delegation agreement shall clearly define how failures of delegated ATM services need to be handled after their successful delegation. **SRD-035** The operational Supervisor and/or the ATSEP shall be able to make the system input to abort a delegation.	

"Undetected corruption for receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic shall be no greater than 1,2 1e-7 [sector operating hours] **SRS-025** The frequency of occurrence of Loss of Service resulting in "Undetected corruption for both delegating and receiving ATSU" preventing the controller to have access to all functionality required to safely manage traffic shall be no greater than 1,2 1e-7 [sector operating hours]	**SRD-036** An ATSU shall have the capability to manage unexpected events and problems that occur during and after a delegation	

Table 2929292929: SRD derived by mapping SRS (functionality&performance) for protective mitigation on to Design Model Elements

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix H Demonstration of Safety Criteria achievability

The safety-related outcomes of the V3 validation exercises (traced back to the safety validation objectives) bring an essential contribution to the demonstration of the Safety Criteria achievability by the Solution design.The exercises safety validation objectives and the related success criteria are summarized in Table below. For more results, please refer to the VALR[19][19][~~18~~].

Exercise ID, Name, Goals	Exercise Safety Validation Objective & related SAC(s)	Success criterion	Coverage (SRS and/or SRD)	Validation results & Level of safety evidence
EXE-PJ.10-W2-93-V3-VALP-002 Delegation of ATM services provision among ATSUs – ENAIRE. The objective is to validate the operational thread of the delegation of ATM services provision among ATSUs in nominal conditions. In particular, this validation activity aims at demonstrating the operational feasibility, operational	**EX2-OBJ-PJ.10-W2-93-V3-VALP-009** To assess the impact in terms of Safety of the ATM services provision delegation concept in nominal conditions	**EX2-CRT-PJ.10-W2-93-V3-VALP-049** The level of safety remains at an acceptable level according to ATCo's expert judgment before, during and after the delegation of ATM services provision in nominal conditions.		Overall, there is an agreement for the night use case and fix time use case with regards to the level of safety being maintained during and after the delegation procedure. For the on-demand (cross-border and ATFM) there are disagreements with regards to the level of safety being maintained during and after the delegation procedure.

acceptance, and performance benefits of the PJ.10-W2-93 concept for the following use cases: • Delegation of ATM services provision at night • Delegation of ATM services provision at fixed time • Delegation of ATM services provision on-demand		**EX2-CRT-PJ.10-W2-93-V3-VALP-050** Impact remains acceptable according to ATCo expert judgment in terms of the management and provision of aircraft separation before, during and after the delegation of ATM services provision in nominal conditions are identified.	**SRS-001** **SRS-003** **SRS-005** **SRS-006** **SRS-007 Partially Covered** **SRS-008 Partially Covered** **SRS-009 Partially Covered** **SRS-015** **SRS-016 Partially Covered** **SRD-001** **SRD-002** **SRD-003 Partially Covered** **SRD-004** **SRD-005** **SRD-006** **SRD-007** **SRD-008** **SRD-009 Partially Covered** **SRD-010** **SRD-011** **SRD-012 Partially Covered** **SRD-013** **SRD-014** **SRD-015** **SRD-016** **SRD-017** **SRD-018 Partially Covered** **SRD-019** **SRD-020 Partially Covered** **SRD-021 Partially Covered** **SRD-022** **SRD-023** **SRD-024 Partially Covered** **SRD-030** **SRD-034 Partially Covered** **SRD-036 Partially Covered**	Overall, there is an agreement for the night use case and fix time use case with regards to the management and provision of aircraft separation, being this acceptable. For the on-demand (cross-border and ATFM) there are disagreements on this matter.

EXE-PJ.10-W2-93-V3-VALP-003 Delegation of ATM services provision among ATSUs – skyguide • Validate the concept of delegation of ATM services provision among ATSUs in nominal and	**EX3-OBJ-PJ.10-W2-93-V3-VALP-008** To assess the impact in terms of Safety of the ATM services provision delegation concept in nominal conditions	**EX3-CRT-PJ.10-W2-93-V3-VALP-043** The level of safety remains at an acceptable level according to ATCo's expert judgment before, during and after the delegation of ATM services provision in nominal conditions.		

EUROPEAN PARTNERSHIP

Co-funded by the European Union

abnormal conditions, contributing to the maturity V3 of the Solution PJ.10-W2-93. • Validate the three architectural options (Y, U and D) of Virtual Centre based platforms, as well as the increase of Maturity of the Virtual Centres and related services, while involving multiple ATSUs connected to one or several ADSPs. This part is being supported by another project SESAR W3 PJ32-VC W3. EXE-PJ.10-W2-93-V3-VALP-003 exercise selected two delegation scenarios from the PJ.10-W2-93 V3 SPR-INTEROP_OSED, which were played in a VC platform of		**EX3-CRT-PJ.10-W2-93-V3-VALP-044** Impact remains acceptable according to ATCo expert judgment in terms of the management and provision of aircraft separation before, during and after the delegation of ATM services provision in nominal conditions are identified.	**SRS-001** **SRS-002** **SRS-003 partially covered** **SRS-004 partially covered** **SRS-005** **SRS-006** **SRS-007 partially covered** **SRS-008 partially covered** **SRS-009** **SRS-011** **SRS-012** **SRS-013** **SRS-014** **SRS-015** **SRD-001** **SRD-002** **SRD-003** **SRD-004** **SRD-005** **SRD-008** **SRD-009** **SRD-010** **SRD-011** **SRD-012 partially covered** **SRD-013** **SRD-014** **SRD-015** **SRD-016** **SRD-017** **SRD-018** **SRD-019** **SRD-020** **SRD-021** **SRD-022** **SRD-023** **SRD-024** **SRD-025 partially covered** **SRD-026** **SRD-028** **SRD-033 partially covered** **SRD-035**	• During the simulation runs, situational awareness and prescribed separation could be maintained. • The execution of the delegation procedure was found to support a safe delegation process. • According to ATCOs feedback, they were generally able to manage traffic in a safe way, although some potential safety related issues were detected mainly due to the lack of several supporting & conflict detection tools that are commonplace for ATS provision, and the level of sector knowledge for the receiving ATCOs. • Use cases with Dynamic AoR (delegated sector collapsed with receiving sector) could lead to potential selective attention from the receiving ATCOs due to gained processing fluency: receiving ATCOs inadvertently

different architectures Y/U/D: • Delegation of ATM services provision at night. • Delegation of ATM services provision in contingency (case of ATSU failure).				directing more of their attention to their usual sector rather than the entire AoR/ collapsed sectors. • While the delegation procedure was found to support a safe delegation process, the interoperability limitations, particularly associated with the U architecture, were found to lack the required maturity: clearances entered by the delegating ATSU were not visible on the receiving ATSU's CWP. The receiving ATCO team had to remember all these clearances (verbally coordinated during the exchange of traffic situation), and re-enter them for each flight after they were in operational mode. • In general, the exchange of traffic situation phase needs to be complemented by adequate supporting tools in order to minimize, to the

Co-funded by the European Union

				furthest extent practicable, the probability of information (or flights) being omitted/ misheard/ misinterpreted.
	EX3-OBJ-PJ.10-W2-93-V3-VALP-009 Safety assessment in abnormal conditions To assess the impact in terms of Safety of the ATM services provision delegation concept in abnormal conditions	**EX3-CRT-PJ.10-W2-93-V3-VALP-045** The level of safety remains at an acceptable level according to ATCo's expert judgment before, during and after the delegation of ATM services provision in abnormal conditions.		

		EX3-CRT-PJ.10-W2-93-V3-VALP-046 Impact remains acceptable according to ATCo's expert judgment in terms of the management and provision of aircraft separation before, during and after the delegation of ATM services provision in abnormal conditions are identified.		• During the simulation runs, situational awareness and prescribed separation could be maintained. • The execution of the delegation procedure was found to support a safe delegation process. • According to ATCOs feedback, they were generally able to manage traffic in a safe way, although some potential safety related issues were detected mainly due to the lack of several supporting & conflict detection tools that are commonplace for ATS provision, and the level of sector knowledge for the receiving ATCOs. • Use cases with Dynamic AoR (delegated sector collapsed with receiving sector) could lead to potential selective attention from the receiving ATCOs due to gained processing fluency: receiving ATCOs inadvertently

				directing more of their attention to their usual sector rather than the entire AoR/ collapsed sectors. • While the delegation procedure was found to support a safe delegation process, the interoperability limitations, particularly associated with the U architecture, were found to lack the required maturity: clearances entered by the delegating ATSU were not visible on the receiving ATSU's CWP. The receiving ATCO team had to remember all these clearances (verbally coordinated during the exchange of traffic situation), and re-enter them for each flight after they were in operational mode. • In general, the exchange of traffic situation phase needs to be complemented by adequate supporting tools in order to minimize, to the

				furthest extent practicable, the probability of information (or flights) being omitted/ misheard/ misinterpreted.
EXE-PJ.10-W2-93-V3-VALP-004 Delegation of ATM services provision among ATSUs – ENAV The objective is to validate the delegation of ATM services provision among ATSUs in nominal conditions and no normal conditions in a Virtual Centre platform. In particular, this validation activity aimed at demonstrating the operational feasibility, operational acceptance, and performance benefits of the PJ.10-W2-93 concept for the following use cases:	**EX4-OBJ-PJ.10-W2-93-V3-VALP-014** To assess the impact in terms of Safety of the ATM services provision delegation concept in nominal conditions	**EX4-CRT-PJ.10-W2-93-V3-VALP-067** The level of safety remains at an acceptable level according to ATCo's expert judgment before, during and after the delegation of ATM services provision in nominal conditions.		In general, the level of safety was maintained acceptable throughout the runs. The procedure itself was considered quite safe. Overall, although the global level of safety was felt quite good, the controllers expressed some safety concerns. However, these concerns were more linked to specific situations in which controllers experienced difficulties with the use of system rather than attributable to a specific working technique or whether the traffic was delegated or not

• Delegation of ATM services provision at night • Delegation of ATM services provision at fixed time • Delegation of ATM services provision on-demand • Delegation of ATM services provision between Civil and Military ATSUs		**EX4-CRT-PJ.10-W2-93-V3-VALP-068** Impact remains acceptable according to ATCo expert judgment in terms of the management and provision of aircraft separation before, during and after the delegation of ATM services provision in nominal conditions are identified.	**SRS-001** **SRS-005** **SRS-006** **SRS-008** **SRS-009** **SRS-010** **SRS-011** **SRS-012** **SRS-013** **SRS-014** **SRS-015 Partially covered** **SRS-016** **SRS-017 Partially covered** **SRD-001** **SRD-002** **SRD-004** **SRD-005** **SRD-006** **SRD-007** **SRD-008** **SRD-010** **SRD-011** **SRD-013** **SRD-014** **SRD-015** **SRD-016** **SRD-017** **SRD-018** **SRD-019** **SRD-022** **SRD-023** **SRD-026** **SRD-028** **SRD-029** **SRD-030** **SRD-032** **SRD-033** **SRD-034** **SRD-036 Partially covered**	According to ATCOs feedback, they were able to manage traffic in a quite safe way during all the phases of the delegation process ensuring a safe aircraft separation.
	EX4-OBJ-PJ.10-W2-93-V3-VALP-015 To assess the impact in terms of Safety of the ATM services provision delegation concept in abnormal conditions	**EX4-CRT-PJ.10-W2-93-V3-VALP-069** The level of safety remains at an acceptable level according to ATCo's expert judgment before, during and after the delegation of ATM services provision in abnormal conditions.		Overall, the level of safety was maintained at acceptable levels throughout the contingency run. In fact, while the occurrence of contingency situation (e.g. VCS failure) prevented the controller to have access to all functionalities required to safely manage traffic, the possibility to delegate the traffic to another fully operating unit can be considered as a mitigations protecting against propagation of effects.

		EX4-CRT-PJ.10-W2-93-V3-VALP-070 Impact remains acceptable according to ATCo's expert judgment in terms of the management and provision of aircraft separation before, during and after the delegation of ATM services provision in abnormal conditions are identified.		During contingency runs, ATCOs were able to safely manage traffic. No major issues to be reported on the occurrence of some potential tactical conflicts. ATCOs stated that they would have feel more confident in case of conflict management tools availability. Controllers were able to manage traffic in a safe way during all the phases of the delegation process also in case of contingency events.
EXE-PJ.10-W2-93-V3-VALP-005 Delegation of ATM services provision among ATSUs – COOPANS The objective is to validate the delegation of ATM services provision among ATSUs considering the following Use Cases: • Delegation of ATM services provision in	**EXE5-OBJ-PJ.10-W2-93-V3-VALP-014** To assess the impact in terms of Safety of the ATM services provision delegation concept in nominal conditions	**EXE5-CRT-PJ.10-W2-93-V3-VALP-014-001** The level of safety remains at an acceptable level according to ATCo's expert judgment before, during and after the delegation of ATM services provision in nominal conditions.		According to expert opinion, safety was not impaired even though ATCOs stated they missed some tools and warnings from their "normal" operational system. There was a varying delay in system inputs/outputs due to limited communication bandwidth with the ADSP which contributed to higher workload, but was not

case of contingency • Delegation of ATM services provision on-demand			**SRS-001** **SRS-003** **SRS-005** **SRS-006** **SRS-007 Partially covered** **SRS-009** **SRS-015 Partially covered** **SRD-001** **SRD-002** **SRD-005** **SRD-006 Partially covered** **SRD-007** **SRD-008** **SRD-009** **SRD-010** **SRD-011** **SRD-012 Partially covered** **SRD-013** **SRD-014** **SRD-015 Partially covered** **SRD-016 Partially covered** **SRD-023 Partially covered** **SRD-030** **SRD-035**	considered to affect safety.
		EXE5-CRT-PJ.10-W2-93-V3-VALP-014-002 Impact remains acceptable according to ATCo expert judgment in terms of the management and provision of aircraft separation before, during and after the delegation of ATM services provision in nominal conditions.		ATCOs were able to ensure the management and provision of aircraft separation thanks to a good situational awareness and efficient coordination between planner and executive ATCOs.
EXE-PJ.10-W2-93-V3-VALP-006 Delegation of ATM services provision among ATSUs – PANSA The objective is to validate the delegation of ATM services provision among ATSUs considering the following Use Cases:	**EXE6-OBJ-PJ.10-W2-93-V3-VALP-014 To assess the impact in terms of Safety of the ATM services provision delegation concept in nominal conditions.**	**EXE6-CRT-PJ.10-W2-93-V3-VALP-014-001** The level of safety remains at an acceptable level before, during and after the delegation of ATM services provision in nominal conditions.	**SRS-001 Partially covered** **SRS-008 Partially covered** **SRD-007 Partially covered** **SRD-030 Partially covered**	Controllers agreed that the level of safety remained acceptable with the introduction of the new operating method particularly in terms of coordination between executive and planner ATCOs.

• Delegation of provision of ATS services – Cross Border; • Night delegation of provision of ATS services.		**EXE6-CRT-PJ.10-W2-93-V3-VALP-014-002** No negative impacts in terms of the management and provision of aircraft separation before, during and after the delegation of ATM services provision in nominal conditions are identified.		ATCOs were able to ensure the management and provision of aircraft separation thanks to a good situational awareness and efficient coordination between planner and executive ATCOs. ATCO should be trained to handle high traffic density in case of delegation of ATM services provision for emergency reason.

Table 3030303030: Solution Safety Validation results

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix I Assumptions, Safety Issues & Limitations

I.1 Assumptions log

Ref	Assumption	Validation
A001	The current ATCO licensing framework has been considered. Training is needed to avoid the lack of ATCO sector-based knowledge.	Basic ATCO training
A002	The safety assessment takes into account the virtual centre architectures considered during the validation activities	To be complemented with Technical requirements developed within the TS-IRS. To be complemented with PJ32 study

Table 3131313131: Assumptions log

I.2 Safety Issues log

The following safety issues were raised during the safety assessment:

Ref	Safety issue	Resolution
I001	The frequency of occurrence of conflict might increase if ATCOs has no access to all the conflicting tool	Availability of this tool is fundamental

Table 3232323232: Safety Issues log

I.3 Operational Limitations log

Ref	Operational Limitations
L001	During the exercises, most of the scenarios were tested on Sectors of the Upper airspace above FL-330, with many stable flights and very few conflictual situations. The reality would be a more complex traffic situation with several potential conflicts.

Table 3333333333: Operational Limitations log

EUROPEAN PARTNERSHIP

Co-funded by the European Union

-END OF DOCUMENT-

EUROPEAN PARTNERSHIP

Co-funded by the European Union