[SESAR Solution PJ.10-W2-93A-93B-93C TS/IRS - Part II - Safety Assessment Report]

Deliverable ID:	**D3.2.060**
Dissemination Level:	**PU**
Project Acronym:	**PJ.10-W2-PROSA**
Grant:	**874464**
Call:	**H2020-SESAR-2019-1**
Topic:	**Separation Management and Controller Tools**
Consortium Coordinator:	**DFS**
Edition Date:	**18 May 2023**
Edition:	**00.01.01**
Template Edition:	**00.00.01**

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Authoring & Approval

Authors of the document

Beneficiary	Date
ENAV	12 Dec 22

Reviewers internal to the project

Beneficiary	Date
DSNA	26 Jan 23
DFS	26 Jan 23
INDRA	26 Jan 23
NATS	26 Jan 23

Reviewers external to the project

Beneficiary	Date

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

Beneficiary	Date
COOPANS	
DSNA	
DFS	
ENAV	
EUROCONTROL	
FREQUENTIS	
INDRA	
LEONARDO	
NATS	
PANSA	
SKYGUIDE	
THALES	

Rejected By - Representatives of beneficiaries involved in the project

Beneficiary	Date

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Document History

Edition	Date	Status	Beneficiary	Justification
00.00.01	12 Dec 22	Draft	ENAV	Initial version
00.00.02	20 Jan 23	Draft	ENAV	Hazard Analysis complemented
00.01.00	30 Jan 23	Final	ENAV	Final for approval
00.01.01	18 May 23	Final	ENAV	Alignment with TS-IRS after the Maturity Gate

PJ.10-W2-PROSA

PJ.10-W2-93 DELEGATION OF ATM SERVICES PROVISION AMONG ATSUS

This document is part of a project that has received funding from the SESAR3 Joint Undertaking under grant agreement No 874464 under European Union's Horizon 2020 research and innovation programme.

Abstract

The PJ.10-W2-93 deals with the different possible cases of delegation of provision of ATM Services amongst ATSUs based on traffic / organisation needs (either static on fix-time transfer schedule (Day/Night) or dynamic, e.g. when the traffic density is below/over certain level) or on contingency needs. The delegation operational concept can be supported by three different architectures, aka "Y", "D" and "U". Each of them has been developed in a specific technological solution and referenced as SESAR PJ.10-W2 Technological Solutions 93A, 93B and 93C.

This document is Part II of the TS/IRS related to the SESAR Project ***PJ.10-W2 Solutions 93A, 93B and 93C.*** Part II provides the Technological Safety Assessment Report (SAR) describing all the safety assurance activities that are requested to be performed in order to prove that the system investigated in the Solution is acceptably safe. To this end, this SAR also contains the Technical System Safety Specification identified for the Solution, complementing (at technological level) the work performed within the PJ.10-W2-93 V3 OSED 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

List of Figures

1 Executive Summary

This document contains the Specimen Safety Assessment for a typical application of the PJ.10-W2-Sol.93A-93B-93C Technological Solution. Those solutions propose three different architectures, of which two are based on Virtual Centre services developed in SESAR 2020 Wave 1 PJ.16-03, and Operational Concepts developed in SESAR 2020 Wave 1 PJ.15-09.

While Solution 93B and 93C are only reaching TRL4 at the end of Wave2, Solution 93A reaches TRL6 and allows OI SDM-217 of PJ.10-W2-Solution 93 to reach V3.

The three different architectures correspond to those identified and proposed by EUROCAE WG122: Architectures “Y”, “D” and “U”.

The Safety Assessment Report (SAR) represents Part II of the TS/IRS document and presents the assurance that the Safety Requirements for the TRL4-6 phases are complete, correct and realistic, thereby providing all material to adequately inform the PJ.10-W2-Sol.93A-93B-93C Solution TS/IRS Part I.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

2 Introduction

2.1 Background

This safety assessment takes into account the work performed in other previous SESAR projects activities:

- PJ.15-09 from SESAR 2020 Wave 1 in which the first use cases of delegation and contingency of ATM services were produced;
- PJ.16-03 from SESAR 2020 Wave 1, which requirements and services specifications serve as a basis for the development of the VC concept, as well as for the development of virtual centre services, to ensure the adequate support to the implementation of the different ATS delegation use cases;
- PJ.10-W2-93 V2 phase outcomes.

Finally this assessment complements, at technological level, the work performed within the PJ.10-W2-93 V3 OSED Part II Safety Assessment Report.

2.2 General Approach to Safety Assessment

According to SESAR Safety Reference Material [2] [3], safety approach identifies three kind of solution types depending on its safety impact of the solution on ATS System. Each solution type: ATS Operational, Other than ATS operational solution or Technological solution demand specific safety approach. Considering the safety impact of PJ.10-W2-93A-93B-93C, it is a technological solution.

In case of a technological solution, the change involves new technology/equipment (not covered by the safety assessment of the operational solutions) with potential for supporting ATS services or services other than ATS, as they exist or as they are expected to evolve in the future.

This safety assessment is conducted as per the SESAR Safety Reference Material (SRM) which allows the derivation of:

- Technical Specification Safety Requirements (TSSR) specifying the functionality of the technological system for the intended uses (the WHAT) – in terms of equipment, performance and integrity/reliability;
- Technical Safety Requirement at Design level (TSRD) defining the design of the technological system (the HOW) in order to meet the TSSRs.

2.3 Scope of the Safety Assessment

Solution 93B and 93C are only reaching TRL4 at the end of Wave2, Solution 93A reaches TRL6 and allows OI SDM-217 of PJ.10-W2-Solution 93 to reach V3.

As per SESAR SRM [2][3]:

- at TRL4 (safe initial design), the safety assessment will derive the initial Technical Safety Requirements at initial design level (iTSRD);
- at TRL6 (safe refined design) the safety assessment will derive the refined Technical Safety Requirements at initial design level (TSRDs).

The supported PJ.10-W2-Solution 93 operational use cases are:

- Delegation of ATM services provision at night,
- Delegation of ATM Services Provision at fixed time,
- Cross-border delegation of ATM services with dynamic AoR for an elementary sector,
- Cross-border optimisation using delegation with static AoR,
- Delegation of ATM services provision following abnormal conditions (ATSU contingency)

The SAR covers the technical aspects of these exercises:

1. EXE-3 led by SkyGuide aimed 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

    Three architectural options (Y, U and D) of Virtual Centre based platforms were validated.
2. 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
    - Delegation of ATM services provision between Civil and Military ATSUs

    This Exercise was validated in a different Scenario and sectorization, using the “Y” Architecture in a Virtual Centre environment.
3. 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

This Exercise was validated using the “Y” Architecture in a Virtual Centre environment.

2.4 Layout of the Document

- Section 1 provides the executive summary of this safety assessment report.
- Section 2 provides an overview of the safety assessment report.
- Section 3 provides an overview of the PJ.10-W2-Sol93A-93B-93C
- Section 4 presents the Technical Safety Specification
- Section 5 presents the Safe Design of the technical system.
- Section 6 presents the Demonstration of achievability of the Technical System Safety Specification
- Section 7 provides the list of acronyms and terminology.
- Section 8 lists the documents referred to in this document.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

3 Setting the Scene of the Safety Assessment

3.1 Concept overview and scope of the change

The delegation of ATM services provision, as described by the OI "SDM-0217_Delegation of ATM Services provision between ATSUs", may be achieved with different system architectures.

PJ.10-W2-93A focuses on the "Y" architecture relying on a delegation between 2 ATSUs sharing the same ADSP and without affecting their respective AoRs.

PJ.10-W2-93B focuses on the "D" architecture relying on a delegation between 2 ATSUs, each one with its own ADSP, and using Virtual Centre (service) interoperability for remotely connecting CWPs from the receiving ATSU to the ADSP of the delegating ATSU without affecting the respective ATSU AoRs.

PJ.10-W2-93C focuses on the "U" architecture relying on a delegation between 2 ATSUs, each one with its own system, and using exchange capabilities between the 2 systems for transferring relevant data to the ATSU receiving the delegation. Each system may be a legacy one or be provided by an ADSP. In this architecture, the respective AoRs are reshaped according to the expected delegation.

For more details refer to TS/IRS Part I [17].

3.2 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 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].

3.3 Intended Operational use of the Technological Concept

3.3.1 Intended use identified from SESAR Operational Solutions

PJ.10-W2-93 represents an operational Solution which addresses OI step SDM-0217. This OI step is supported by different sets of Enablers which are associated with different technical architectures (Y, D and U) which are based on the taxonomy defined by EUROCAE WG-122 [19]. The three technical Solutions have been defined to explore these different architectures:

- PJ.10-W2-93A: Y-architecture supporting delegation of ATM services provision amongst ATSUs
- PJ.10-W2-93B: D-architecture supporting delegation of ATM services provision amongst ATSUs
- PJ.10-W2-93C: U-architecture supporting delegation of ATM services provision amongst ATSUs

3.3.2 Other intended use outside SESAR

No additional applications were identified.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

3.4 Relevant applicable standards

Each of these Technological Solutions is corresponding to a particular Virtual Centre architecture as proposed in the taxonomy issued by the EUROCAE WG122 [19].

4 Technical Safety Specification

The purpose of this section is to document the Technical Specification Safety Requirements for the corresponding Technological Solution.

4.1 Overview of activities performed

The Technical Safety Specification is composed of Technical Specification Safety Requirements (TSSRs) and that they are derived from the intended use identified in section 3.3.

This section addresses the following activities:

- the derivation of the Technical Specification Safety Requirements - TSSRs (functionality and performance) in normal and abnormal conditions – section 4.2
- the derivation of the Technical Specification Safety Requirements - TSSRs (integrity/reliability) to address functionality failures – section 4.3
- process assurance of the Technical Safety Specification – section 4.4

4.2 Technical Specification Safety Requirements – TSSR (functionality and performance)

4.2.1 TSSR from SESAR operational solution intended use and/or relevant standards

The following TSSRs has been retrieved from V3 PJ.10-W2-93 OSED Part II [9] based on the use cases for normal operations:

TSSR ID	TSSR
TSSR-001	The delegation of ATS provision shall be supported by the CWP (ATS and Voice).
TSSR-002	The operational Supervisor of receiving ATSU shall be supported by the system to abort the ongoing delegation.
TSSR-003	A receiving ATSU shall be appropriately equipped and staffed in order to provide ATS in the pre-defined airspace of the delegating ATSU.
TSSR-004	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.
TSSR-005	ATSEP of the ATSU shall be able to control systems running at the ATSU, including network connection to ADSP at all times.

Table 1. TSSR normal operations The following TSSRs has been retrieved from V3 PJ.10-W2-93 OSED Part II [9] based on the use cases for abnormal operations:

TSSR ID	TSSR
TSSR-006	In case of contingency, coordination and synchronization messages shall be exchanged between ATSUs.
TSSR-007	In case of contingency, coordination and synchronization messages shall be exchanged between ATC and/or Voice ADSPs.

Table 2. TSSR abnormal operations

TSSR from other intended use

No TSSR from other intended use identified.

4.3 Technical Specification Safety Requirements - TSSR (integrity /reliability)

4.3.1 TSSR from SESAR operational solution intended use and/or relevant standards

The list of Operational Hazards is based on Wave 1 PJ.16-03 SAR Appendix D – Hazards Consequences [7]. 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 managing one or many aircraft for receiving ATSU	Near Mid Air Collision (MF3a)	ATC collision prevention B3B4	MAC-SC2a
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	Imminent Infringement (MF5.9)	ATC Collision Prevention B3B4	MAC-SC3

	behaving correctly preventing the controller to have access to all functionality required to safely manage traffic.			
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	Near Mid Air Collision (MF3a)	ATC collision prevention B3B4	MAC-SC2a

	controller from managing safe separation of traffic			

Table 3. Operational Hazards

Virtual Centre services shall be designed to reduce the impact of loss of service for the following failure modes:

1 or only a few aircraft: Represents a failure mode that impacts on a small number, no more than 3, aircraft for receiving or both receiving and delegating ATSUs.

Many or all aircraft: Represents a failure mode that impacts on more than 3 or all aircraft for receiving or both receiving and delegating ATSUs.

Service Loss (one workstation): Represents a failure mode within the Service that results in data and or functions not being provided or available to the end user OR the data, functions are obviously operating incorrectly for receiving or both receiving and delegating ATSUs.

Service Loss (two workstations): Represents a failure mode within the Service that results in data and or functions not being provided or available to the end user OR the data, functions are obviously operating incorrectly for receiving or both receiving and delegating ATSUs.

Detected Corruption: Represents a failure mode where data or functions provided by the Service are incorrect but detected as incorrect by the Service due to deficiencies in design for receiving or both receiving and delegating ATSUs.

Undetected Corruption: Represents a failure mode where data or functions provided by the Service are incorrect and not detected as incorrect by the Service due to deficiencies in design for receiving or both receiving and delegating ATSUs.

The explanation on the derivation of the following integrity/reliability requirements can be found in the PJ.10-W2-93 V3 OSED Part II [9].

TSSR ID	TSSR for failure *(integrity/reliability)*	Related Operational Hazard	Severity & IM
TSSR-008	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
TSSR-009	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

EUROPEAN PARTNERSHIP

Co-funded by the European Union

TSSR-010	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
TSSR-011	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
TSSR-012	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
TSSR-013	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
TSSR-014	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
TSSR-015	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 4. TSSR for failure (integrity/reliability)

4.3.2 TSSR from other intended use

No TSSR from other intended use identified.

4.4 Process assurance of the Technical Safety Specification

The safety assessment was conducted according to SRM. The Technical Specification Safety Requirements (TSSRs) identified refer to the functionalities & performance characteristics derived from the (potential) operational uses envisaged for the technological solution limited to the potential safety implication on the side of the operational users (i.e. ATS service provider).

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

The following safety activities were performed with the participation of PJ.10-W2-93 solution partners:

Safety assessment activity	Scope	Personnel involved
HP&SAF Scoping & Change Assessment session	Definition safety strategy Safety planning	Safety experts Human Factors Expert ATCOs Operational experts
Safety Metrics and Indicators session	Identification of applicable metrics and indicators to be applied in the exercises for safety evidence	
HAZID activity	Hazard identification Safety System Requirements	

Table 5. Safety Activities

EUROPEAN PARTNERSHIP

Co-funded by the European Union

5 Safe Design of the Technical System

5.1 Overview of activities performed

This section addresses the following activities:

- introduction of the design model (initial or refined) of the Solution technical system – section 5.2
- derivation of Technical Safety Requirements (functionality & performance) at Design level (TSRD) in normal and abnormal conditions of operation - section 5.3
- assessment of the adequacy of the design (initial or refined) in the case of internal failures and mitigation of the Solution functionality hazards (identified in section 4.3) through derivation from TSSRs (integrity/reliability) of Technical Safety Requirements (functionality & performance) and Technical Safety Requirements (integrity/reliability) at Design level (TSRD) - section 5.4
- realism of the refined safe design (i.e. achievability and “testability” of the TSRD) - section 5.5
- process assurance at the initial or refined safe design level – section 5.6

5.2 Design Model of the Solution Technical System

5.2.1 Description of the Technical System 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 [14] and TS/IRS [16] documents.

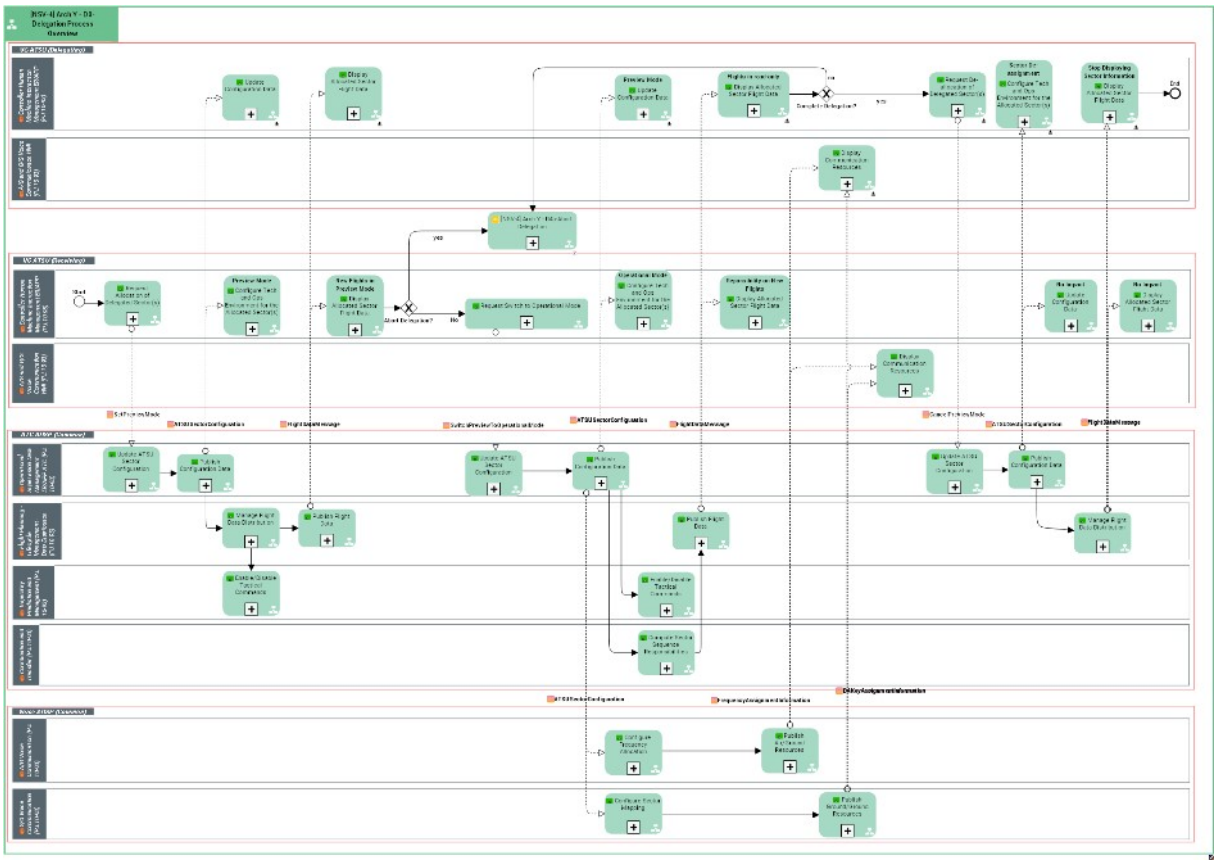

Figure 1. [NSV-4] Arch Y - D0-Delegation Process Overview

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 6. NSV-4 functions

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

5.3.1 Technical Safety Requirements at Design level for Normal and Abnormal conditions

The table below contains the list of Technical Safety Requirements at Design level (functionality and performance) for Normal and Abnormal conditions of operations. Most of these requirements have been extracted from PJ.10-W2-93 V3 OSED Part II SAR [8].

Technical Safety Requirement ID [Design Model element]	Technical Safety Requirement description (functionality & performance)	Derived from TSSR (ID)
TSRD-001 [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.	TSSR-001 TSSR-004

TSRD-002 [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 operational mode to preview mode in the delegating ATSU.	TSSR-001 TSSR-004
TSRD-003 [Preview 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.	TSSR-001 TSSR-004
TSRD-004 [Preview Mode]	The frequency of the delegated sector should automatically be disabled when the preview mode is terminated at the delegating ATSU.	TSSR-001 TSSR-004
TSRD-005 [all phases of the delegation]	Concerned technical staff shall receive appropriate training to perform shutdown/restart/reboot of operational equipment.	TSSR-005
TSRD-006 [abort delegation]	The operational Supervisor and/or the ATSEP shall be able to make the system input to abort a delegation.	TSSR-001 TSSR-002 TSSR-003
TSRD-007 [all phases of the delegation]	Recurrent Training shall be provided to VC technical staff in order to guarantee an optimal maintenance of competence.	TSSR-005
TSRD-008 [all phases of the delegation]	Synchronization between ATC ADSP and Voice ADSP supporting both receiving and delegating ATSUs is needed. This could be e.g. synchronization of frequency table data, etc.	TSSR-001 TSSR-004
TSRD-009 [all phases of the delegation]	The AMQP or equivalent message framework should provide a framework which will ensure a tamper proof message exchange between clients and servers.	TSSR-001 TSSR-003

TSRD-010 [all phases of the delegation]	The AMQP or equivalent message framework shall ensure that the Sender and Receiver are mutually agreed upon counter parties - No possibility for injection of Spam should be available.	TSSR-001 TSSR-003

Table 7: TSRD (functionality and performance) satisfying TSSRs for Normal conditions

The SRD for abnormal conditions identified in the V3 PJ.10-W2-93 OSED Part II [9] are applicable in the context of this document. In addition, the following abnormal conditions have been also identified:

	Abnormal condition	Effect	Mitigation of Effects / TSSR
ABN 001	Coordinated Cyber Security attack specific to the Virtual Centre architecture.	The ATM system making use of a Virtual Centre architecture may not be able to function as intended and safety levels (i.e. loss of separation) may be jeopardized due to coordinated cyber security attack. The operational effect would be loss of capability for controller to communicate with a/c.	Security assessment in accordance with best practise shall be conducted
ABN 002	Major communication malfunction	The ATM system making use of a Virtual Centre architecture may not be able to function as intended and safety levels may be jeopardized due to major communication failure.	Some of the identified Security Requirements (e.g., REQ-PJ10-W2-93-TS-SEC.003) are also applicable to mitigate the risk of encountering a contingency situation or avoiding the propagation of effects of its occurrence. For more details, please refer to TS/IRS [16]. TSRD-011: All critical equipment shall have redundant configurations to ensure switch-over in case of failure

Table 8. TSRD (functionality and performance) satisfying TSSRs for Abnormal conditions

5.3.2 Additional TSRD from Static/dynamic analysis of the technical system behaviour

No additional TSRDs were defined from static and dynamic analysis.

5.4 Technical Safety Requirements at design level addressing Internal System Failures

EUROPEAN PARTNERSHIP

Co-funded by the European Union

5.4.1 Design analysis with respect to internal system failure conditions

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

- Ensure identification of a complete list of failures that could cause each hazard
- Ensure identification of the required Mitigation means preventing causes to occur or preventing their effect to propagate towards each hazard
- Contribute to demonstrate the feasibility and effectiveness of the contingency procedures associated to the degraded modes of operation in which the technical 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 C and V3 PJ.10-W2-93 OSED Part II [9].

5.4.2 Technical Safety Requirements at design level addressing internal system failures

All the SRD for failure conditions identified in the V3 PJ.10-W2-93 OSED Part II [9] are applicable in the context of this document. In addition, the following TSRDs have been also identified (for more information, refer to Appendix C.2):

Technical Safety Requirement ID	Technical Safety Requirement description	Derived from TSSR integrity/reliability (ID)
TSRD-012	Coordination & Transfer Management service shall have Service Assurance Level (SAL) SAL3 after safety mitigation.	TSSR-008 TSSR-009
TSRD-013	Flight Data Distribution & Management services shall have Service Assurance Level (SAL) SAL3 after safety mitigation.	TSSR-008 TSSR-009
TSRD-014	Surveillance service shall have Service Assurance Level (SAL) SAL3 after safety mitigation.	TSSR-008 TSSR-009
TSRD-015	Voice Communication Distribution & Management service shall have Service Assurance Level (SAL) SAL3 after safety mitigation.	TSSR-008 TSSR-009 TSSR-010
TSRD-016	Correlation Distribution & Management services shall have Service Assurance Level (SAL) SAL3 after safety mitigation.	TSSR-008 TSSR-009
TSRD-017	Monitor Aids, Operational Supervisor, Secondary Surveillance Radar, Safety Nets, Technical	TSSR-008

	Supervisor services shall have Service Assurance Level (SAL) SAL4 after safety mitigation.	TSSR-009 TSSR-010 TSSR-011 TSSR-012 TSSR-013 TSSR-014 TSSR-015
TSRD-018	All services shall be segregated to ensure continuity of other services in case of malfunction of one specific service.	TSSR-008 TSSR-009 TSSR-010 TSSR-011 TSSR-012 TSSR-013 TSSR-014 TSSR-015
TSRD-019	All services shall have assigned a Service Assurance Level (SAL) to ensure proper Assurance Level of the service.	TSSR-008 TSSR-009 TSSR-010 TSSR-011 TSSR-012 TSSR-013 TSSR-014 TSSR-015
TSRD-020	The VCCI shall ensure that no corrupted data is provided to any communicating client.	TSSR-013
TSRD-021	The contract with the data providers shall ensure appropriate service availability, integrity, performance, security, etc	TSSR-013

TSRD-022	The communication service shall meet appropriate targets (KPIs) with regard to site availability, service interruption per site, network response time, packet delivery ratio, etc. to ensure that (related) hazard safety requirements are met and the probability of their occurrence is reduced as far as practicable.	TSSR-008 TSSR-009 TSSR-010 TSSR-011 TSSR-012 TSSR-013 TSSR-014 TSSR-015
TSRD-023	The AMQP or equivalent message framework shall be resilient towards technical failure of the underlying communication infrastructure, so that no transaction based messages, i.e. requests are lost.	TSSR-008 TSSR-009 TSSR-010 TSSR-011 TSSR-012 TSSR-013 TSSR-014 TSSR-015

Table 9. TSRD to mitigate functionality hazards

Also, the Reliability Requirements defined in the TS/IRS are applicable for addressing internal system failures. For more information, please refer to TS/IRS [16].

5.5 Realism and testability of the Safe Design

Considering the development and results of validation exercises executed and the safety assessment performed, it can be stated that safety assumptions are correct and coherent with the described scenarios, and that the requirements 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.

5.6 Process assurance of the 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.

TSRD ID	TS/IRS requirements ID	Requirement Text
TSRD-001	REQ-PJ.10-W2.93-TS-SAF024	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.
TSRD-002	REQ-PJ.10-W2.93-TS-SAF025	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.
TSRD-003	REQ-PJ.10-W2.93-TS-SAF026	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.
TSRD-004	REQ-PJ.10-W2.93-TS-SAF027	The frequency of the delegated sector should automatically be disabled when the preview mode is terminated at the delegating ATSU.
TSRD-005	REQ-PJ.10-W2.93-TS-SAF009	Concerned technical staff shall receive appropriate training to perform shutdown/restart/reboot of operational equipment.
TSRD-006	REQ-PJ.10-W2.93-TS-SAF028	The operational Supervisor and/or the ATSEP shall be able to make the system input to abort a delegation.
TSRD-007	REQ-PJ.10-W2.93-TS-SAF029	Recurrent Training shall be provided to VC technical staff in order to guarantee an optimal maintenance of competence.
TSRD-008	REQ-PJ.10-W2.93-TS-SAF030	Synchronization between ATC ADSP and Voice ADSP supporting both receiving and delegating ATSUs is needed. This could be e.g. synchronization of frequency table data, etc.
TSRD-009	REQ-PJ.10-W2.93-TS-SAF035	The AMQP or equivalent message framework should provide a framework which will ensure a tamper proof

		message exchange between clients and servers.
TSRD-010	REQ-PJ.10-W2.93-TS-SAF037	The AMQP or equivalent message framework shall ensure that the Sender and Receiver are mutually agreed upon counter parties - No possibility for injection of Spam should be available.
TSRD-012	REQ-PJ.10-W2.93-TS-SAF001	Coordination & Transfer Management service shall have Service Assurance Level (SAL) SAL3 after safety mitigation.
TSRD-013	REQ-PJ.10-W2.93-TS-SAF002	Flight Data Distribution & Management services shall have Service Assurance Level (SAL) SAL3 after safety mitigation.
TSRD-014	REQ-PJ.10-W2.93-TS-SAF003	Surveillance service shall have Service Assurance Level (SAL) SAL3 after safety mitigation.
TSRD-015	REQ-PJ.10-W2.93-TS-SAF004	Voice Communication Distribution & Management service shall have Service Assurance Level (SAL) SAL3 after safety mitigation.
TSRD-016	REQ-PJ.10-W2.93-TS-SAF005	Correlation Distribution & Management services shall have Service Assurance Level (SAL) SAL3 after safety mitigation.
TSRD-017	REQ-PJ.10-W2.93-TS-SAF006	Monitor Aids, Operational Supervisor, Secondary Surveillance Radar, Safety Nets, Technical Supervisor services shall have Service Assurance Level (SAL) SAL4 after safety mitigation.
TSRD-018	REQ-PJ.10-W2.93-TS-SAF007	All services shall be segregated to ensure continuity of other services in case of malfunction of one specific service.
TSRD-019	REQ-PJ.10-W2.93-TS-SAF008	All services shall have assigned a Service Assurance Level (SAL) to ensure proper Assurance Level of the service.
TSRD-020	REQ-PJ.10-W2.93-TS-SAF032	The VCCI shall ensure that no corrupted data is provided to any communicating client.
TSRD-021	REQ-PJ.10-W2.93-TS-SAF033	The contract with the data providers shall ensure appropriate service

		availability, integrity, performance, security, etc
TSRD-022	REQ-PJ.10-W2.93-TS-SAF034	The communication service shall meet appropriate targets (KPIs) with regard to site availability, service interruption per site, network response time, packet delivery ratio, etc. to ensure that (related) hazard safety requirements are met and the probability of their occurrence is reduced as far as practicable.
TSRD-023	REQ-PJ.10-W2.93-TS-SAF036	The AMQP or equivalent message framework shall be resilient towards technical failure of the underlying communication infrastructure, so that no transaction based messages, i.e. requests are lost.

6 Demonstration of achievability of the Technical System Safety Specification

Achievability of the TSSRs has been demonstrated through the validation objectives defined for Solutions PJ10-W2-93A-93B-93C and validated during exercises and additional specific safety assessment activities. (i.e. data analysis, Safety and HP workshops).

In the framework of the solutions PJ10-W2-93A-93B-93C, the validation exercises reported in section 2.3 have been performed and the VALR [18] presents the detailed results coming from these validation exercises. The exercises validation objectives and the related success criteria are summarized in Table below. These results have to be complemented with the ones related to the operational aspects reported in both VALR [18] and PJ.10-W2-93 SAR [9].

Exercise ID, Name, Goals	Validation Objective	Validation Exercise Success Criterion ID	Coverage (SAC, TSRS and/or TSRD)	Exercise Validation Results
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 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	EX3-OBJ-PJ.10-W2-93a-V3-VALP-001 Maturity Assessment To assess the maturity of the Virtual Centre architecture and services environment conditions	EX3-CRT-PJ.10-W2-93a-V3-VALP-01-001 A "VC maturity assessment report" is provided	**TSSR-001** **TSSR-002 Partially Covered** **TSSR-003** **TSSR-004** **TSSR-005** **TSSR-006 Partially Covered** **TSRD-001 Partially Covered** **TSRD-002 Partially Covered** **TSRD-003 Partially Covered** **TSRD-004 Partially Covered** **TSRD-005** **TSRD-006 Partially Covered** **TSRD-007**	N/A - No longer Valid Objective from the SJU feedback
	EX3-OBJ-PJ.10-W2-93a-V3-VALP-002 Validation Platform To produce and complement/provide the technical validation platform	EX3-CRT-PJ.10-W2-93a-V3-VALP-02-001 A Virtual Centre (VC) validation platform based on the Y architecture is put in place and supports the validation of the delegation scenarios dedicated to the Y architecture		Status of both ATC & Voice ADSPs are monitored thanks to supervision tools put in place either locally at the ATSU level and/or at the location of the remote ADSP. The ADSP related services are also monitored from the remote ATSUSs.
		EX3-CRT-PJ.10-W2-93a-V3-VALP-02-002 A Technical Supervision		

	place to monitor the status of the ATC ADSP and its services		
	EX3-CRT-PJ.10-W2-93a-V3-VALP-02-003 A Technical Supervision service is put in place to monitor the status of the Voice ADSP		
EX3-OBJ-PJ.10-W2-93a-V3-VALP-003 Virtual Centre Services To increase the number of defined as well as implemented Virtual Centre services	EX3-CRT-PJ.10-W2-93a-V3-VALP-03-001 Operational Supervision Management & Distribution (OPSUPM/D) services can support delegation scenarios in all their phases (Initial, Preview and final operational modes)		The ADSPs were fully supervised from the ATSUs to follow all the phases of the delegation: from Operation to Preview and then to Operational at the receiving. The same applies at the delegating ATSU. Some new services have been defined and validated and some existing ones have been validated at a higher maturity (TRL6)
	EX3-CRT-PJ.10-W2-93a-V3-VALP-03-002 Additional services OR already defined services under PJ16.03 but not yet validated, have been validated		
	EX3-CRT-PJ.10-W2-93a-V3-VALP-03-003 Additional - or updated operations within existing services- have been implemented and validated		

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 different architectures Y/U/D: • Delegation of ATM services provision at night. Delegation of ATM services provision in contingency (case of ATSU failure).	EX3-OBJ-PJ.10-W2-93a-V3-VALP-004 Interoperability To increase the number of defined as well as implemented Virtual Centre services	EX3-CRT-PJ.10-W2-93a-V3-VALP-04-001 Services from one ADSP have been provided to CWPs from different vendors/ANSPs	**TSRD-008** **TSRD-018 Partially Covered** **SAC#01** **SAC#02** **SAC#03**	Standard services are used between CCS and iTEC ADSPs and the various CWPs
		EX3-CRT-PJ.10-W2-93a-V3-VALP-04-002 CWPs of a vendor/ATSU have consumed the same services from ADSPs of different vendors		
		Performance of the A/G and G/G communications between CWPs of a same or of different voice ADSP(s) are judged acceptable by End users (ATCOs, SUPs, ATSEPs)		
	EX3-OBJ-PJ.10-W2-93a-V3-VALP-005 Virtual Centre services performance To complement the performance assessment of the Virtual Centre architecture and services	EX3-CRT-PJ.10-W2-93a-V3-VALP-05-001 Response time from the ADSP(s) to CWPs requests remains within a defined threshold		The overall performance of the VC components (Network, CWPs, ADSPs voice and ATC) were measured and good figures were shown, see below under EX3-OBJ-PJ.10-W2-93a-V3-VALP-005. The response time at the ATC or Voice CWPs are judged acceptable by the ATCOs and SUPs.
		EX3-CRT-PJ.10-W2-93a-V3-VALP-05-002 Network capacity has been evaluated as being sufficient to support data flows within the Validation Platform		
		EX3-CRT-PJ.10-W2-93a-V3-VALP-05-003 Removed as it is the same		

		as EX3-CRT-PJ.10-W2-93a-V3-VALP-05-001		
		EX3-CRT-PJ.10-W2-93a-V3-VALP-05-004 Average time for a CWP switch to a Preview Mode is acceptable and Safe for the operations		
		EX3-CRT-PJ.10-W2-93a-V3-VALP-05-005 Average time for a CWP switch from a Preview to Operational Mode is acceptable and Safe for the operations		
		EX3-CRT-PJ.10-W2-93a-V3-VALP-05-006 The Global time to perform the overall delegation process is acceptable for the operations		
	EX3-OBJ-PJ.10-W2-93b-V3-VALP-001 Maturity Assessment To assess the maturity of the Virtual Centre architecture and services environment conditions	EX3-CRT-PJ.10-W2-93b-V3-VALP-01-001 A "VC maturity assessment report" is provided		N/A - No longer Valid Objective from the SJU feedback
	EX3-OBJ-PJ.10-W2-93b-V3-VALP-002 Validation Platform To produce and complement/provide the technical validation platform	EX3-CRT-PJ.10-W2-93b-V3-VALP-02-001 A Virtual Centre (VC) validation platform based on the D architecture is put		Status of both ATC & Voice ADSPs are monitored thanks to supervision tools put in place either locally at the ATSU level

	in place and supports the validation of the delegation scenarios dedicated to the D architecture		and/or at the location of the remote ADSP. The ADSP related services are also monitored from the remote ATSUSs.
	EX3-CRT-PJ.10-W2-93b-V3-VALP-02-002 A Technical Supervision service is put in place to monitor the status of the ATC ADSP and its services		
	EX3-CRT-PJ.10-W2-93b-V3-VALP-02-003 A Technical Supervision service is put in place to monitor the status of the Voice ADSP		
EX3-OBJ-PJ.10-W2-93b-V3-VALP-003 Virtual Centre Services To increase the number of defined as well as implemented Virtual Centre services	EX3-CRT-PJ.10-W2-93b-V3-VALP-03-001 Operational Supervision Management & Distribution (OPSUPM/D) services can support delegation scenarios in all their phases (Initial, Preview and final operational modes)		The ADSPs were fully supervised from the ATSUs to follow all the phases of the delegation: from Operation to Preview and then to Operational at the receiving. The same applies at the delegating ATSU.
	EX3-CRT-PJ.10-W2-93b-V3-VALP-03-002 Additional services OR already defined services under PJ16.03 but not		

	yet validated, have been validated		
	EX3-CRT-PJ.10-W2-93b-V3-VALP-03-003 Additional - or updated operations within existing services- have been implemented and validated		
EX3-OBJ-PJ.10-W2-93b-V3-VALP-004 Interoperability To increase the number of defined as well as implemented Virtual Centre services	EX3-CRT-PJ.10-W2-93b-V3-VALP-04-001 Services from one ADSP have been provided to CWPs from different vendors/ANSPs		Standard services are used between CCS and iTEC ADSPs and the various CWPs and the specific DFS CWP was able to connect to two different ADSPs: CCS and iTEC
	EX3-CRT-PJ.10-W2-93b-V3-VALP-04-002 CWPs of a vendor/ATSU have consumed the same services from ADSPs of different vendors		
	EX3-CRT-PJ.10-W2-93b-V3-VALP-04-003 Performance of the A/G and G/G communications between CWPs of a same or of different voice ADSP(s) are judged acceptable by End users (ATCOs, SUPs, ATSEPs)		
EX3-OBJ-PJ.10-W2-93b-V3-VALP-005 Virtual Centre services performance To complement the performance	EX3-CRT-PJ.10-W2-93b-V3-VALP-05-001 Response time from the ADSP(s) to CWPs requests remains		The overall performance of the VC components (Network, CWPs, ADSPs voice and ATC) were

	assessment of the Virtual Centre architecture and services	within a defined threshold		measured and good figures were shown, see below under EX3-OBJ-PJ.10-W2-93a-V3-VALP-005. The response time at the ATC or Voice CWPs are judged acceptable by the ATCOs and SUPs.
		EX3-CRT-PJ.10-W2-93b-V3-VALP-05-002 Network capacity has been evaluated as being sufficient to support data flows within the Validation Platform		
		EX3-CRT-PJ.10-W2-93b-V3-VALP-05-003 Removed as it is the same as EX3-CRT-PJ.10-W2-93b-V3-VALP-05-001		
		EX3-CRT-PJ.10-W2-93b-V3-VALP-05-004 Average time for a CWP switch to a Preview Mode is acceptable and Safe for the operations		
		EX3-CRT-PJ.10-W2-93b-V3-VALP-05-005 Average time for a CWP switch from a Preview to Operational Mode is acceptable and Safe for the operations		
		EX3-CRT-PJ.10-W2-93b-V3-VALP-05-006 The Global time to perform the overall delegation process is acceptable for the operations		

	EX3-OBJ-PJ.10-W2-93c-V3-VALP-001 **Maturity Assessment** To assess the maturity of the Virtual Centre architecture and services environment conditions	EX3-CRT-PJ.10-W2-93c-V3-VALP-01-001 A "VC maturity assessment report" is provided		N/A - No longer Valid Objective from the SJU feedback
	EX3-OBJ-PJ.10-W2-93c-V3-VALP-002**Validation Platform** To produce and complement/provide the technical validation platform	EX3-CRT-PJ.10-W2-93c-V3-VALP-02-001 A Virtual Centre (VC) validation platform based on the U architecture is put in place and supports the validation of the delegation scenarios dedicated to the U architecture		EX3-CRT-PJ.10-W2-93c-V3-VALP-02-001 is not considered as a SC by the SJU Status of both ATC & Voice ADSPs are monitored thanks to supervision tools put in place either locally at the ATSU level and/or at the location of the remote ADSP
		EX3-CRT-PJ.10-W2-93c-V3-VALP-02-002 A Technical Supervision service is put in place to monitor the status of the ATC ADSP and its services		
		EX3-CRT-PJ.10-W2-93c-V3-VALP-02-003 A Technical Supervision service is put in place to monitor the status of the Voice ADSP		
	EX3-OBJ-PJ.10-W2-93c-V3-VALP-003**Virtual Centre Services** To increase the number of defined as well as implemented Virtual Centre services	EX3-CRT-PJ.10-W2-93c-V3-VALP-03-001 Specific inter-ADSP services have been defined to manage airspace delegation in “U” architecture		The synchronisation work between the CCS and iTEC ADSPs has well started but a lot of missing data have made this solution as not enough mature, see below analysis
		EX3-CRT-PJ.10-W2-93c-V3-VALP-04-		While the voice ADSP was as much

	EX3-OBJ-PJ.10-W2-93c-V3-VALP-004 **Interoperability** To increase the number of defined as well as implemented Virtual Centre services	001 Specific to U: the ADSPs have successfully shared data between them to allow for delegation		mature as for the Y/D architectures, the data sharing between the ADSPs was just not sufficient to guarantee a safe delegation procedure. However, there was no issue to play UC# with Dynamic AoR under the U architecture
		EX3-CRT-PJ.10-W2-93c-V3-VALP-04-002 Specific to U: the ADSP has been able to increase or reduce its AoR		
		EX3-CRT-PJ.10-W2-93c-V3-VALP-04-003 The Voice ADSPs (when many) are able to exchange voice communications A/G and G/G		
	EX3-OBJ-PJ.10-W2-93c-V3-VALP-005 **Virtual Centre services performance** To complement the performance assessment of the Virtual Centre architecture and services	EX3-CRT-PJ.10-W2-93c-V3-VALP-05-001 Network capacity has been evaluated as being sufficient to support data flows within the Validation Platform		For this Objective, the results obtained from the U/D architectures are also valid for the U architecture for the first five SC which are all of them validated OK. However, for the last two criteria (% of coordinated flights), the level of automation was not acceptable for the operations.
		EX3-CRT-PJ.10-W2-93c-V3-VALP-05-002 Quality of Service (QoS) during the EXE runs has been evaluated		
		EX3-CRT-PJ.10-W2-93c-V3-VALP-05-003 Average time for a CWP switch to a Preview Mode is acceptable and Safe for the operations		
		EX3-CRT-PJ.10-W2-93c-V3-VALP-05-004 Average time for a CWP switch from a Preview to Operational Mode		

		is acceptable and Safe for the operations		
		EX3-CRT-PJ.10-W2-93c-V3-VALP-05-005 The Global time to perform the overall delegation process is acceptable for the operations		
		EX3-CRT-PJ.10-W2-93c-V3-VALP-05-006 Specific to U: % of Coordinated flights between ADSPs against total number of flights is in a acceptable rate for the operations		
		EX3-CRT-PJ.10-W2-93c-V3-VALP-05-007 Specific to U: % of manually coordinated flights between ATSUs against total number of flights is in a acceptable rate for the operations		
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	EX4-OBJ-PJ.10-W2-93a-V3-VALP-001 To assess the maturity of the Virtual Centre architecture and services environment conditions	EX4-CRT-PJ.10-W2-93a-V3-VALP-01-001 A "VC maturity assessment report" is provided	**TSSR-001** **TSSR-002** **TSSR-003** **TSSR-004**	Updated the VC Services in the Maturity Report PJ32 WP3
	EX4-OBJ-PJ.10-W2-93a-V3-VALP-002To produce and complement/provide the technical validation platform	EX4-CRT-PJ.10-W2-93a-V3-VALP-02-001 A Virtual Centre (VC) validation platform based on the Y architecture is put in place and supports the validation of the delegation scenarios dedicated	**TSSR-005** **TSSR-006 Partially Covered** **TSRD-001** **TSRD-002** **TSRD-003** **TSRD-004**	Reported in the EXE 4 Availability Note based on a VC Architectures

	to the Y architecture		
	EX4-CRT-PJ.10-W2-93a-V3-VALP-02-002 A Technical Supervision service is put in place to monitor the status of the ATC ADSP and its services		
EX4-OBJ-PJ.10-W2-93a-V3-VALP-003To increase the number of defined as well as implemented Virtual Centre services	EX4-CRT-PJ.10-W2-93a-V3-VALP-02-003 A Technical Supervision service is put in place to monitor the status of the Voice ADSP		
	EX4-CRT-PJ.10-W2-93a-V3-VALP-03-001 Operational Supervision Management & Distribution (OPSUPM/D) services can support delegation scenarios in all their phases (Initial, Preview and final operational modes)		One ADSP with 2 different ATSUs were considered in the Validation. Several List of the operation in the appropriate services Have been validated (OSUP and Technical Supervision)
	EX4-CRT-PJ.10-W2-93a-V3-VALP-03-002 Additional services OR already defined services under PJ16.03 but not yet validated, have been validated		
	EX4-CRT-PJ.10-W2-93a-V3-VALP-03-003 Additional - or updated operations within existing services- have been implemented and validated		
EX4-OBJ-PJ.10-W2-93a-V3-VALP-004To increase	EX4-CRT-PJ.10-W2-93a-V3-VALP-04-		Standard services are used between

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: • 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	the number of defined as well as implemented Virtual Centre services	001 Services from one ADSP have been provided to CWPs from different vendors/ANSPs	**TSRD-005** **TSRD-006** **TSRD-007** **TSRD-008**	CCS ADSP and the various CWPs of LIBB and LIRR ATSUs provided by LEONARDO with a "Y" Architecture
		EX4-CRT-PJ.10-W2-93a-V3-VALP-04-002 CWPs of a vendor/ATSU have consumed the same services from ADSPs of different vendors	**TSRD-018 Partially covered** **SAC#001**	
		EX4-CRT-PJ.10-W2-93a-V3-VALP-04-003 Performance of the A/G and G/G communications between CWPs of a same or of different voice ADSP(s) are judged acceptable by End users (ATCOs, SPVRs, ATSEPs)	**SAC#002** **SAC#003**	
	EX4-OBJ-PJ.10-W2-93a-V3-VALP-005Virtual Centre services performance To complement the performance assessment of the Virtual Centre architecture and services	EX4-CRT-PJ.10-W2-93a-V3-VALP-05-001 Response time from the ADSP(s) to CWPs requests remains within a defined threshold		Starting from the Verification, integration and Validation the overall performances of the system were measured with an appropriate analysis resulted acceptable range of QoS.
		EX4-CRT-PJ.10-W2-93a-V3-VALP-05-002 Network capacity has been evaluated as being sufficient to support data flows within the Validation Platform		
		EX4-CRT-PJ.10-W2-93a-V3-VALP-05-003 Quality of		

		Service (QoS) during the EXE runs has been evaluated		
		EX4-CRT-PJ.10-W2-93a-V3-VALP-05-004 Average time for a CWP switch to a Preview Mode is acceptable and Safe for the operations		
		EX4-CRT-PJ.10-W2-93a-V3-VALP-05-005 Average time for a CWP switch from a Preview to Operational Mode is acceptable and Safe for the operations		
		EX4-CRT-PJ.10-W2-93a-V3-VALP-05-006 The Global time to perform the overall delegation process is acceptable for the operations		
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 case of contingency	EXE5-OBJ-PJ.10-W2-93-V3-VALP-024 To assess the maturity of the Virtual Centre architecture and services	EXE5-CRT-PJ.10-W2-93-V3-VALP-024-001 A "VC maturity assessment report" is provided	**TSSR-002** **TSSR-003** **TSRD-005** **TSRD-006** **TSRD-007** **TSRD-008** **Partially Covered**	This Validation Objective status is OK. Overall, the Y-architecture based platform was mature enough and provided the requested services to the operators.
	EXE5-OBJ-PJ.10-W2-93-V3-VALP-025 To produce and complement/provide the technical validation platform	EXE5-CRT-PJ.10-W2-93-V3-VALP-025-001 Validation platforms based on a "legacy Y" architecture are put in place and are ready for use to	**SAC#001** **SAC#002** **SAC#003**	This Validation Objective status is OK. The main identified limitation in the virtual centre architecture that

• Delegation of ATM services provision on-demand		play the identified operational scenarios under PJ10.93		was found under the validation was the speed in transfer of data. A VPN connection via public internet was used, and delays in data transmission was observed during all runs, especially in the later part of the runs, when a lot of data occupied the available connection.

7 Acronyms and Terminology

Term	Definition
ADSP	ATM Data Service Provider
AIM	Accident Incident Model
AMPQ	Advanced Message Queuing Protocol
ANSP	Air Navigation Service Provider
AoR	Area of Responsibility
ATCO	Air Traffic Controller
ATSEP	Air traffic safety electronics personnel
ATSU	Air Traffic Services Unit
CNS	Communication Navigation Surveillance
FHA	Functional Hazard Analysis
HMI	Human Machine Interface
HP	Human Performance
LoA	Letter of Agreement
MAC-ER	Mid Air Collision En-Route
MAC-SC	Mid Air Collision Severity Classes
OE	Operational Environment
OH	Operational Hazard
OLDI	On-Line Data Interchange
OSED	Operational Service Environment Description
SAL	Service Assurance Level
SAP	Safety Assessment Plan
SAR	Safety Assessment Report
SPR	Safety Performance Requirements
SRD	Safety Requirements at ATS Design level

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SRM	SESAR Safety Reference Methodology
SRS	Safety Requirements at ATS Service level
TS/IRS	Technical Specification / Interface Requirements Specification
TSRS	Technical Specification Safety Requirements
TSRD	Technical Safety Requirements at Design Level
UC	Use Case
VALP	Validation Plan
VALR	Validation Report
VC	Virtual Centre
VCCI	Virtual Centre Communication Infrastructure
VCS	Voice Communication System

Table 10: Acronyms

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] (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)

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

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

[7] SESAR SOLUTION PJ.16-03 VC SPR-INTEROP/OSED FOR TRL6 - PART II – Safety Assessment Report

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

[9] SESAR2020 PJ.10-W2-93 V3 SPR-INTEROP/OSED Part II – Safety Assessment Report

Human Performance

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

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

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

General

[13] SESAR 2020 PJ19 Validation Targets (2020)

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

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

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

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

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

[19] EUROCAE: Virtual Centre – Strategy for Standardisation – Phase 1, November 2021

Appendix A Defining the Technical Safety Specification based on other intended use

A.1 Define TSSRs for Normal and Abnormal conditions

Within the Safety & HP Scoping and change assessment session of a preliminary safety impact assessment (including initial hazard identification) was conducted, involving operational experts which are relevant for the use of the technological concept (ATCOs, technical experts, HF experts, Safety experts), to understand the potential safety implication of the solution. The results of the initial hazards identification for normal and abnormal conditions and the related TSSRs are presented in section 4.2.2.

Furter details on the derivation of requirements are provided in the PJ.10-W2-93 V3 SAR [9].

A.1.1 Static analysis of the technical specification

No new TSSR was identified from a static analysis of the functional system behaviour.

A.1.2 Dynamic analysis of the technical specification

No new TSSR was identified from a dynamic analysis of the functional system behaviour.

A.2 Define TSSRs addressing failure conditions

EUROPEAN PARTNERSHIP

Co-funded by the European Union

A.2.1 FHA

Use Case / Functionality Failure mode	Example of causes & preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Functionality hazard & Severity
Delegation of ATM services provision in case of contingency / Partial or Complete Loss	ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure (Main Comm failure, Fallback Comm failure) Operator 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 / Partial or Complete Loss	ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure (Main Comm failure, Fallback Comm failure) Operator 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
Delegation of ATM services provision in case of contingency / Service Loss	ADSP Failure (ATC ADSP failure, Voice 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

Use Case / Functionality Failure mode	Example of causes & preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Functionality hazard & Severity
Delegation of ATM services provision in case of contingency / Service Loss	ADSP Failure (ATC ADSP failure, Voice 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
Delegation of ATM services provision in case of contingency / Detected Corruption	Data corrupted (Data corrupted by ATC ADSP; Data corrupted by Voice ADSP) ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure Maintenance Error Technical Personnel Error (Erroneous data input by operator) / Lack of training	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

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Use Case / Functionality Failure mode	Example of causes & preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Functionality hazard & Severity
Delegation of ATM services provision in case of contingency / Undetected Corruption	Data corrupted (Data corrupted by ATC ADSP; Data corrupted by Voice ADSP) ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure Maintenance Error Technical Personnel Error (Erroneous data input by operator) / Lack of training	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

Table 11. FHA working table

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix B Designing the Solution technical system for normal and abnormal conditions

B.1 Deriving TSRDs from TSSRs

Table below shows the TSRD derived from the TSRS presented in section 5.3.1.

TSSR for Normal&Abnormal Operation (ID & content)	Technical Safety Requirement at Design level[1] (TSRD) or Assumption	Maps onto
TSSR-001 TSSR-004	TSRD-001 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]
TSSR-001 TSSR-004	TSRD-002 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]
TSSR-001 TSSR-004	TSRD-003 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]
TSSR-001 TSSR-004	TSRD-004 The frequency of the delegated sector should automatically be disabled when the preview mode is terminated at the delegating ATSU.	[Preview Mode]

[1] iTSRD for the initial design or rTSRD for the refined design

TSSR-005	TSRD-005 Concerned technical staff shall receive appropriate training to perform shutdown/restart/reboot of operational equipment.	[all phases of the delegation]
TSSR-001 TSSR-002 TSSR-003	TSRD-006 The operational Supervisor and/or the ATSEP shall be able to make the system input to abort a delegation.	[abort delegation]
TSSR-005	TSRD-007 Recurrent Training shall be provided to VC technical staff in order to guarantee an optimal maintenance of competence.	[all phases of the delegation]
TSSR-001 TSSR-004	TSRD-008 Synchronization between ATC ADSP and Voice ADSP supporting both receiving and delegating ATSUs is needed. This could be e.g. synchronization of frequency table data, etc.	[all phases of the delegation]
TSSR-001 TSSR-003	TSRD-009 The AMQP or equivalent message framework should provide a framework which will ensure a tamper proof message exchange between clients and servers.	[all phases of the delegation]
TSSR-001 TSSR-003	TSRD-010 The AMQP or equivalent message framework shall ensure that the Sender and Receiver are mutually agreed upon counter parties - No possibility for injection of Spam should be available.	[all phases of the delegation]
TSSR-001 TSSR-006	TSRD-011 All critical equipment shall have redundant configurations to ensure switch-over in case of failure	[all phases of the delegation]

Table 12: TSRDs derived by mapping TSSRs for normal and abnormal conditions of operation to Design Model Elements

B.2 Static analysis of the technical system

From the analysis of the NOV-5 / NSV-4 diagrams developed in the framework of the solution, the TSRD presented in section B1 have been derived. No additional SRDs considered after static analysis of the functional system behaviour.

B.3 Dynamic analysis of the technical system

Real time simulations have been conducted and they represent a form of dynamic analysis. Meanwhile, no additional TSRDs have been derived from the execution of the validation exercises.

Appendix C Designing the technical system for addressing Internal System Failures

This appendix provides the several causes for each of the identified hazards in Appendix A. Note that this is based in SESAR 2020 Wave 1 PJ.16-03 work and that all data is not presented here.

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

C.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. The table below lists the causes identified and relates them to these hazards.

Causes	Hazard Description	Hazard Identification
ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure (Main Comm failure, Fallback Comm failure) Operator Failure	Loss of Service prevents controller from managing one or many aircraft for receiving ATSU	OH 01
ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure (Main Comm failure, Fallback Comm failure) Operator Failure	Loss of Service prevents controller from managing one or many aircraft for both delegating and receiving ATSUs	OH 02
ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure Maintenance Error	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

Causes	Hazard Description	Hazard Identification
Technical Personnel Error / Lack of training		
ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure Maintenance Error Technical Personnel Error / Lack of training	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 (Data corrupted by ATC ADSP; Data corrupted by Voice ADSP) ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure Maintenance Error Technical Personnel Error (Erroneous data input by operator) / Lack of training	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 (Data corrupted by ATC ADSP; Data corrupted by Voice ADSP)	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

Causes	Hazard Description	Hazard Identification
ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure Maintenance Error Technical Personnel Error (Erroneous data input by operator) / Lack of training		

Table 13. List of causes, generating hazards

Common Cause Analysis

Hazard Identification	Causes	Consequences (Common cause analysis)	
OH 01	ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure (Main Comm failure, Fallback Comm failure) Operator Failure	Near Mid Air Collision (MF3a)	Increase of workload; Decrease of situational awareness
OH 02	ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure (Main Comm failure, Fallback Comm failure) Operator Failure		
OH 06	Data corrupted (Data corrupted by ATC ADSP; Data corrupted by Voice ADSP) ADSP Failure (ATC ADSP failure, Voice ADSP failure)		

Hazard Identification	Causes	Consequences (Common cause analysis)	
	Infrastructure failure Maintenance Error Technical Personnel Error (Erroneous data input by operator) / Lack of training		
OH 03	ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure Maintenance Error Technical Personnel Error / Lack of training	Imminent Infringement (MF5.9)	
OH 04	ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure Maintenance Error Technical Personnel Error / Lack of training		
OH 05	Data corrupted (Data corrupted by ATC ADSP; Data corrupted by Voice ADSP) ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure Maintenance Error Technical Personnel Error (Erroneous data input by operator) / Lack of training	Imminent Collision (MF4)	

Table 14. 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 (ATC ADSP failure, Voice ADSP failure) Infrastructure failure (Main Comm failure, Fallback Comm failure) Operator Failure	Near Mid Air Collision (MF3a)	Increase of workload; Decrease of situational awareness	Operating methods (procedures) covers all operations (normal and abnormal conditions); Training for ATCOs covers all operations (normal and abnormal conditions); Systems redundancy SAL assigned to all services Training for ATSEP Recurrent Training for all the technical and operational staff License for ATSEPs of the ADSP for the technical systems they are operating Coordination and synchronization messages exchange between ATSUs
OH 02	Loss of Service prevents controller from managing one or many aircraft for both delegating and receivingATSUs	ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure (Main Comm failure, Fallback Comm failure) Operator 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 (Data corrupted by ATC ADSP; Data corrupted by Voice ADSP) ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure Maintenance Error			

Hazard Identification	Hazard Description	Causes	Consequences (Common cause analysis)		Mitigations
		Technical Personnel Error (Erroneous data input by operator) / Lack of training			
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 safely manage traffic.	ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure Maintenance Error Technical Personnel Error / Lack of training	Imminent Infringement (MF5.9)		
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	ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure Maintenance Error Technical Personnel Error / Lack of training			

Hazard Identification	Hazard Description	Causes	Consequences (Common cause analysis)		Mitigations
	safely manage traffic.				
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 (Data corrupted by ATC ADSP; Data corrupted by Voice ADSP) ADSP Failure (ATC ADSP failure, Voice ADSP failure) Infrastructure failure Maintenance Error Technical Personnel Error (Erroneous data input by operator) / Lack of training	Imminent Collision (MF4)		

Table 15. List of mitigations to reduce likelihood of hazards

The Reliability Requirements defined in the TS/IRS [16] are applicable for addressing internal system failures.

C.2 Deriving TSRD from the TSSR (functionality&performance) for protective mitigation

Within the Safety Assessment conducted for V3 PJ.10-W2-93 [9], 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.

In addition to these requirements, this document presents further requirements based on allocation of a Service Assurance Level (SAL) for all services done in accordance with the hazard identification and analysis made in the Appendix A and PJ.10-W2-93 V3 OSED Part II [9]. Loss of service is the failure mode when specific services are lost, it means that the overall capability to manage traffic has been lost. The loss of a specific service results in occurrence of specific hazards. The analysis made in the SAR reports the highest Severity Class for the identified hazards (i.e. MAC-SC2a, MAC-SC2b, MAC-SC3). The process for the allocation of the SAL has been defined:

- Taking into account current regulation and standards on assurance levels;
- Being in line with the SRM [2] approach (hazards identification, severity classes, etc.);
- Using, as relevant, existing tools, techniques and processes already defined in the SRM [2] (AIM, FHA, etc.)

In order to associate a SAL, the severity of the effect of the hazard given by the Severity Classification Schemes from SRM Guidance G.3 [3] has been used thereby leading to dedicated tables.

MAC-ER/TMA	**Severity Class**							
Likelihood of generating such an effect	***MAC-SC1***	***MAC-SC2a***	***MAC-SC2b***	***MAC-SC3***	***MAC-SC4a***	***MAC-SC4b***	***MAC-SC5***	***No immediate effect on safety***
Very Possible	**SAL1**	**SAL3**	**SAL3**	**SAL3**	**SAL3**	**SAL4**	**SAL4**	**SAL5**
Possible	**SAL2**	**SAL3**	**SAL3**	**SAL3**	**SAL4**	**SAL4**	**SAL4**	**SAL5**
Very Unlikely	**SAL2**	**SAL3**	**SAL3**	**SAL4**	**SAL4**	**SAL4**	***SAL4***	**SAL5**
Extremely Unlikely	**SAL3**	**SAL3**	**SAL4**	**SAL4**	**SAL4**	***SAL4***	***SAL4***	**SAL5**

Table 16. Service Assurance Level Allocation per Severity Class

In order to ensure the mitigation effectiveness, the following safety requirements have been introduced:

Technical Safety Requirement ID	**Technical Safety Requirement at Design level[2] (TSRD)**	**Maps onto Enabler or Design Model Elements**
TSSR-008 TSSR-009	TSRD-012 Coordination & Transfer Management service shall have Service Assurance Level (SAL) SAL3 after safety mitigation.	SVC-015_Provision and Consumption of Arrival Sequence Management Service CoordinationAndTransferManagement (PJ.32-WP3)

TSSR-008 TSSR-009	TSRD-013 Flight Data Distribution & Management services shall have Service Assurance Level (SAL) SAL3 after safety mitigation.	SVC-008_Provision and Consumption of FlightDataDistribution Service in the context of Virtual Centres. SVC-009_Provision and Consumption of FlightDataManagement Service in the context of Virtual Centres FlightDataDistribution (PJ.32-WP3) FlightDataManagement (PJ.32-WP3)
TSSR-008 TSSR-009	TSRD-014 Surveillance service shall have Service Assurance Level (SAL) SAL3 after safety mitigation.	SVC-028_Provision and Consumption of Surveillance Data Distribution Service SurveillanceDataDistribution
TSSR-008 TSSR-009 TSSR-010	TSRD-015 Voice Communication Distribution & Management service shall have Service Assurance Level (SAL) SAL3 after safety mitigation.	SVC-033_Provision and Consumption of Voice Comm Information Distribution Service SVC-034_Provision and Consumption of Voice Comm Management Service VoiceCommManagement VoiceCommInformationDistribution
TSSR-008 TSSR-009	TSRD-016 Correlation Distribution & Management services shall have Service Assurance Level (SAL) SAL3 after safety mitigation.	SVC-016_Provision and Consumption of Correlation Distribution Service SVC-017_Provision and Consumption of Correlation Management Service CorrelationManagement CorrelationDistribution (PJ.32-WP3)
TSSR-008 TSSR-009 TSSR-010 TSSR-011 TSSR-012 TSSR-013 TSSR-014	TSRD-017 Monitor Aids, Operational Supervisor, Secondary Surveillance Radar, Safety Nets, Technical Supervisor services shall have Service Assurance Level (SAL) SAL4 after safety mitigation.	SVC-029_Provision and Consumption of Technical Supervision Distribution Service SVC-020_Provision and Consumption of Monitoring Aids Distribution Service SVC-023_Provision and Consumption of Safety Net (SNET) Alert Distribution Service

TSSR-015		SVC-022_Provision and Consumption of Operational Configuration Management Service SVC-021_Provision and Consumption of Operational Configuration Distribution Service MonitoringAidsDistribution (PJ.32-WP3) SNETAlertDistribution OperationalConfigurationDistribution (PJ.10-93) OperationalConfigurationManagement (PJ.10-93) TechnicalSupervisionDistribution (PJ.32-WP3)
TSSR-008 TSSR-009 TSSR-010 TSSR-011 TSSR-012 TSSR-013 TSSR-014 TSSR-015	TSRD-018 All services shall be segregated to ensure continuity of other services in case of malfunction of one specific service.	ER APP ATC 184_ATM Data Service Provider for ATC services in a Virtual Centre context ER APP ATC 185_ATM Data Service Provider for Voice services in a Virtual Centre context
TSSR-008 TSSR-009 TSSR-010 TSSR-011 TSSR-012 TSSR-013 TSSR-014 TSSR-015	TSRD-019 All services shall have assigned a Service Assurance Level (SAL) to ensure proper Assurance Level of the service.	ER APP ATC 184_ATM Data Service Provider for ATC services in a Virtual Centre context ER APP ATC 185_ATM Data Service Provider for Voice services in a Virtual Centre context

TSSR-013	TSRD-020 The VCCI shall ensure that no corrupted data is provided to any communicating client.	Communication Infrastructure
TSSR-013	TSRD-021 The contract with the data providers shall ensure appropriate service availability, integrity, performance, security, etc	ER APP ATC 184_ATM Data Service Provider for ATC services in a Virtual Centre context ER APP ATC 185_ATM Data Service Provider for Voice services in a Virtual Centre context
TSSR-008 TSSR-009 TSSR-010 TSSR-011 TSSR-012 TSSR-013 TSSR-014 TSSR-015	TSRD-022 The communication service shall meet appropriate targets (KPIs) with regard to site availability, service interruption per site, network response time, packet delivery ratio, etc. to ensure that (related) hazard safety requirements are met and the probability of their occurrence is reduced as far as practicable.	Communication Infrastructure
TSSR-008 TSSR-009 TSSR-010 TSSR-011 TSSR-012 TSSR-013 TSSR-014 TSSR-015	TSRD-023 The AMQP or equivalent message framework shall be resilient towards technical failure of the underlying communication infrastructure, so that no transaction based messages, i.e. requests are lost.	Communication Infrastructure

Table 17. TSRD for protective mitigation

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix D Assumptions, Safety Issues & Limitations

D.1 Assumptions log

A set of assumptions have been developed for each VC service and documented in the TS-IRS Part I [17].

D.2 Safety Issues log

No safety issues were identified during the assessment process.

D.3 Operational Limitations log

No operational limitations were identified during the assessment process.

-END OF DOCUMENT-

EUROPEAN PARTNERSHIP

Co-funded by the European Union