PJ.W2 PROSA

D4.2.020-PJ.10-W2-96 AG-TRL6-Final TS-IRS-Part II-SAR

Deliverable ID:	**D4.2.020**
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:	**16 February 2023**
Edition:	**00.02.00**
Template Edition:	**00.00.01**

Founding Members
EUROPEAN UNION EUROCONTROL
SESAR JOINT UNDERTAKING

Authoring & Approval

Authors of the document

Name/Beneficiary	Position/Title	Date
HungaroControl	Safety expert	10/10/2022

Reviewers internal to the project

Name/Beneficiary	Position/Title	Date
Skyguide	Task Contributor	16/11/2022

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

Name/Beneficiary	Position/Title	Date
LDO	Task Contributor	16/11/2022
Skyguide	Task Contributor	16/11/2022
NATS	Task Contributor	02/12/2022

Rejected By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date

Document History

Edition	Date	Status	Author	Justification
00.00.01	10/10/2022	Draft	HungaroControl	Creation of document
00.01.00	11/11/2022	Revised draft	HungaroControl	Updated based on validation results
00.02.00	16/02/2023	Final	Hungarocontrol	Updated version addressing SJU comments

Copyright Statement

PJ.10-W2 PROSA

SEPARATION MANAGEMENT AND CONTROLLER TOOLS

This Deliverable 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

The PJ.10-W2-Sol.96 AG deals with new methods of controller interaction with Human Machine Interface (HMI), implementing a fade-out algorithm in a very high complexity environment to bring a positive effect on the controller productivity with no negative impact on human performance, safety and capacity.

This document is Part II of the TS/IRS related to the SESAR Project ***PJ.10-W2-Sol.96*** - *"Attention Guidance"* function at technology readiness level (TRL). 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 contains also the Technical System Safety Specification identified for the Solution.

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This document contains the Specimen Safety Assessment for a typical application of the PJ.10-W2-Sol.96 Technological Solution. The Functional Block “Attention Guidance” for en-route (ER) of the European Air Traffic Management (ATM) Architecture (EATMA) is created with new AG-related functions: Attention Guidance Logic and Attention Guidance Measures. These functions will also deal with the

- identification of AG impacts on the overall architecture, and
- development of functional and non-functional requirements.

The Safety Assessment Report (SAR) represents Part II of the TS/IRS document and presents the assurance that the Safety Requirements for the TRL6 phases are complete, correct and realistic, thereby providing all material to adequately inform the PJ.10-W2-Sol.96 Solution TS/IRS Part I.

2 Introduction

2.1 Background

PJ.10-W2-Sol.96 AG starts taking into account the work performed by S2020 SOL16-04 Wave 1 project. PJ.10-W2-Sol.96 AG's starting maturity level is TRL4 and it targets to reach TRL6 maturity at the end of Wave 2 activities.

During PJ16.04 Attention Guidance (AG) activity fulfilled in achieving a better understanding of the phenomenon "attention" and interdependencies with other cognitive processes which helps to better understand the mechanisms of attention guidance and consequently, to avoid pitfalls along the design of attention guidance assistance systems. It constitutes the basis for the envisioned attention guidance and adaptive automation concepts.

2.2 General Approach to Safety Assessment

According to SESAR Safety Reference Material [2], safety approach identifies three kind of solution types depending on its safety impact of the solution on ATS System (as presented in Figure 1). Each solution type: ATS Operational, Other than ATS operational solution or Technological solution demand specific safety approach. Considering the safety impact of PJ.10-W2-96 AG, 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. The design safety driver is the specification of the functionalities & performance characteristics derived from the (potential) operational usages envisaged for that technological solution limited to the potential safety implication on the side of the ATS service provider or aviation undertaking (e.g. airline) using that service.

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 PJ.10-W2-96 AG aims to achieve the TRL6 maturity level. Following SESAR SRM [2], a Technological Safety Plan (TSAP) as a part of TVALP and a Technological Safety Assessment Report (TSAR) as a part of TSIRS [4] shall be delivered. The safety outcomes are the (Final) Technical Safety requirements (TSRDs), with high fidelity evidence, providing input (besides TSAR) to Technical Specification (Section 4.2) and TVALR [3] (Section 4).

This SAR describes safety activities carried out for the following validation exercises:

- **EXE-PJ.10-96-AG-TRL6-01** (Skyguide/Skysoft-ATM) – A real time simulation which evaluated the determination of the KPI values; it will address the use of fade out algorithm to reduce the workload and improve ATCO's situation awareness.

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-Sol-96
- 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.

3 Setting the Scene of the Safety Assessment

This section provides the main informations collected within SAF&HP Scoping and Change assessement and Safety Assessment Plan development processess.

3.1 Concept overview and scope of the change

The PJ.10-W2-96 Attention Guidance deals with new methods of controller interaction with Human Machine Interface (HMI), implementing a fade-out algorithm in a very high complexity environment. The fade-out algorithm supports the ATCO by putting the “largely non-conflictual” flights in “fade-out” status which means they are displayed in a way it does not attract the user’s attention. Implementing a fade-out algorithm allows the ATCO to visualize the flights for which attention is required and a manual input may be necessary.

The aim of the application is to release ATCOs from the monitoring and the scanning of “largely non-conflictual” flights and to increase the ability to focus on relevant flights by reducing the amount of information to analyse on HMI.

For more details refer to TS/IRS Part I [4].

3.2 Stakeholders’ expected benefits with potential Safety impact

Figure 1 BIM ATCOs

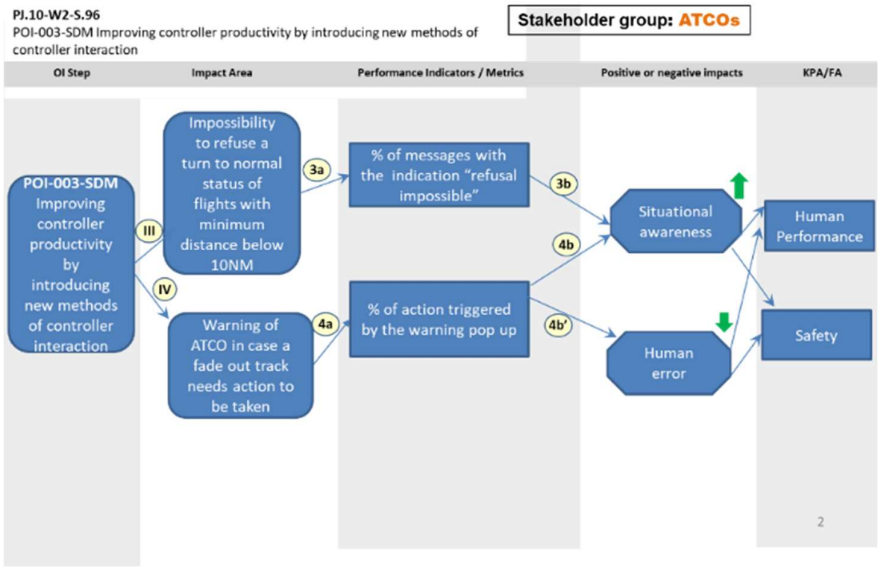

Figure 2 BIM ATCOs

3.3 Intended Operational use of the Technological Concept

3.3.1 Intended use identified from SESAR Operational Solutions

The Attention Guidance function is intended for area controllers in very high complexity environment above FL355.

Currently, there is no SESAR operational solution for which the Attention Guidance technology, as covered by the PJ10-W2-96 Technological solution, is an enabler. Therefore, its intended use within SESAR is limited to the use cases identified in the scope of the solution:

Name	Description
UC-10-96-TRL6-TS-101	Guiding the ATCO's attention on relevant air traffic *Flights that are largely non-conflictual are put in "fade-out" status. Supporting the controller in maintaining timely the relevant flights to scan in normal display and fading-out the others leads to increase the ability to focus on relevant flights and may at the end increase efficiency and safety as well as reduce workload*
UC-10-96-TRL6-TS-102	ATCO's input triggering the fade out algorithm Flights that are largely non-conflictual are put in "fade-out" status. If the ATCO performs an input on the flight, the fade out algorithm is processed.

Name	Description
UC-10-96-TRL6-TS-103	Acknowledgement of a flight in “intermediate fade-out” status A flight in “intermediate fade-out” status is acknowledged by the ATCO to keep the situation awareness
UC-10-96-TRL6-TS-104	Flight turning to “intermediate normal display” status When in “fade-out” status, the flight turns to “intermediate normal display” status if the minimum lateral distance is strictly lower than 18 NM with another track during 3 track updates.
UC-10-96-TRL6-TS-105	Acknowledgement of a flight in “intermediate normal display” status A flight in “intermediate normal display” status is acknowledged by the ATCO to keep the situation awareness
UC-10-96-TRL6-TS-106	Refusal of a flight in “intermediate normal display” status. When in “intermediate normal display” status, a manual refusal is performed by the ATCO to turn the flight in “normal display” status if the minimum distance is higher than 10 NM.
UC-10-96-TRL6-TS-107	Impossibility to refuse a flight in “intermediate normal display” status. When in “intermediate normal display” status and a manual refusal is performed by the ATCO, an indication is displayed to inform of the impossibility to refuse the flight if the minimum lateral distance is below 10 NM.
UC-10-96-TRL6-TS-108	Warn ATCO in case the Top of Descent is reached. In case a flight is in fade-out status, the system raises an alert when the Top of descent is reached (TOD1 or TOD2).
UC-10-96-TRL6-TS-109	Warn ATCO in case the flight is at a certain distance from the XPT In case a flight is in fade-out status, the system raises an alert when the track is at a certain distance from the XPT.
UC-10-96-TRL6-TS-110	Warn ATCO in case an exit conflict is raised In case a flight is in fade-out status, the system raises an alert if two flights exit the centre at the same point, the same level and more or less the same time.
UC-10-96-TRL6-TS-111	Warn ATCO in case an electronic coordination is received and does not trigger a conflict

Name	Description
	In case a flight is in fade-out status, the system raises an alert when an electronic coordination is received and does not trigger a conflict
UC-10-96-TRL6-TS-112	Warn ATCO in case an electronic coordination is received and triggers a conflict In case a flight is in fade-out status, the system raises an alert when an electronic coordination is received and triggers a conflict. The flight is displayed in “normal display” status and flashes.
UC-10-96-TRL6-TS-113	Warn ATCO in case the system raises a RAM alert In case the flight is in fade-out status, the system raises a RAM alert when the flight does not follow its route. The flight turns to “normal display” status and flashes.
UC-10-96-TRL6-TS-114	Warn ATCO in case the system raises a CLAM alert In case the flight is in fade-out status, the system raises a CLAM alert when the flight does not follow the CFL. The flight turns to “normal display” status and flashes.
UC-10-96-TRL6-TS-115	Warn ATCO in case the system raises an EHS CLAM alert In case the flight is in fade-out status, the system raises an EHS CLAM alert when the ATCO does not follow the selected altitude of the flight. The flight turns to “normal display” status and flashes.
UC-10-96-TRL6-TS-116	Warn ATCO in case the SSR code is set to 7500, 7600 or 7700 In case the flight is in fade-out status, the system raises an alert when the SSR code of the flight is set to 7500, 7600 or 7700. The flight turns to “normal display” status and flashes.
UC-10-96-TRL6-TS-117	Warn ATCO in case of emergency alarm In case the flight is in fade-out status, the system raises an alert when the flight is in emergency. The flight turns to “normal display” status and flashes.
UC-10-96-TRL6-TS-118	Warn the ATCO in case of conflict when changing a level In case of a level change on a non-fade-out flight, the system shall warn the user on levels potentially in conflict with fade-out flights.

Table 1 PJ10-W2-96 Use cases

3.3.2 Other intended use outside SESAR

No additional applications were identified.

3.4 Relevant applicable standards

No applicable standards related to the Technological Solution.

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 PJ10-W2-96 TS/IRS based on the use cases for normal operations:

TSSR	Mapping to Use Cases
TSSR_10.96_001 The solution shall enable the safe and timely provision of air traffic management.	UC-10-96-TRL6-TS-101; UC-10-96-TRL6-TS-102; UC-10-96-TRL6-TS-103; UC-10-96-TRL6-TS-106; UC-10-96-TRL6-TS-108; UC-10-96-TRL6-TS-109; UC-10-96-TRL6-TS-111;
TSSR_10.96_002 The solution shall ensure that a potentially safety critical event is detected by ATCo in a timely manner in order to take appropriate action.	UC-10-96-TRL6-TS-104; UC-10-96-TRL6-TS-105; UC-10-96-TRL6-TS-107; UC-10-96-TRL6-TS-110; UC-10-96-TRL6-TS-112; UC-10-96-TRL6-TS-113; UC-10-96-TRL6-TS-114; UC-10-96-TRL6-TS-115; UC-10-96-TRL6-TS-116; UC-10-96-TRL6-TS-117; UC-10-96-TRL6-TS-118

Table 2 TSSRs for normal operations

The following abnormal conditions were identified as relevant for PJ10-W2-96:

Abnormal condition	Effect	TSSR

ABN 001	Emergency situation when STCA triggered	When STCA is triggered (for aircraft in fade out) ATCO may not be aware of the conflicting aircraft which can result in loss of separation.	**TSSR_10.96_002** The solution shall ensure that a potentially safety critical event is detected by ATCo in a timely manner in order to take appropriate action.
ABN 002	Aircraft SSR code set to 7500, 7600 or 7700	When SSR code set to 7500, 7600 or 7700 (by aircraft in fade out) ATCO may not be aware of the aircraft in emergency and will not be able to safely handle it.	**TSSR_10.96_002** The solution shall ensure that a potentially safety critical event is detected by ATCo in a timely manner in order to take appropriate action.
ABN 003	CLAM or EHS CLAM is triggered	When CLAM or EHS CLAM is triggered (by aircraft in fade out) ATCO may not be aware of the aircraft deviating from its Cleared Flight level by a value greater than a threshold.	**TSSR_10.96_002** The solution shall ensure that a potentially safety critical event is detected by ATCo in a timely manner in order to take appropriate action.
ABN 004	RAM alert is triggered	When RAM is triggered (by aircraft in fade out) ATCO may not be aware of the aircraft deviating from its planned heading	**TSSR_10.96_002** The solution shall ensure that a potentially safety critical event is detected by ATCo in a timely manner in order to take appropriate action.
ABN 005	Adverse weather	Adverse weather usually avoided by aircraft and restructure the traffic which is complex to handle.	**TSSR_10.96_002** The solution shall ensure that a potentially safety critical event is detected by ATCo in a timely manner in order to take appropriate action.

Table 3 Abnormal conditions

4.2.2 TSSR from other intended use

Not applicable.

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

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

Hz ID	Description	Operational effects	TSSR for failure	Severi
HZ 01	Total loss of attention guidance	No AG measures are initiated due to AG failure. Aircraft in fade-out are already under ATCO responsibility. The only change is the status from fade-out to normal status. Operation immediately changes back to conventional which may cause a momentary disruption of ATCo task execution and slight increase in workload.	-	No im safety
HZ 02	Partial loss of attention guidance	AG measures are not initiated due to AG failure. Aircraft in fade-out are already under ATCO responsibility. The only change is the status from fade-out to normal status. Operation immediately changes back to conventional which may cause a momentary disruption of ATCo task execution and slight increase in workload.	-	No im safety
HZ 03	Corruption of attention guidance	Potentially resulting in a delayed or missed action by the ATCo. Safety impact may be mitigated by other existing (non- AG) system functionalities but may cause a momentary disruption of ATCo task execution. Safety impact may be more significant than in Hz#01 and 02 due to there being an expectation by the ATCo that AG is available to assist in task execution.	**TSSR_10.96_003** The likelihood of corruption of Attention Guidance shall be no more than 4E-07 per flight hour.	Severi

Table 4 Functional hazards

TSSR_10.96_003 safety requirement at service level is calculated based on SRM using the Severity: MAC-SC3 related values of:

Maximum Tolerable Frequency of Occurrence: **MTFoO [per fh]=1e-4**

Overall number of operational hazards for a given severity class: **N=25**

Impact Modification factor: **IM=10**

4.3.2 TSSR from other intended use

Not applicable.

4.4 Process assurance of the Technical Safety Specification

The safety assessment was conducted according to SRM 0. 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 (**Error! Reference source not found.**) with the participation of PJ10-W2-96 solution partners including air traffic controllers, concept designers, ATM engineers, human factors and safety experts.

Safety assessment activity	Scope	Deliverable receiving the outcome
HP&SAF Scoping & Change Assessment session	Definition safety strategy Safety planning	Safety Plan
Safety Metrics and Indicators session	Identification of applicable metrics and indicators to be applied in the exercises for safety evidence	Safety Plan
HAZID workshop	Hazard identification Safety System Requirements	Initial SAR, Interim TS/IRS

Table 5 Safety assurance activity

5 Safe Design of the Technical System

The purpose of this section is to document the Technical Safety Requirements at Design level (TSRDs) for the PJ10-W2-96 Technological Solution.

The TSRDs are design characteristics of the technical system which ensure that the system operates as specified and is able to achieve the Design Safety Drivers of the technological solution.

The safety assurance activities feeding this section has been conducted at refined design level in TRL6 and result in the set of the rTSRD – Technical Safety Requirements at Refined Design level.

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 from the TSSRs (functionality and performance) of section 4.2, and supported by the analysis of the initial or refined design model - section 5.3
- assessment of the adequacy of the design (initial or refined) in the case of internal failures and mitigation of the Solution 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

Design Model of the Solution is presented via EATMA models in Appendix B by Figure 2-5.

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

The purpose of this section is to derive Safety Requirements at Design level (TSRD) in normal and abnormal conditions of operations The TSRDs (functionality and performance) are derived from the TSSRs (functionality and performance) which have been identified in sub-section 4.2 of this template.

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

Table 6 contains the consolidated list of Technical Safety Requirements at Design level (functionality and performance) for Normal and Abnormal conditions of operations mapping to the Technical Specification Safety Requirements (TSSRs) documented in section 4.2.

Technical Safety Requirement ID [Design Model element]	Technical Safety Requirement description (functionality & performance)	Derived from TSSR (ID)
REQ-PJ.10-TS-AG01.0001	The system shall not introduce additional delay in the workflow of the operator (controller).	**TSSR_10.96_001**
REQ-PJ.10-TS-AG01.0002	The system shall provide a high level of usability, i.e. support ATCOs to reach their task goals efficiently and to appropriate user acceptance levels.	**TSSR_10.96_001**
REQ-PJ.10-TS-AG01.0003	The system shall at least support controllers to maintain an acceptable level of situational awareness.	**TSSR_10.96_001; TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0004	The system should reduce the workload of the controller.	**TSSR_10.96_001**
REQ-PJ.10-TS-AG01.0005	The system shall provide an intelligent fade out algorithm in order to reduce the number of displayed flights (in normal status display colour) at each moment. A flight can be faded out if and only if the flight is largely non-conflictual	**TSSR_10.96_001; TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0033	A flight shall be considered as largely non-conflictual if the minimum lateral distance is above 20NM from the other flights or the vertical profile is not intercepting the other flights.	**TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0008	The system shall recalculate the fade out algorithm upon a controller input that implies a change in the profile (level (CFL, XFL, EFL), direct or heading, speed).	**TSSR_10.96_001; TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0009	If a flight is largely non-conflictual, the system shall turn it into an “intermediate fade-out” status.	**TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0010	The system shall provide a facility to display a flight in an “intermediate fade-out” status. In this case, the callsign and a one-minute speed vector of the flight will be displayed in “fade-out” colour. The other elements of the flight remain in “normal” colour.	**TSSR_10.96_001;**
REQ-PJ.10-TS-AG01.0011	The system shall provide a facility to manually acknowledge a flight in “intermediate fade-out” status. Once acknowledged, the flight turns to fade out colour.	**TSSR_10.96_001;**

REQ-PJ.10-TS-AG01.0014	When in “fade-out” status, the system shall turn a flight into an “intermediate normal display” status if the minimum lateral distance becomes strictly below 18NM during 3 track updates.	**TSSR_10.96_001; TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0015	The system shall provide a facility to display a flight in an “intermediate normal display” status. In this case, the call sign, and the one-minute speed vector will be displayed in “normal display” colour. The other elements of the flight will remain in “fade out” colour.	**TSSR_10.96_001;**
REQ-PJ.10-TS-AG01.0016	The system shall provide a facility to manually acknowledge a flight in “intermediate normal display” status. All the elements of the flight will turn to “normal display” colour and the one-minute speed vector won’t be displayed any longer	**TSSR_10.96_001;**
REQ-PJ.10-TS-AG01.0018	The system shall prevent the user from refusing a flight in “intermediate normal display” status when the minimum lateral distance between two flight’s profiles is below 10 NM considering the uncertainty. In this case, a “PLTCA”” indication on the flight will be displayed in “warning display” colour to warn the user.	**TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0019	The system shall provide a facility to flash a flight in “intermediate normal display” status when not manually acknowledged by the user after one minute. The callsign and the one-minute speed vector will flash.	**TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0020	The system shall provide a facility to acknowledge a flight in “intermediate normal display” status when flashing. The flight will turn into “normal display” colour.	**TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0024	If the flight is in “fade-out” status, the system shall warn the user when the flight is at a warning distance from the XPT. In this case, the call sign of flight will be displayed in white colour. Moreover the frequency of the flight will be forced to display in warning colour.	**TSSR_10.96_001;**

REQ-PJ.10-TS-AG01.0034	If the flight is in “fade-out” status, the system shall warn the user when the flight exits the centre at the same point, the same level and more or less the same time. In this case, the call sign of flight will be displayed in white colour. Moreover the XFL of the flight will be forced to display in warning colour.	**TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0025	If the flight is in “fade-out” status, the system shall warn the user when there is a CLAM or EHS CLAM alert. In this case, the call sign of the flight will be displayed in white colour and the CFL will be displayed in warning colour.	**TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0026	If the flight is in “fade-out” status, the system shall warn the user when there is a RAM alert (Route Adherence Monitoring). In this case, the call sign of the flight will be displayed in white colour. Moreover the heading of the flight will be displayed in warning colour.	**TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0027	If a flight is in “fade-out” status and an emergency situation occurs (STCA, SSR code set to 7500, 7600 or 7700), the system shall turn all the elements of the flight in “normal display” colour and flash the flight.	**TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0028	If a flight is in “fade-out” status and an emergency situation occurs, the system shall allow the user to turn all the elements of the flight in “normal display” colour to make a change in the route or the diversion for instance. In this case, the track will flash. Once the change is performed, the system shall newly process the algorithm.	**TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0029	In case the flight is flashing, the system will allow the user to acknowledge the flash in order to stop it.	**TSSR_10.96_001;**
REQ-PJ.10-TS-AG01.0030	The system shall provide a facility to enable/disable the fade-out algorithm per CWP.	**TSSR_10.96_001;** **TSSR_10.96_002**
REQ-PJ.10-TS-AG01.0031	If the flight is in “fade-out” status and an electronic coordination is received without triggering any conflict, the system shall warn the user. In this case, the call sign of the flight will be	**TSSR_10.96_001;**

	displayed in white colour and the coordination in blue colour.	
REQ-PJ.10-TS-AG01.0032	If the flight is in "fade-out" status and an electronic coordination is received triggering a conflict, the system shall warn the user. In this case, the call sign of the flight will be displayed in white colour and the coordination in blue colour. Moreover, an indication on the flight will be displayed to indicate that the received coordination triggers a conflict.	**TSSR_10.96_002;**
REQ-PJ.10-TS-AG01.0034	When changing the level of a non-fade-out flight, the system shall provide a facility to indicate the levels potentially in conflict with fade-out flights.	**TSSR_10.96_001; TSSR_10.96_002;**

Table 6: TSRD (functionality and performance) satisfying TSSRs for Normal and 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

The purpose of this section is toSafety Requirements at Design level (TSRDs) addressing

TSRDs are derived from the TSSRs (integrity/reliability) and TSSR (functionality &performance) which have been identified when addressing failure conditions in the technical safety specification.

5.4.1 Technical Safety Requirements at design level addressing internal system failures

Technical Safety Requirement ID	Technical Safety Requirement description (integrity/ reliability)	Derived from TSSR integrity/reliability (ID)
REQ-PJ.10-TS-AG01.0035	The likelihood of an aircraft incorrectly stays in "fade-out" status shall be operationally acceptable as per regulation applicable to local implementation.	**SRS 003** The likelihood of corruption of Attention Guidance shall be no more than 4E-07 per flight hour.
REQ-PJ.10-TS-AG01.0036	The likelihood of ATCO is incorrectly able to change an aircraft status to fade-out shall be operationally acceptable as per regulation applicable to local implementation.	
REQ-PJ.10-TS-AG01.0037	The likelihood of an aircraft's status changes to "fade-out" without ATCO approval shall be operationally	

	acceptable as per regulation applicable to local implementation.	
REQ-PJ.10-TS-AG01.0038	The likelihood of ATCO is unable to change aircraft status to normal shall be operationally acceptable as per regulation applicable to local implementation.	
REQ-PJ.10-TS-AG01.0039	The likelihood of RAM/ CLAM/ TOD/ Emergency detection failure in case of aircraft in fade-out shall be operationally acceptable as per regulation applicable to local implementation.	

Table 7. TSRD (integrity/ reliability) to mitigate functionality hazards

Table 8 provides the consolidated list of Technical Safety Requirements at Design level (functionality and performance) addressing internal system failures. Include the following:

Technical Safety Requirement ID	Technical Safety Requirement description (functionality & performance)	Derived from TSSR (ID)
REQ-PJ.10-TS-AG01.0040	The Controller shall be informed about the status of the AG and be alerted in case of a failure.	**TSSR 004** The solution shall enable the safe and timely provision of air traffic management in degraded mode of AG.
REQ-PJ.10-TS-AG01.0041	In case of system failure all aircraft shall be displayed in normal status.	
TSRD 001	ATCO shall be able to prevent overload and manage workload by reducing capacity in case of AG failure.	
TSRD 002	Contingency procedures shall be in place in case of AG malfunction.	
TSRD 003	ATCO training shall include contingency procedures in case of AG malfunction.	
REQ-PJ.10-TS-AG01.0030	The system shall provide a facility to enable/disable the fade-out algorithm per CWP.	

Table 8. Additional TSRDs (functionality & performance) to mitigate functionality hazards

5.5 Realism and testability of the Safe Design

The refined technical safety requirements at the design level (rTSRD) derived in this assessment target mainly two domains: equipment and human factors.

Equipment related Safety Requirements, including functionality and system performance, are provided in qualitative manner for success approach or quantified for failure approach.

Human factors' related Safety Requirements were derived through assessment done jointly by Human performance, safety and in cooperation with controllers participating in validation exercises, therefore are considered fully achievable.

Therefore, rTSRD defined in this SAR are considered achievable.

5.6 Process assurance of the Safe Design

The safety assessment was conducted according to SRM 0. In order to identify refined set of Technical Safety Requirements at Design Level (rTSRD) a dedicated workshop with subject matters experts was conducted addressing both success approach (defining at the level of each component what it is required to fulfil in terms of functionality and performance) and failure approach (defining at the level of each component what it is required to fulfil in terms of integrity and additional functionalities).

The following safety activities were performed (Table 9**Error! Reference source not found.**) with the participation of PJ10-W2-96 solution partners including air traffic controllers, concept designers, ATM engineers, human factors, and safety experts.

Safety assessment activity	Scope	Deliverable receiving the outcome
Refined Technical Safety Requirements at Design Level (TSRD) validation workshop	Technical Safety Design Requirements validation (mitigation efficiency & realism)	SAR Final TS/IRS

Table 9 Safety activities performed in PJ10-W2-96-AG

6 Demonstration of achievability of the Technical System Safety Specification

Achievability of the TSSRs has been demonstrated through the safety validation objectives defined for Solution PJ10-W2-96 and validated during exercises and additional specific safety assessment activities. (i.e. data analysis, Safety and HP workshops).

Chapter 4.2.3 in the TVALR [3] presents the results coming from the validation exercises.

7 Acronyms and Terminology

Term	Definition
ABN	Abnormal
ADD	Architecture Description Document
AG	Attention Guidance
AOR	Area of Responsibility
ATCO	Air Traffic Controller Operator
ATM	Air Traffic Management
CC	Capability Configuration
CLAM	Cleared Level Alert Monitoring
EATMA	European ATM Architecture
E-ATMS	European Air Traffic Management System
EFL	Entry Flight Level
EHS CLAM	Enhanced Cleared Level Alert Monitoring
ER	En-Route
FAA	Federal Aviation Administration
HAZID	Hazard Identification
HMI	Human Machine Interface
HZ	Hazard
HP	Human Performance
IER	Information Exchange Requirement
INTEROP	Interoperability Requirements
IRS	Interface Requirements Specification
ISRM	Information Services Reference Model
NAF	NATO Architecture Framework
NSOV	NAF Service Oriented View
NOV	NAF Operational View

NSV	NAF System View
OSED	Operational Service and Environment Definition
QoS	Quality of Service
RAM	Route Adherence Monitoring
rTSRD	refined Technical Specification Safety Requirements
SAF	Safety
SAR	Safety Assessment Report
SDD	Service Description Document
SESAR	Single European Sky ATM Research Programme
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SoaML	Service Oriented Architecture Modelling Language
SPR	Safety and Performance Requirements
SWIM	System Wide Information Model
TOD	Top of Descent
TRL	Technology Readiness Level
TS	Technical Specification
TSAP	Technological Safety Plan
TSSR	Technical Specification Safety Requirements
TSRD	Technical Safety Requirements at Design Level
TVALR	Technical Validation Report
UML	Unified Modelling Language
V&V	Validation and Verification
WSDL	Web Services Definition Language
XFL	Exit Flight Level
XSD	XML Schema Definition

Table 10: Acronyms

8 References

Safety

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

[2] SESAR Safety Reference Material

[3] SESAR Solution 96 AG TVALR

[4] PJ.10-W2-96 AG TS/IRS Part I

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 Table 11.

Hz ID	Hazard	Impact	TSSR
Hz-1	System parameters are not suitable in every circumstance	The specified system parameters will not be able to suit efficiently all the circumstances related to different sector configurations. Due to inadequate minimums: • relevant aircrafts might be in „fade-out" status, decreasing the situational awareness of the ATCO • the status of some aircrafts might change frequently, increasing the workload of the ATCO • the vast majority of aircrafts might be in „normal" status, decreasing the efficiency of the system (a situation with limited safety impact)	**TSSR_10.96_001** The solution shall enable the safe and timely provision of air traffic management. **TSSR_10.96_002** The solution shall ensure that a potentially safety critical event is detected by ATCo in a timely manner in order to take appropriate action.
Hz-2	The system is not able to handle very high traffic complexity scenarios	In case of very high complexity traffic (e.g. 80-90% of the capacity, severe weather conditions – thunderstorm activity) using the system might increase workload.	**TSSR_10.96_001** The solution shall enable the safe and timely provision of air traffic management.
Hz-3	The system is not able to handle	Identification of an aircraft declared emergency in „fade out" status might cause difficulties. If the pilot does not indicate	**TSSR_10.96_002** The solution shall ensure that a potentially safety critical event is detected by ATCo

	emergency scenarios	squawk 7700 (entirely or on time), feasibility of system alert is limited.	in a timely manner in order to take appropriate action.
Hz-4	The system is not able to handle abnormal scenarios	Identification of an aircraft deviating from its trajectory (including lateral and vertical deviation) in „fade out" status might cause difficulties.	**TSSR_10.96_002** The solution shall ensure that a potentially safety critical event is detected by ATCo in a timely manner in order to take appropriate action.
Hz-5	The system is not able to handle normal scenarios	ATCOs' SA is decreased due to the aircrafts in „fade-out" status. • Identification of an aircraft closing to its exit point in „fade out" status might cause difficulties. • Identification of an aircraft closing to its TOD point in „fade out" status might cause difficulties. • Identification of an aircraft calling the ATCO in „fade out" status might cause difficulties. • The aircrafts changing from „fade-out" to „normal" status can cause surprise to ATCOs. • Aircrafts in „fade-out" status can be mistaken with other sectors' traffic (displayed in grey).	**TSSR_10.96_001** The solution shall enable the safe and timely provision of air traffic management. **TSSR_10.96_002** The solution shall ensure that a potentially safety critical event is detected by ATCo in a timely manner in order to take appropriate action.
Hz-6	Using the new system increases ATCO's workload.	By adding approval of status change as a new task to ATCO, workload can be higher.	**TSSR_10.96_001** The solution shall enable the safe and timely provision of air traffic management.

Table 11 TSSR derived for normal conditions

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 static analysis of the functional system behaviour.

A.2 Define TSSRs addressing failure conditions

A.2.1 FHA Workshop

Hz ID	Use case	Example of causes & preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Functional hazard; Severity
HZ 01	AG functions are not available for all aircraft.	AG failure	No AG measures are initiated due to AG failure. Aircraft in fade-out are already under ATCO responsibility. The only thing that changes is the status from fade-out to normal status. Operation immediately changes back to conventional which may cause a momentary disruption of ATCo task execution and slight increase in workload.	**SRD candidate:** In case of system failure all aircraft shall be displayed in normal status.	Total loss of attention guidance Severity: **No immediate safety effect**

Hz ID	Use case	Example of causes & preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Functional hazard; Severity
HZ 02	Some AG functions are not available, or AG functions are not available for every aircraft.	AG failure	AG measures are not initiated due to AG failure. Aircraft in fade-out are already under ATCO responsibility. The only thing that changes is the status from fade-out to normal status. Operation immediately changes back to conventional which may cause a momentary disruption of ATCo task execution and slight increase in workload.	**SRD candidate:** In case of system failure all aircraft shall be displayed in normal status. **REQ-PJ.10-TS-AG01.0030** The system shall provide a facility to enable/disable the fade-out algorithm per CWP.	Partial loss of attention guidance Severity: **No immediate safety effect**
HZ 03	An aircraft incorrectly stays in "fade-out" status OR ATCO is incorrectly able to change an aircraft status to fade-out	AG malfunction	ATCo is in the belief that aircraft in fade-out status is largely non-conflictual. In case such a malfunction ATCo will .not be aware of a conflict in time. It will potentially result in a delayed or missed action by the ATCo. Safety impact may be mitigated by other existing (non- AG) system functionalities but may cause a momentary disruption of ATCo task execution. Safety impact may be more significant than in Hz#01 and 02 due to there being an expectation by the	(ATCO detection is highly unlikely.) **REQ-PJ.10-TS-AG01.0030** The system shall provide a facility to enable/disable the fade-out algorithm per CWP.	Corruption of Attention Guidance Severity: **MAC-SC3**

Hz ID	Use case	Example of causes & preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Functional hazard; Severity
			ATCo that AG is available to assist in task execution.		
	An aircraft's status changes to "fade-out" without ATCO approval	AG malfunction	ATCO may not be aware of status changes which degrades their situational awareness.	**REQ-PJ.10-TS-AG01.0030** The system shall provide a facility to enable/disable the fade-out algorithm per CWP.	
	ATCO is unable to change aircraft status to normal	AG malfunction	Potentially resulting in a delayed or missed action by the ATCo. Safety impact may be mitigated by other existing (non- AG) system functionalities but may cause a momentary disruption of ATCo task execution.	**REQ-PJ.10-TS-AG01.0030** The system shall provide a facility to enable/disable the fade-out algorithm per CWP.	
	An aircraft's status incorrectly stays in normal	AG malfunction	More aircraft are in normal status than should be. **No safety effect foreseen.**	**REQ-PJ.10-TS-AG01.0030** The system shall provide a facility to enable/disable the fade-out algorithm per CWP. (ATCO detection is highly unlikely.)	
	An aircraft's status changes to normal without ATCO approval	AG malfunction	More aircraft are in normal status than should be. **No safety effect foreseen.**	**REQ-PJ.10-TS-AG01.0030**	

Hz ID	Use case	Example of causes & preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Functional hazard; Severity
				The system shall provide a facility to enable/disable the fade-out algorithm per CWP.	
	RAM/CLAM/TOD/Emergency detection failure in case of aircraft in fade-out	AG malfunction	Aircraft in emergency stays in fade-out which does not support ATCO in detection. Potentially resulting in a delayed or missed action by the ATCo. Safety impact may be mitigated by other existing (non- AG) system functionalities but may cause a momentary disruption of ATCo task execution.	**REQ-PJ.10-TS-AG01.0030** The system shall provide a facility to enable/disable the fade-out algorithm per CWP.	

Table 12. FHA working table

A.2.2 FHA Participation List

The FHA session took place at 2022.10.28 via online platform.

Company	Title
HungaroControl	Safety expert
HungaroControl	Air traffic controller
Skyguide	Air traffic controller
Skyguide	Technical expert
NATS	Human Factors expert

Table13 FHA participants

Insert project logo here

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

B.1 Deriving TSRDs from TSSRs

The following diagrams (Figure 3-6) presents the modelling of Use cases 101-107 identified in the scope of the solution.

[NSV-4][UC-101-102-103] Guiding ATCO's attention on relevant air traffic; acknoledgement of a flight in intermediate fade-out status

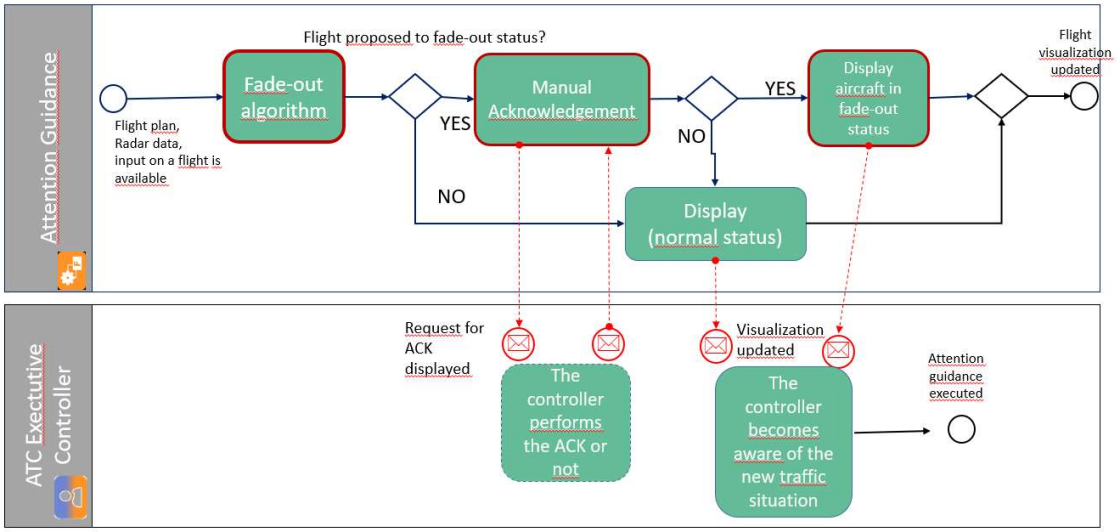

Figure 3 NSV-4 for Use case 101-102-103

[NSV-4][UC-104-105-106-107] Flight turning to intermediate normal display status; Acknoledgement/refusal of a flight in intermediate normal display status.

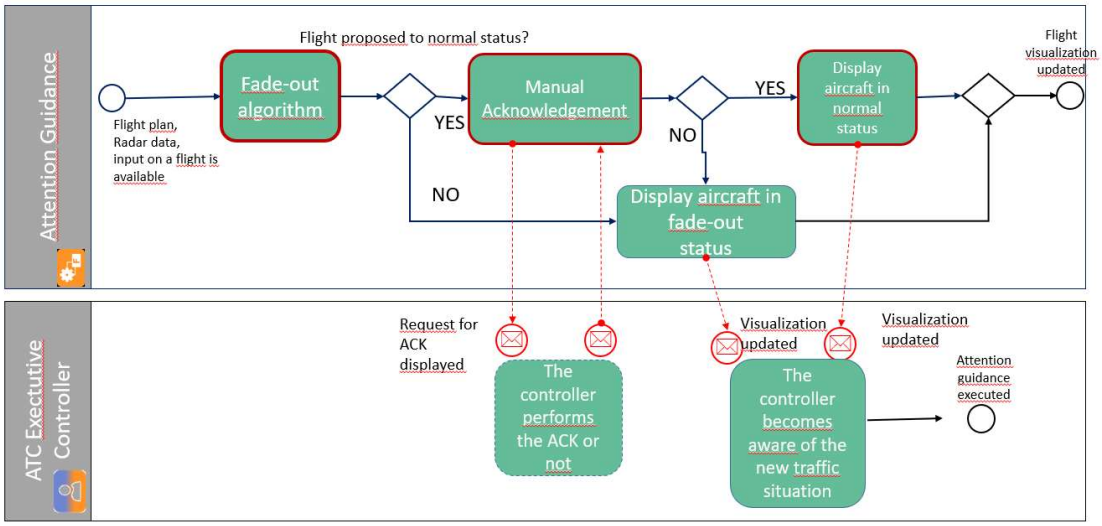

Figure 4 NSV-4 for Use case 104-105-106-107

[NSV-4][UC-106] Light warnings on fade out flights

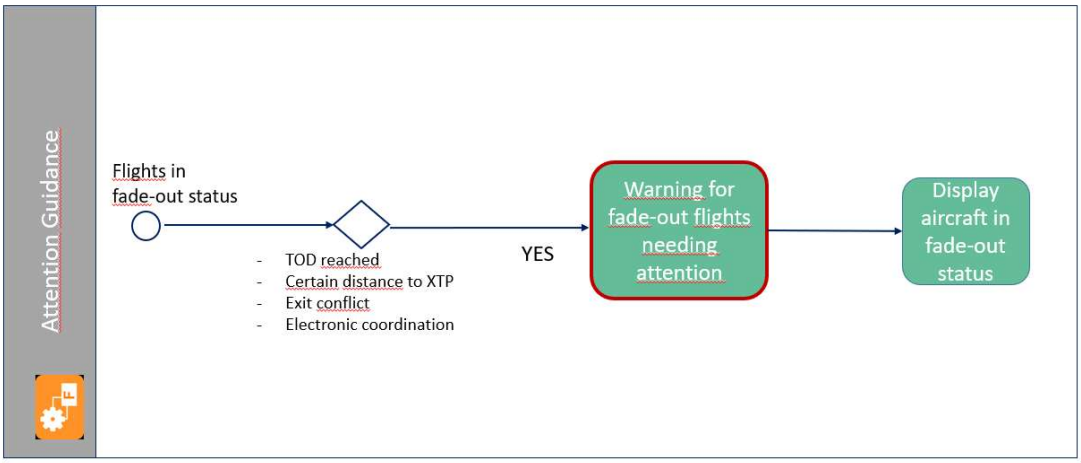

Figure 5 NSV-4 for Use case 106

[NSV-4][UC-107] Strong warnings on fade out flights

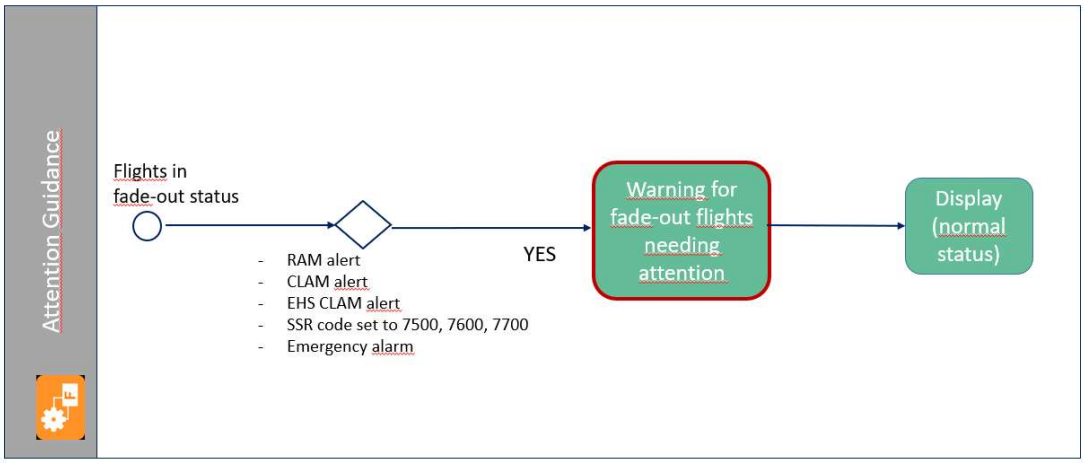

Figure 6 NSV-4 for Use case 107

TSSR for Normal & Abnormal Operation (ID & content)	Technical Safety Requirement at Design level[1] (TSRD) or Assumption	Maps onto
TSSR_10.96_001 The solution shall enable the safe and timely provision of air traffic management.	**REQ-PJ.10-TS-AG01.0001** The system shall not introduce additional delay in the workflow of the operator (controller). **REQ-PJ.10-TS-AG01.0002** The system shall provide a high level of usability, i.e. support ATCOs to reach their task goals efficiently and to appropriate user acceptance levels. **REQ-PJ.10-TS-AG01.0003** The system shall at least support controllers to maintain an acceptable level of situational awareness. **REQ-PJ.10-TS-AG01.0004** The system should reduce the workload of the controller. **REQ-PJ.10-TS-AG01.0005** The system shall provide an intelligent fade out algorithm in order to reduce the number of displayed flights (in normal status display colour) at each moment. A flight can be faded out if and only if the flight is largely non conflictual. **REQ-PJ.10-TS-AG01.0008** The system shall recalculate the fade out algorithm upon a controller input that implies a change in the profile (level (CFL, XFL, EFL), direct or heading, speed). **REQ-PJ.10-TS-AG01.0010** The system shall provide a facility to display a flight in an “intermediate fade-out” status. In this case, the leader line and a one minute speed vector of the flight will be displayed in “fade-out” colour. The other elements of the flight remains in “normal” colour.	Use Case 101; 102; 103; 104; 105; 106; 107

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

	REQ-PJ.10-TS-AG01.0011 The system shall provide a facility to manually acknowledge a flight in "intermediate fade-out" status. Once acknowledged, the flight turns to fade out colour. **REQ-PJ.10-TS-AG01.0014** When in "fade-out" status, the system shall turn a flight candidate to "normal display" into an "intermediate normal display" status if the minimum lateral distance becomes strictly below 18NM during 3 track updates. **REQ-PJ.10-TS-AG01.0015** The system shall provide a facility to display a flight in an "intermediate normal display" status. In this case, the call sign, and the one minute speed vector will be displayed in "normal display" colour. The other elements of the flight will remain in "fade out" colour. **REQ-PJ.10-TS-AG01.0016** The system shall provide a facility to manually acknowledge a flight in "intermediate normal display" status. All the elements of the flight will turn to "normal display" colour and the one minute speed vector won't be displayed any longer. **REQ-PJ.10-TS-AG01.0029** In case the flight is flashing, the system will allow the user to acknowledge the flash in order to stop it. REQ-PJ.10-TS-AG01.0030 The system shall provide a facility to enable/disable the fade-out algorithm per CWP. **REQ-PJ.10-TS-AG01.0031** If the flight is in "fade-out" status and an electronic coordination is received without triggering any conflict, the system shall warn the user. In this case, the call sign of the flight will be displayed in white colour and the coordination in blue colour. **REQ-PJ.10-TS-AG01.0032** When changing the level of a non-fade-out flight, the system shall	

	provide a facility to indicate the levels potentially in conflict with fade-out flights.	
TSSR_10.96_002 The solution shall ensure that a potentially safety critical event is detected by ATCo in a timely manner in order to take appropriate action.	**REQ-PJ.10-TS-AG01.0003** The system shall at least support controllers to maintain an acceptable level of situational awareness. **REQ-PJ.10-TS-AG01.0005** The system shall provide an intelligent fade out algorithm in order to reduce the number of displayed flights (in normal status display colour) at each moment. A flight can be faded out if and only if the flight is largely non conflictual. **REQ-PJ.10-TS-AG01.00033** A flight shall be considered as largely non conflictual if the minimum lateral distance is above 20NM from the other flights or the vertical profile is not intercepting the other flights. **REQ-PJ.10-TS-AG01.0008** The system shall recalculate the fade out algorithm upon a controller input that implies a change in the profile (level (CFL, XFL, EFL), direct or heading, speed). **REQ-PJ.10-TS-AG01.0009** If a flight is largely non conflictual, the system shall turn it into an “intermediate fade-out” status. **REQ-PJ.10-TS-AG01.0014** When in “fade-out” status, the system shall turn a flight candidate to “normal display” into an “intermediate normal display” status if the minimum lateral distance becomes strictly below 18NM during 3 track updates. **REQ-PJ.10-TS-AG01.0018** The system shall prevent the user from refusing a flight in “intermediate normal display” status when the minimum lateral distance between two flight’s profiles is below 10 NM considering the uncertainty. In this case, a “PLTCA” indication on the flight will be displayed in “warning display” colour to warn the user.	Use Case 101; 102; 103; 104; 105; 106; 107

	REQ-PJ.10-TS-AG01.0019 The system shall provide a facility to flash a flight in “intermediate normal display” status when not manually acknowledged by the user after one minute. The callsign and the one minute speed vector will flash. **REQ-PJ.10-TS-AG01.0020** The system shall provide a facility to acknowledge a flight in “intermediate normal display” status when flashing. The flight will turn into “normal display” colour. **REQ-PJ.10-TS-AG01.0024** If the flight is in “fade-out” status, the system shall warn the user when the flight exits the centre at the same point, the same level and more or less the same time. In this case, the call sign of flight will be displayed in white colour. Moreover the XFL of the flight will be forced to display in warning colour. **REQ-PJ.10-TS-AG01.0025** If the flight is in “fade-out” status, the system shall warn the user when there is a CLAM or EHS CLAM alert. In this case, the call sign of the flight will be displayed in white colour and the CFL will be displayed in warning colour. **REQ-PJ.10-TS-AG01.0026** If the flight is in “fade-out” status, the system shall warn the user when there is a RAM alert (Route Adherence Monitoring). In this case, the call sign of the flight will be displayed in white colour. Moreover the heading of the flight will be displayed in warning colour. **REQ-PJ.10-TS-AG01.0027** If a flight is in “fade-out” status and an emergency situation occurs (STCA, SSR code set to 7500, 7600 or 7700), the system shall turn all the elements of the flight in “normal display” colour and flash the flight. **REQ-PJ.10-TS-AG01.0028** If a flight is in “fade-out” status and an emergency situation occurs, the	

	system shall allow the user to turn all the elements of the flight in "normal display" colour to make a change in the route or the diversion for instance. In this case, the track will flash. Once the change is performed, the system shall newly process the algorithm. **REQ-PJ.10-TS-AG01.0030** The system shall provide a facility to enable/disable the fade-out algorithm per CWP. **REQ-PJ.10-TS-AG01.0032** When changing the level of a non-fade-out flight, the system shall provide a facility to indicate the levels potentially in conflict with fade-out flights.	

Table 14: TSRDs derived by mapping TSSRs for normal and abnormal conditions of operation to Design Model Elements

B.2 Static analysis of the technical system

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

B.3 Dynamic analysis of the technical system

Table 14 contains the link between the hazards identified in the Scoping and change assessment (Appendix A.1) and the Validation objectives of the Real time simulation. (The results are presented in SESAR Solution 96 AG TVALR [3].)

All identified Hazards are addressed by TSRDs via TSSRs (presented in Appendix A1) and no additional TSRDs were defined.

Hz ID	Hazard	Impact	VAL OBJ
Hz-1	System parameters are not suitable in every circumstance	The specified system parameters will not be able to suit efficiently all the circumstances related to different sector configurations. Due to inadequate minimums: • relevant aircrafts might be in „fade-out" status, decreasing the situational awareness of the ATCO • the status of some aircrafts might change frequently, increasing the workload of the ATCO • the vast majority of aircrafts might be in „normal" status, decreasing the efficiency of the system (a situation with limited safety impact)	OBJ-10.96AG-TRL6-TVALP-S01 Assess Controllers acceptance of the logic behind AG function in normal situations
Hz-2	The system is not able to handle very high traffic complexity scenarios	In case of very high complexity traffic (e.g. 80-90% of the capacity, severe weather conditions – thunderstorm activity) using the system might increase workload.	OBJ-10.96AG-TRL6-TVALP-S07 Assess Controllers Workload when providing ATS with AG function
Hz-3	The system is not able to handle emergency scenarios	Identification of an aircraft declared emergency in „fade out" status might cause difficulties. If the pilot does not indicate squawk 7700 (entirely or on time), feasibility of system alert is limited.	OBJ-10.96AG-TRL6-TVALP-S05 Assess Controllers acceptance of alarms and alerts when providing ATS with AG function in abnormal situations
Hz-4	The system is not able to handle abnormal scenarios	Identification of an aircraft deviating from its trajectory (including lateral and vertical deviation) in „fade out" status might cause difficulties.	OBJ-10.96AG-TRL6-TVALP-S05 Assess Controllers acceptance of alarms and alerts when providing ATS with AG function in abnormal situations
Hz-5	The system is not able to handle normal scenarios	ATCOs' SA is decreased due to the aircrafts in „fade-out" status. Identification of an aircraft closing to its exit point in „fade out" status might cause difficulties.	OBJ-10.96AG-TRL6-TVALP-S06 Assess Controllers Situational awareness when providing ATS with AG function

		Identification of an aircraft closing to its TOD point in „fade out" status might cause difficulties. Identification of an aircraft calling the ATCO in „fade out" status might cause difficulties. The aircrafts changing from „fade-out" to „normal" status can cause surprise to ATCOs. Aircrafts in „fade-out" status can be mistaken with other sectors' traffic (displayed in grey).	
Hz-6	Using the new system increases ATCO's workload.	By adding approval of status change as a new task to ATCO, workload can be higher.	OBJ-10.96AG-TRL6-TVALP-S02 Assess Controllers acceptance of changing to fade-out status when providing ATS with AG function. OBJ-10.96AG-TRL6-TVALP-S03 Assess Controllers acceptance of changing to normal status when providing ATS with AG function.

Table 15 Hazards validated during real-time simulation

.

Appendix C Designing the technical system for addressing Internal System Failures

This appendix presents the detailed risk evaluation and mitigation of the functionality hazards identified at Section 4.3, performed at the level of the technical system design.

C.1 Deriving TSRD from TSSR (integrity/reliability)

Hz ID	Description	Operational effects	TSSR for failure	TSRD for failure
HZ 03	Corruption of Attention Guidance Severity: MAC-SC3 MTFoO= 1e-4 N=25 IM=10	ATCO may not be able to detect a conflict Loss of ATCO situational awareness	**SRS 003** The likelihood of corruption of Attention Guidance shall be no more than 4E-07 per flight hour.	**REQ-PJ.10-TS-AG01.0035** The likelihood of an aircraft incorrectly stays in "fade-out" status shall be operationally acceptable as per regulation applicable to local implementation. **REQ-PJ.10-TS-AG01.0036** The likelihood of ATCO is incorrectly able to change an aircraft status to fade-out shall be operationally acceptable as per regulation applicable to local implementation. **REQ-PJ.10-TS-AG01.0037** The likelihood of an aircraft's status changes to "fade-out" without ATCO approval shall be operationally acceptable as per regulation applicable to local implementation. **REQ-PJ.10-TS-AG01.0038** The likelihood of ATCO is unable to change aircraft status to normal shall be operationally acceptable as per regulation applicable to local implementation. **REQ-PJ.10-TS-AG01.0039** The likelihood of RAM/ CLAM/ TOD/ Emergency detection failure in case of aircraft in fade-out shall be operationally acceptable as per regulation applicable to local implementation.

Table 16 TSRDs for failure

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

The purpose is to derive TSRD (functionality & performance) from the SRS (functionality & performance) that have been derived in §4.4.2 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.

Table 17 shows the Safety Requirements at ATS Service level (SRS) functionality & performance derived in section 4.4.2 for protective mitigation and derive additional Safety Requirements at Design level (SRD) (functionality and performance) for internal failure conditions of operation.

SRS (functionality & performance) for protective mitigation (ID & content)	Safety Requirement at Design level[2] (SRD) or Assumption
SRS 004 The solution shall enable the safe and timely provision of air traffic management in degraded mode of AG.	**REQ-PJ.10-TS-AG01.0040** The Controller shall be informed about the status of the AG and be alerted in case of a failure.
	REQ-PJ.10-TS-AG01.0041 In case of system failure all aircraft shall be displayed in normal status.
	TSRD 001 ATCO shall be able to prevent overload and manage workload by reducing capacity in case of AG failure.
	TSRD 002 Contingency procedures shall be in place in case of AG malfunction.
	TSRD 003 ATCO training shall include contingency procedures in case of AG malfunction.
	REQ-PJ.10-TS-AG01.0030 The system shall provide a facility to enable/disable the fade-out algorithm per CWP.

Table 17 Safety Requirements at Design level

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

Appendix D Assumptions, Safety Issues & Limitations

D.1 Assumptions log

No assumptions were identified during the assessment process.

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

Insert project logo here

-END OF DOCUMENT-

Insert project logo here

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