

D4.1.020 PJ10-W2-96 ASR TS/IRS for TRL6 - Part II - Safety Assessment Report

Deliverable ID:	D4.1.020
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:	22 March 2023
Edition:	01.00.00
Template Edition:	00.00.04

Authoring & Approval

Authors of the document

Beneficiary	Date
INTEGRA	22/12/2021

Reviewers internal to the project

Beneficiary	Date
ANS CR	17/02/2023
CRIDA	20/02/2023
INDRA	13/02/2023
ENAIRE	20/02/2023
DLR (AT-One)	16/02/2023
NATMIG/SINTEF	20/02/2023
LEONARDO	20/02/2023
COOPANS	

Reviewers external to the project

Beneficiary	Date

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

Beneficiary	Date
ANS CR	28/02/2023
CRIDA	Silent approval
INDRA	28/02/2023
ENAIRE	28/02/2023
DLR (AT-One)	Silent approval
NATMIG/SINTEF	Silent approval
LEONARDO	28/02/2023
COOPANS	Silent approval

Rejected By - Representatives of beneficiaries involved in the project

Beneficiary	Date
-------------	------

Document History

Edition	Date	Status	Beneficiary	Justification
00.00.01	22/12/2021	Initial	Integra	New Document
00.00.02	15/12/2022	Intermediate	Integra	Input from exercises
00.00.03	10/02/2023	Final draft	Integra	For review
00.01.00	23/02/2023	Revised Draft	Integra	Sent out for approvals
00.01.01	28/02/2023	Final	INTEGRA	Final version for submission to the SJU
01.00.00	22/03/2023	Approved	SJU	The deliverable has been approved by the SJU

Copyright Statement © 2023 – INDRA, LEONARDO, DLR (AT-One), ENAIRE, NLR, SINTEF, ANS CR (B4), ACG/COOPANS, CCL/COOPANS. All rights reserved. Licensed to SESAR3 Joint Undertaking under conditions.

PJ 10-W2- PROSA

SEPARATION MANAGEMENT AND CONTROLLER TOOLS

This Safety Assessment Report is part of a project that has received funding from the SESAR 3 Joint Undertaking under grant agreement No 874464 under European Union's Horizon 2020 research and innovation programme.



Abstract

This is a final Safety Assessment Report for SESAR Solution PJ.10-W2-96 Automatic Speech recognition - HMI Interaction modes for ATC Centre.

It provides Technical Safety Specification of the solutions addressing the Technical Specification Safety Requirements (TSSRs). These requirements specify the functionalities & performance characteristics derived from the operational uses envisaged for the technological solutions. It also addresses Technical Safety Requirements at Design level (TSRDs) as 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 solutions.

Table of Contents

Abstract	4
1 Executive Summary.....	8
2 Introduction.....	9
2.1 Background	9
2.2 General Approach to Safety Assessment	10
2.3 Scope of the Safety Assessment	10
2.4 Layout of the Document	10
3 Setting the Scene of the Safety Assessment	11
3.1 Concept overview and scope of the change	11
3.2 Stakeholders' expected benefits with potential Safety impact	11
3.3 Intended Operational use of the Technological Concept	12
3.4 Relevant applicable standards	14
4 Technical Safety Specification.....	15
4.1 Overview of activities performed	15
4.2 Technical Specification Safety Requirements – TSSR (functionality and performance)...	15
4.3 Technical Specification Safety Requirements - TSSR (integrity /reliability)	17
4.4 Process assurance of the Technical Safety Specification	20
5 Safe Design of the Technical System	21
5.1 Overview of activities performed	21
5.2 Design Model of the Solution Technical System	21
5.3 Deriving Technical Safety Requirements at Design level for Normal and Abnormal conditions	22
5.4 Technical Safety Requirements at design level addressing Internal System Failures	24
5.5 Realism and testability of the Safe Design	26
5.6 Process assurance of the Safe Design	27
6 Demonstration of achievability of the Technical System Safety Specification	27
7 Acronyms and Terminology.....	32
8 References	35
Appendix A Defining the Technical Safety Specification based on other intended use. 36	
A.1 Define TSSRs for Normal and Abnormal conditions.....	36
A.2 Define TSSRs addressing failure conditions.....	37

Appendix B	<i>Designing the Solution technical system for normal and abnormal conditions</i>	45
B.1	Deriving TSRDs from TSSRs	45
B.2	Static analysis of the technical system.....	47
B.3	Dynamic analysis of the technical system	47
Appendix C	<i>Designing the technical system for addressing Internal System Failures...</i>	49
C.1	Deriving TSRD from TSSR (integrity/reliability)	49
C.2	Deriving TSRD from the TSSR (functionality&performance) for protective mitigation	54
Appendix D	<i>Assumptions, Safety Issues & Limitations</i>	57
D.1	Assumptions log	57
D.2	Safety Issues log	57
D.3	Operational Limitations log.....	57

List of Tables

Table 1 Use Cases applicable to the PJ10-W2-96 ASR	14
Table 2: TSRD (functionality and performance) satisfying TSSRs for Normal and Abnormal conditions	23
Table 3: Additional TSRDs derived from static and dynamic analysis of the technical system behaviour (normal and abnormal conditions of operation)	24
Table 4. Additional TSRDs (functionality & performance) to mitigate functionality hazards.....	26
Table 5. TSRD (integrity/ reliability) to mitigate functionality hazards.....	26
Table 6: Acronyms.....	33
Table 7: Glossary of terms.....	34
Table 8. FHA working table	Error! Bookmark not defined.
Table 9: TSRDs derived by mapping TSSRs for normal and abnormal conditions of operation to Design Model Elements	47
Table 10. Example of table detailing the fault tree causes and associated preventive mitigations (TSRD)	52
Table 11. Example of FMEA (Failure Modes and Effects Analysis) table	54
Table 12: TSRDs derived by mapping TSSRs for Protective mitigation of functionality hazard to Design Model Elements	56
Table 13: Assumptions log	57
Table 14: Safety Issues log.....	Error! Bookmark not defined.

Table 15: Operational Limitations log Error! Bookmark not defined.

List of Figures

Figure 1: [TBD] Solution Technical System Design Model.....Error! Bookmark not defined.

1 Executive Summary

This document contains the Specimen Safety Assessment for a typical application of the PJ10-W2-96 Technological Solution. The Safety Assessment Report (SAR) represents Part II of the TS/IRS document and presents the assurance that the Safety Requirements for the TRL2-TRL6 phases are complete, correct, and realistic, thereby providing all material to adequately inform the PJ10-W2-96 Solution TS/IRS Part I.

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

It addresses the following activities:

- The derivation of the Technical Specification Safety Requirements - TSSRs (functionality and performance) in normal and abnormal conditions
- The derivation of the Technical Specification Safety Requirements - TSSRs (integrity/reliability) to address functionality failures
- Process assurance of the Technical Safety Specification
- The derivation of Technical Safety Requirements (functionality & performance) at Design level (TSRD) in normal and abnormal conditions of operation from the TSSRs (functionality and performance), and supported by the analysis of the initial or refined design model
- The assessment of the adequacy of the design (initial or refined) in the case of internal failures and mitigation of the PJ10-W2-96 ASR solution functionality hazards through derivation from TSSRs (integrity/reliability) of Technical Safety Requirements (functionality & performance) and Technical Safety Requirements (integrity/reliability) at Design level (TSRD).

2 ¹Introduction

The safety assessment is conducted in line with SESAR Safety Reference Material [3] focusing on Guidance O mainly) and in accordance with [1].

2.1 Background

The PJ10-W2-96 Technological Solution addresses the Automatic Speech Recognition (ASR) technology validated within SESAR context in the SESAR2020 PJ.16-04 Wave 1 project. SESAR 2020 Wave 1 PJ.16-04 project investigated new methods of controller interaction with the Human Machine Interface (HMI) at the Controller Working Position (CWP). The solution developed guidance and assessment methods regarding HMI, investigated new HMI needs and interaction modes in relation with SESAR solutions (including new user interface technologies such as speech recognition, multi-touch, and gaze detection). PJ16-04 main focus was En-Route and, Approach environments.

PJ10-W2-96 ASR Solution also benefits from the experience in a number of other projects on Automatic Speech Recognition in ATC. The first assistant-based speech recognition system (ABSR) for an ATC approach area has been built in the project AcListant[®] with laboratory speech data of ATCos and validated for aircraft radar label maintenance task in the project AcListant[®]-Strips. However, the development of this first ABSR system based on expert knowledge and adapting it to different environments manually would have been costly. Thus, the idea of the following SESAR Exploratory Research project MALORCA [9] for other ATC approach areas with ops room data from ATCos was to automatically learn the needed models, i.e., acoustic model, language model, command prediction model, etc. MALORCA [9] project focused on the Automatic Speech Recognition, with the aim to significantly reduce controller's workload and increase ATM efficiency. The results demonstrated a command recognition rates between 90% and 95 between 90% and 95% (error rate between 2% and 5%) with assistant-based speech recognition (i.e. an AMAN dynamically generates context information to increase the recognition rate). Without context generation the recognition rate was only between 50% and 80%. Besides, the speech recognition was deemed as the more reliable input sensor, at least in the simulation setup.

The following, currently running, SESAR2020 Exploratory Research project HAAWAI focusses also on the en-route area and additionally considers pilot utterances. HAAWAI aims to develop machine learning based applications for readback error detection and ATCo workload estimation. The German national funded ASR project STARFiSH concentrates on recognition of ATCo utterances on ground and considers a specific airport layout. The currently running SESAR2020 Industrial Research project PJ.05-97.2 aims to develop an ASR system for a tower environment to reach TRL4 maturity at the end of Wave 2 activities. During all those ASR projects an initial ontology for the annotation of ATC commands has been defined, later coordinated and agreed between major European ATM stakeholders and is still further enhanced.

¹ The opinions expressed herein reflect the author's view only. Under no circumstances shall the SESAR3 Joint Undertaking be responsible for any use that may be made of the information contained herein.

2.2 General Approach to Safety Assessment

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

Considering the safety impact of the solutions PJ.10-W2-96 ‘HMI Interaction modes for ATC Centre’ is considered as technological solutions.

The application of the technological solution safety strategy is motivated by the fact that the PJ.10-W2-96 ASR is exclusively concerning the system components offering new interaction modes with existing technologies, proving the same information to air traffic controllers.

2.3 Scope of the Safety Assessment

The scope of technological safety assessment is equivalent to the scope of the PJ.10-W2-96 ASR solution: therefore, it covers the operational environment conditions, OI steps/Enablers, Use Cases and Scenarios (in the Solution scope as per the TS/IRS) which will be covered by solution validation exercises.

The PJ.10-W2-96 ASR solution aims to achieve the TRL6 maturity by the end of Wave 2 activities. Following SESAR Safety Reference Materials, the safety assessment will deliver safe initial design (mainly by defining functionality, performance and integrity/reliability Technical Safety Requirements at design level (ITSRD) that will be documented as appropriate in the TS/IRS Part I).

Since the properties of the context in which the Technological Solution is to be used is crucial to the safety assessment, this assessment cannot be considered as generic but specific to the context of use defined in section 3.2 and consequently, the term ‘specimen’ safety assessment will be used.

2.4 Layout of the Document

This safety report consists of the following sections

- Section 1 - presenting the Executive summary;
- Section 2 - presenting the Scope and approach to safety assessment from safety perspective;
- Section 3 - describing the scene of the Safety Assessment;
- Section 4 - describing the Technical Safety Specifications;
- Section 5 - describing Safe Design of the Technical System;
- Section 6 - demonstration of achievability of the Technical System Safety Specification;
- Section 7 - presenting Acronyms;
- Section 8 - presenting References and applicable documents.

3 Setting the Scene of the Safety Assessment

3.1 Concept overview and scope of the change

ASR in ATM domain matured in Wave 1 up to TRL-4 and enabled the definition of rules for transformation of a sequence of ATC words into ATC concepts (so called ontology). This ontology will be developed further and prepared for standardization. In Wave 2 ASR will operate also on real life data and the objective is to reach TRL-6.

Two main functional blocks are within the scope of solution PJ.10-W2-96 ASR:

- Automatic Speech Recognition, performing recognition functions.
- Controller Human Machine Interaction Management ER/APP, displaying recognised commands and adjusting display following ASR inputs.

The role considered to be within the scope of the solution is ATC Executive Controller, mainly benefiting from Automatic Speech Recognition. As input comes from the ATCO-pilot spoken dialog, ASR is the appropriate technology to reduce ATCO's workload by directly filling the command masks and radar labels using the spoken commands instead of manually inputting them into the system. This requires integration of artificial intelligence (AI) and machine learning algorithms. Highlighting of targets, user-friendly and intuitive operation will increase controller productivity.

The solution operates in a medium TMA and En-Route environment and ATCOs are the end users. HMI prototypes will be developed in order to present the results of the speech recognition (highlighting of targets, user-friendly and intuitive operation etc.) in the best way to the controllers.

ASR in the ATC environment can still be enhanced. The solution aims to a commands recognition rate better than 85%, which is quite ambitious. Therefore, comparison algorithms will be developed avoiding that wrong recognitions are missed by the controller and used by subsequent systems. This requires integration of artificial intelligence (AI) and machine learning algorithms for the intelligent data provision to the controllers. In addition, the solution will also investigate how ASR may be used to enable faster and more predictable navigation in 3D visualizations of the air space sectorisation when using dynamic air space configuration (DAC). One of the challenges that will be addressed is how to combine using speech to communicate with pilots and other ATCOs with using speech to control the 3D navigation.

The improvements in the HMI interaction modes and technologies aim to minimise the workload of the TMA and En-Route Controllers and may be applicable in current operations and/or in future operational concepts still under development and scope of other SESAR Solutions.

Solution 96 ASR deals with both the current operating TMA and En-Route environment and future environments and is aligned to the current evolution happening within the SESAR 2020 Programme.

3.2 Stakeholders' expected benefits with potential Safety impact

The application of ASR technology will directly impact controllers' performance by automatically filling in the command masks and radar labels from the spoken commands instead of controller manually inputting them into the system.

As input comes from the ATCO-pilot spoken dialog, ASR is the appropriate technology to reduce ATCO's workload.

A high percentage of callsigns correctly identified from pilot's utterance will increase the controller's situational awareness and decrease potential for human error and consequently have a positive impact on safety. Situational awareness will increase especially when the flight crew performs the first contact as it confirms to the controller the callsign from the aircraft contacting or performing the readback.

A high number of controller's commands correctly identified will reduce controllers' workload and also potential for human error by implementing them automatically into the system without a need for manual input by the controller. In addition, ASR will allow to the controller to check the last commands as they will be provided in the historical annotation of the commands. This will have a positive impact on human performance and subsequently on safety as well.

3.3 Intended Operational use of the Technological Concept

3.3.1 Intended use identified from SESAR Operational Solutions

Besides its application in the En-Route and TMA environment, the application of the Automatic Speech Recognition in the tower environment is also addressed within the scope of the SESAR by the PJ05-W2-97.2 Technological solution. Furthermore, potential usage of the ASR commands to trigger visualisation of sectorisation is envisaged within the operational solution PJ.09-W2-44 'Dynamic Airspace Configuration (DAC). Namely, the ASR would recognize voice commands related to an upcoming sectorization change and flights that would be affected by this change and highlight these changes in the CWP. Further to this, it would support the navigating of the 3D visualization of the air space in the CWP through voice commands recognition.

The main use of the ASR is described in the Use cases identified within the solution PJ.10-W2-96 listed in the table below (more details on each of the Use Cases can be found in the section 3.1.1.2 of the TS/IRS Part I):

Use Case	Use Case Title	Description
#3.1	Highlight of callsigns on the CWP from pilot utterances.	This use of the ASR technology will increase controller's situational awareness and reduce their workload, by quickly identifying new flights entering the sector or flight crews requesting actions from ATCos (e.g. trajectory change, flight level change or information)
#3.2	Highlight of callsigns on the CWP from controllers utterances.	The illumination of the callsign coming from a controller utterance provides a safety check to the controller that will be able to detect if there is a difference between the callsign mentioned and the flight in the CWP where the command is being introduced.
#3.3	Annotation of controllers commands.	A historical annotation of the provided commands will be available to the controller for consultation. This will, at the same time, increase controllers' situational

Use Case	Use Case Title	Description
		awareness and provide a safety check as they will be able to check the instructions given to the flights. This UC is an intermediate step before the semi-automatic/automatic input of commands in the CWP using ASR.
#3.4	Pre-filling of commands in the CWP	In this use case ATCOs will be presented with the recognized (and validated) command types together with the command values in the CWP. ATCOs will then be able to accept/reject or correct the commands.
#3.5	Voice commands for highlighting an upcoming sectorization change in the CWP	When using dynamic airspace configuration (DAC), it is important for the ATCOs to understand the upcoming changes (both horizontally and vertically) in the airspace configuration, both in the sector being controlled by an ATCO, and to the neighbouring sectors. This use case will provide special voice commands for the ATCOs to investigate such changes before they occur.
#3.6	Voice commands for highlighting the flights that will be affected by an upcoming sectorization change in the CWP	When using dynamic airspace configuration (DAC), it is important for the ATCOs to understand how the current traffic is affected by the sector changes, particularly flights that need to be handed over to a different sector as a consequence of the sector changes. This use case will provide special voice commands for the ATCOs to highlight affected flights before and just after a sectorization change.
#3.7	Voice commands for navigating the 3D visualization of the air space in the CWP	One of the tools provided in the CWP to increase the ATCOs understanding of changes in the airspace configuration is a 3D visualization of the air space. This use case will provide special voice commands for navigating the 3D visualization and for highlighting certain parts of it.
#3.8	Prefilling of Datalink commands	After the Logon and Connecting procedure have been fulfilled, ATCOs will utter the datalink commands and the CWP will prefill the command values to be

Use Case	Use Case Title	Description
		accepted/rejected or corrected by the ATCOs.

Table 1 Use Cases applicable to the PJ10-W2-96 ASR

3.3.2 Other intended use outside SESAR

The STARFiSH² (Safety and Artificial Intelligence Speech Recognition) project integrates the AI-based speech recognition ABSR into an A-SMGCS monitoring system for ground traffic at Fraport AG. A joint application of ABSR and A-SMGCS recognizes the instructions given by air traffic controllers to pilots, extracts the commands (semantics) contained therein and integrates the results into the user interface of the A-SMGCS. An additional safety net for AI applications is intended to ensure that errors in AI-based speech recognition cannot have any negative effects on the overall system.

The application developed in STARFiSH is prototypically integrated into the simulation environment of Fraport AG. The data for training the AI-based components of the project are also recorded here as part of several simulations and supplemented by recordings from real operation from Frankfurt.

The automatic speech recognition has been also investigated on the airborne side. The Voice Crew Interaction (VOICI)³ project under Clean Sky 2 has aimed to develop an intelligent "natural crew assistant" in a cockpit environment. The system comprises three main technologies, namely sound recording, speech recognition and artificial intelligence (AI). This includes a cockpit-embedded speech-processing system that understands aviation terminology, as well as an array of low-noise optical microphones and optimised array processing for it. The VOICI system also features a new and more efficient speech synthesis, adapted to aviation terminology and noise levels.

3.4 Relevant applicable standards

EUROCAE ED-137B (Interoperability Standards for VoIP ATM Components) has been identified as the applicable standard for VoIP communications in ATC environments. Therefore, the integration of the ASR system in the ATS architecture, at least regarding VoiceFlow forwarding from VCS to ASR, should comply with this standard to assure interoperability with Voice Communication Systems.

Chapter 12 in ICAO Doc 4444 refers to Phraseology. Communication procedures and standard phraseology are detailed in this document.

² See also homepage https://www.dlr.de/fl/en/desktopdefault.aspx/tabid-1149/1737_read-74905/

³ See also homepage <https://www.sintef.no/projectweb/voici/>

4 Technical Safety Specification

The purpose of this section is to document the Technical Specification Safety Requirements for the PJ10-W2-96 ASR Technological Solution.

The Technical Specification Safety Requirements (TSSRs) specify 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 ATS service provider, other than ATS service provider or aviation undertaking (e.g. airline) using those functionalities.

4.1 Overview of activities performed

This section presents the Technical Specification Safety Requirements (TSSRs) that are derived from the intended use identified in section 3.3.

The Technical Safety Specification are expressed in terms of the data and functionalities provided according to required properties such as: type, scope / applicability, format, interface protocols, accuracy, resolution, latency / refresh rate, integrity, etc. These properties are to be defined by the intended users based on the corresponding operational uses as identified in section 3.3.

Safety assurance activities, presented in this section are in line with PJ10-W2-96 ASR Safety Assessment Plan section 5. The activities were derived from Guidance A.2 and Guidance O of the Safety Reference Material as relevant for TRL6.

This section addresses the following activities:

- Review and analysis of the functional architecture description to ensure completeness of technical system description (based on the NSV-4 models)
- Walkthrough with SMEs using Sequence diagrams based on use cases
- Hazard identification session Walkthrough with SMEs
- 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 section lists the Technical Safety Requirements (TSSR) related to the Technological concept

ID	Description	Use Case
----	-------------	----------

TSSR-96-01	A callsign recognised by ASR from pilot's utterance shall be highlighted in the CWP HMI.	UC 1
TSSR-96-02	A callsign recognised by ASR from ATCO's utterance shall be highlighted in the CWP HMI.	UC 2 UC 3 UC 4 UC 8
TSSR-96-03	A callsign recognised by ASR from ATCO's utterance shall be displayed on CWP HMI in the form of a historical annotation.	UC 3
TSSR-96-04	The controller's utterance shall be transformed into a sequence of ATC commands.	UC 2 UC 3 UC 4 UC 8
TSSR-96-05	A command recognized as part of an ATCO's utterance shall be displayed in the CWP HMI.	UC 3 UC 4 UC 8
TSSR-96-06	The command recognized and displayed by ASR shall be accepted if correct, automatically by the system or manually by the controller.	UC 4 UC 8
TSSR-96-07	If a command recognised by ASR is identified as incorrect by the controller, he/she shall be able to correct it.	UC 4 UC 8
TSSR-96-08	ATCO shall be able to reject the command incorrectly identified by ASR and displayed.	UC 4 UC 8
TSSR-96-09	A sector recognised by ASR from ATCO's utterance shall be highlighted in the CWP HMI.	UC 5
TSSR-96-10	An upcoming layout of sectors recognised by ASR from ATCO's utterance shall be highlighted in the CWP HMI.	UC 5 UC 7
TSSR-96-11	The relevant flights shall be highlighted in the CWP HMI from ATCO's utterance to highlight the flights affected by the upcoming sectorization change.	UC 6
TSSR-96-12	ATCO shall be able to navigate 3D visualization of the airspace.	UC 7

Table 2 Technical Safety Requirements derived from solution operational use

Table 3 presents the Technical Safety Requirements derived for abnormal conditions.

ID	Abnormal condition	Effect	TSSR for abnormal conditions
TSSR-96-13	Adverse weather, emergency	In case the severe event occurs, the less frequent phraseology,	ASR shall be able to process the ATCO utterances containing less frequent phraseology / way points

		and/or unusual (less-frequent) waypoints could be used.	with the same level of performance as for normal operations.
--	--	---	--

Table 3 Technical Safety Requirements derived for abnormal conditions.

4.2.2 TSSR from other intended use

N/A

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

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

The Functional hazard analysis was conducted in order to prepare the technical design analysis with respect to internal system failure conditions in Section 5.4, one Functionality Hazard is defined in relation to each identified TSSR integrity/reliability.

Functionality hazard	Operational effect	TSSR for Failure	Severity
FHz#01 Significant delay in ASR command recognition and/or display.	If the use of ASR introduces delays in the usage of speech information (display of inputs, identification of aircraft, etc.) this may cause the ATCo to focus on specific flight/area of the AoR until they can verify that the action induced by ASR has been correctly processed and displayed. This may have negative impact on ATCo situational awareness.	TSSR-96-14 The time needed to display command recognized by ASR shall be optimised to support controller's task execution.	No safety impact
FHz#02 ASR fails to identify an aircraft from pilot's utterance – no aircraft is highlighted No safety issue	If pilot performs the radio call and the flight is not highlighted ATCo may have to scan the AoR to locate the aircraft. No difference to current operating method. However, if ASR functionality to highlight the callsign is defined in the new operating method, there is a default expectation by the ATCo that it is functional and assisting in locating aircraft, resulting in minor workload increase and situational awareness reduction.	TSSR-96-15 Required callsign recognition rate from pilot's utterance shall be set to a level appropriate for the application used and shall be high enough to ensure that occasional ASR errors do not disrupt ATCo task execution.	No safety impact
FHz#03 ASR fails to identify an aircraft from controller's	If ATCo performs the radio call it is assumed the impact is minor as the ATCo attention is focused on the aircraft being called and the impact is negligible.	TSSR-96-16 Required callsign recognition rate from ATCO's utterance shall be set to a level appropriate for the application	No safety impact

utterance— no aircraft is highlighted No safety issue		used and shall be high enough to ensure that occasional ASR errors do not disrupt ATCo task execution.	
FHz#04 ASR erroneously identifies an aircraft from pilot's utterance — wrong aircraft is highlighted No safety issue	If pilot performs the radio call and erroneous flight is highlighted, the ATCo may focus on the highlighted aircraft and issue the clearance intended for the calling aircraft to the wrong flight. The difference to current operating method is that while occasional callsign confusion may occur between similar callsigns, now the ASR system is enforcing the ATCos perception of issuing the clearance to what is expected to be the correct flight. If the confusion is not clarified through read-back and hear-back procedure or with the assistance of the planning controller, issued clearance to the wrongly highlighted aircraft may result in an unintended trajectory change. From safety perspective this is not significantly different from current operating method.	TSSR-96-17 Required callsign recognition error rate from pilot's utterance shall be set to a level appropriate for the application used and shall be low enough to ensure that occasional ASR errors do not disrupt ATCo task execution.	No safety impact
FHz#05 ASR erroneously identifies an aircraft from controller's utterance — wrong aircraft is highlighted	If ATCO performs the radio call and erroneous flight is highlighted, it is assumed the impact is minor as the ATCO's attention is on the aircraft being called and the impact of erroneous highlight is negligible.	TSSR-96-18 Required callsign recognition error rate from ATCO's utterance shall be set to a level appropriate for the application used and shall be low enough to ensure that occasional ASR errors do not disrupt ATCo task execution.	No safety impact
FHz#06 ASR fails to identify a command from controller's utterance.	The failure of ASR to identify a complete command forces ATCo to manually make the input. In such cases the negative impact on ATCo workload and situational awareness increases is expected, as in the new operating method there is a default expectation by the ATCo that ASR is functional and assisting in inputting commands in the labels.	TSSR-96-19 Required command recognition rate from ATCO's utterance shall be set to a level appropriate for the application used and shall be high enough to ensure that occasional ASR errors do not disrupt ATCo task execution.	No safety impact
FHz#07 ASR erroneously identifies a command from	In cases where inputs are provided but are erroneous the ATCo will have to recognize the error and change information already input into the system. Depending on the ATM-system, some parts of correcting the clearance, etc. route change, may require manipulation of the FPL route data to input the correction. In	TSSR-96-20 Required command recognition error rate from ATCO's utterance shall be set to a level appropriate for the application used and shall be low enough to ensure that	No safety impact

controller's utterance No safety issue	such cases the impact on ATCo workload and potential disruption to the ATCo workflow may be higher than in cases where only missing data needs to be input to complete the clearance.	occasional ASR errors do not disrupt ATCo task execution.	
FHz#08 ASR recognizes an incorrect callsign, and the command is displayed for the incorrect flight in the CWP HMI.	In cases where inputs are provided but are erroneous (i.e. command input for wrong aircraft), ATCo will have to recognize the error and change information already input into the system. If the error is not recognized by the controller, the contacted pilot will nevertheless follow the clearance issued by controller on the frequency. The erroneous input in the label of another aircraft will soon be detected by clearance monitoring aids (e.g. CLAM, RAM, MONA)	TSSR-96-18 Required callsign recognition error rate from ATCO's utterance shall be set to a level appropriate for the application used and shall be low enough to ensure that occasional ASR errors do not disrupt ATCo task execution.	No safety impact
FHz#09 ASR erroneously identifies the sector from controller's utterance – wrong sector/layout/ flights is/are highlighted	This may cause to controller to get an erroneous understanding of how the sector being controlled will change. The system highlights wrong set of flights based on wrongly recognised controller utterance resulting in erroneous understanding of which flights will be affected by the changes in the sector being controlled.	TSSR-96-20 Required command recognition error rate from ATCO's utterance shall be set to a level appropriate for the application used and shall be low enough to ensure that occasional ASR errors do not disrupt ATCo task execution.	No safety impact
FHz#10 ASR erroneously identifies the command for navigating the 3D visualization of the air space in the CWP.	In the new operating method there is a default expectation by the ATCo that ASR is functional and assisting in navigating the 3D visualization of the airspace, resulting in minor workload increase.	TSSR-96-20 Required command recognition error rate from ATCO's utterance shall be set to a level appropriate for the application used and shall be low enough to ensure that occasional ASR errors do not disrupt ATCo task execution.	No safety impact

Table 4

4.3.2 TSSR from other intended use

N/A

4.4 Process assurance of the Technical Safety Specification

The safety assessment was conducted according to SRM [3]. The Technical Safety Requirements were derived specifying the change in the operational services under normal, abnormal conditions and to mitigate functional I Hazards caused by failures internal to the ATM/ANS functional system & analyse associated mitigations such as to satisfy the Safety drivers.

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

The following safety activities were performed (table below with the participation of PJ10-W2-96 ASR solution partners including operational experts, concept developers, es ATM experts, human factors, and safety experts.

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

Table 8 Safety activities performed to derive TSSR.

5 Safe Design of the Technical System

This section provides the **Technical Safety Requirements at Design level (TSRDs)** for the PJ10-W2-96 ASR solution. The TSRDs are design characteristics/items 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.

TSRDs are mapped on the elements/components of the ASR system that are changed or affected by the change (through change in behaviour or through new interactions introduced).

The derived TSRDs are consistent with the set of requirements produced by the Solution team in charge of TS/IRS Part I.

5.1 Overview of activities performed

This section addresses the following activities:

- introduction of the design model (initial or refined) of the PJ10-W2-96 ASR 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 PJ10-W2-96 ASR 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

The Design Models used as a high-level architectural representation of the PJ10-W2-96 ASR solution systems design for the identification of the Technical Safety Requirements (functionality & performance) at Design level (TSRD) in normal and abnormal conditions of operation from the TSSRs (functionality and performance) are the NSV-4 diagrams produced by the project team Part I of TS/IRS:

- *[NSV-4] Display and highlight with Automatic Speech Recognition*
- *[NSV-4] Prefilling of commands with Automatic Speech Recognition*

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.

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

In Table 5 below, is provided the consolidated list of Technical Safety Requirements at Design level (functionality and performance) for Normal and Abnormal conditions of operations derived by mapping the Technical Specification Safety Requirements (TSSRs) documented in section 4.2 onto the related elements of the Design Model. For each TSRD is indicated the element of the design model (i.e. NSV-4 model) on which the TSRD is placed, as well as the associated TSSR. The requirements corresponding to the ones defined in the TS/IRS Part I are provided with the identical requirements identification as in TS/IRS Part I.

The detail of the derivation process is included in Appendix B.

Technical Safety Requirement ID [Design Model element]	Technical description (functionality & performance)	Safety Requirement (functionality & TSSR (ID))
REQ-10.96-01-TS-HMI.0010 <i>[NSV-4] Display and highlight with Automatic Speech Recognition</i> <i>Element: Controller HMI Management</i>	The HMI shall highlight the Track Label or part of it (or the track symbol) after recognizing the corresponding callsign.	TSSR-96-01 TSSR-96-02
REQ-10.96-01-TS-SF.0090 (New) <i>[NSV-4] Display and highlight with Automatic Speech Recognition</i> <i>[NSV-4] Prefilling of commands with Automatic Speech Recognition</i> <i>Element: Automatic Speech Recognition</i>	The voice flow (spoken words) shall be analysed and transformed into a text string.	TSSR-96-04
REQ-10.96-01-TS-SF.0100 (New) <i>[NSV-4] Display and highlight with Automatic Speech Recognition</i> <i>[NSV-4] Prefilling of commands with Automatic Speech Recognition</i> <i>Element: Automatic Speech Recognition</i>	The Apply Ontology and Logical Check function shall analyse the text string and transform it into the corresponding ATC concepts (following the Ontology) and perform a logical check to discard incoherent commands.	TSSR-96-04
REQ-10.96-01-TS-HMI.0020 <i>[NSV-4] Display and highlight with Automatic Speech Recognition</i>	The HMI shall present the recognized (and validated) command types together	TSSR-96-05

<i>[NSV-4] Prefilling of commands with Automatic Speech Recognition Element: Controller HMI Management</i>	with the command values in the radar label.	
REQ-10.96-01-TS-HMI.0030 <i>[NSV-4] Prefilling of commands with Automatic Speech Recognition Element: Manual acceptance: ATC Executive Controller Automatic acceptance: Automatic Speech Recognition</i>	The HMI shall enable acceptance of automatically inserted values by ATCo clicking on the value, by clicking on confirmation button in the dialogue line or by enabling automatic acceptance of recognized command values if the controller does not correct them within a predefined time frame (e.g. 10 seconds).	TSSR-96-06
REQ-10.96-01-TS-HMI.0040 <i>[NSV-4] Prefilling of commands with Automatic Speech Recognition Element: ATC Executive Controller</i>	The HMI shall enable manual correction/update of automatically proposed command value/type.	TSSR-96-07
REQ-10.96-01-TS-SF.0110 (New) <i>[NSV-4] Prefilling of commands with Automatic Speech Recognition Element: ATC Executive Controller</i>	The HMI associated with ASR shall enable the ATCo to reject recognized command values for pre-filling radar label values by clicking on a rejection button.	TSSR-96-08
REQ-10.96-01-TS-HMI.0070 <i>[NSV-4] Display and highlight with Automatic Speech Recognition Element: Controller HMI Management</i>	The HMI shall enable the ATCOs to give special commands for highlighting upcoming changes to the sectorization.	TSSR-96-10
REQ-10.96-01-TS-HMI.0080 <i>[NSV-4] Display and highlight with Automatic Speech Recognition Element: Controller HMI Management</i>	The HMI shall enable the ATCOs to give special commands for highlighting how upcoming changes to the sectorization will affect the flights being controlled by an ATCO.	TSSR-96-11
REQ-10.96-01-TS-HMI.0090 <i>[NSV-4] Display and highlight with Automatic Speech Recognition Element: Controller HMI Management</i>	The HMI shall enable the ATCOs to give special commands for navigating the 3D visualization of the air space.	TSSR-96-12
REQ-10.96-01-TS-SF.0120 (New) <i>[NSV-4] Prefilling of commands with Automatic Speech Recognition Element: Automatic Speech Recognition</i>	ASR shall be able to process and recognize less used phraseology/waypoints.	TSSR-96-13

Table 5: TSSR (functionality and performance) satisfying TSSRs for Normal and Abnormal conditions

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

in Table 6 is provided the consolidated list of the additional TSRDs (functionality and performance) derived from the dynamic analysis of the technical system behaviour (in normal and abnormal conditions of operations). For each TSRD is indicated the element of the design model on which the TSRD is placed, as well as the corresponding TSSR.

The details of the dynamic analysis derivation process is included in Appendix B.

Technical Safety Requirement ID [Design Model Element], [Source]	Technical Safety Requirement content	TSSR (ID)
REQ-10.96-01-TS-SF.0130 (New) <i>[NSV-4] Display and highlight with Automatic Speech Recognition</i> Element: Controller HMI Management	The HMI shall display a callsign recognised by ASR from ATCO's utterance in the form of a historical annotation to the ATCO.	TSSR-96-03
REQ-10.96-01-TS-SF.0140 (New) <i>[NSV-4] Display and highlight with Automatic Speech Recognition</i> Element: Controller HMI Management	The HMI shall enable the ATCOs to give special commands for highlighting a sector of interest.	TSSR-96-09

Table 6: Additional TSRDs derived from static and dynamic analysis of the technical system behaviour (normal and abnormal conditions of operation)

5.4 Technical Safety Requirements at design level addressing Internal System Failures

The purpose of this section is to present the Technical Safety Requirements at Design level (TSRDs) addressing internal system failures (e.g. failure of the technical system component).

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.

The following TSRDs are derived from a bottom up failure modes and effects analysis encompassing the analysis of common causes and from the TSSR (functionality & performance) aimed at the protective mitigation of the functionality hazards).

5.4.1 Design analysis with respect to internal system failure conditions

In order to identify a complete list of ASR component failures that could cause each functionality hazard top-down and bottom-up analysis have been performed.

For each functionality hazard, the top-down addressed the identification of ASR components failures and combinations thereof that could cause the functionality hazard. To achieve that, a table of causes

showing for each functionality hazard its causes and the associated mitigations was used (Appendix C.1.1).

Besides TSRD (functionality&performance) already derived in Section 4.2, additional TSRD (functionality&performance) were identified to ensure the satisfaction of the TSSR (integrity/reliability) associated to the functionality hazard.

TSRD (integrity/reliability) associated to internal system failures were derived from the TSSR (integrity/reliability), driven by the causal analysis of each functionality hazard, accounting for the existing or new proposed preventive mitigations and with due consideration of any potential common cause failure.

The bottom-up analysis of the failure modes was performed in order to complement the results obtained through top-down analysis. It ensured a more in depth causal analysis of failure of specific parts of the ASR system design.

5.4.2 Technical Safety Requirements at design level addressing internal system failures

In Table 7 is provided the consolidated list of Technical Safety Requirements at Design level (functionality and performance) addressing internal system failures. It includes:

- TSRD (functionality and performance) derived from the TSSR (integrity/reliability) from section 4.3 to provide adequate mitigations to reduce the likelihood that specific failures would propagate up to the functionality hazard.
- the TSRD (functionality and performance) to provide mitigation against functionality hazard effects (protective mitigation formalized as TSSR (functionality&performance) derived during the functionality hazard assessment at Appendix A.2).

For each TSRD (functionality&performance) is also indicated the element of the design model (i.e. NSV-4 model) on which the TSRD is placed, as well as the originating TSSR.

The detail of the derivation process is included in Appendix C.

Technical Safety Requirement ID	Technical Safety Requirement description (functionality & performance)	Derived from TSSR (ID) or Common cause failure
REQ-10.96-01-TS-HMI.0060	The ASR system should provide the functionality to be switched off and switched on when necessary.	TSSR-96-14 TSSR-96-19 TSSR-96-20
REQ-10.96-01-TS-SF.0150 (new)	If the confidence level of the callsign recognition is not sufficiently high, it shall not be highlighted.	TSSR-96-15 TSSR-96-16 TSSR-96-17

		TSSR-96-18
REQ-10.96-01-TS-HMI.0040	The HMI shall enable manual correction/update of automatically proposed command value/type.	TSSR-96-19 TSSR-96-20
REQ-10.96-01-TS-SF.0110 (New)	The HMI associated with ASR shall enable the ATCO to reject recognized command values for pre-filling radar label values by clicking on a rejection button.	TSSR-96-20

Table 7. Additional TSRDs (functionality & performance) to mitigate functionality hazards

Table 8 presents the consolidated list of Technical Safety Requirements at Design level (integrity/reliability) addressing internal system failures derived from the TSSRs (integrity/reliability) documented in section 4.3. For each TSRD is also indicated the element of the design model on which the TSRD is placed, as well as the originating TSSR.

The detail of the derivation process is included in Appendix C.

Technical Safety Requirement ID	Technical Safety Requirement description (integrity/reliability)	Derived from TSSR integrity/reliability (ID)
REQ-10.96-01-TS-ReTi.0010	ASR should send not later than 1.0 second a recognized callsign to the cooperating ATC system when the controller has pressed the push-to-talk-button and fully said the callsign (aircraft identifier).	TSSR-96-14
REQ-10.96-01-TS-ReTi.0020	For 99.9% of the ATCO utterances except callsign itself, the system shall be able to give the output in less than two seconds after the ATCO has released the push-to-talk button.	TSSR-96-14
REQ-10.96-01-TS-Perf.0050	The Command Recognition Rate of ASR for pilots SHOULD be higher than 75%.	TSSR-96-15
REQ-10.96-01-TS-Perf.0040	The Command Recognition Rate of ASR of ATCOs should be higher than 85%.	TSSR-96-16 TSSR-96-19
REQ-10.96-01-TS-Perf.0030	The Command Recognition Error Rate of ASR SHOULD be less than 5% for pilots	TSSR-96-17
REQ-10.96-01-TS-Perf.0010	The Command Recognition Error Rate of ASR should be less than 2.5% for ATCOs.	TSSR-96-18 TSSR-96-20

Table 8. TSRD (integrity/ reliability) to mitigate functionality hazards

5.5 Realism and testability of the Safe Design

The Safety Requirements related to ASR system have been addressed in the validation exercises. The objective evidence on the performance and functionality of the ASR has been derived from the human-in-the-loop real-time simulations using the platforms representing the operational environment as close as feasible to the actual ones.

The changes in human tasks introduced by the usage of the ASR system impact only the input tasks made by the controller in the CWP HMI. Namely, controller needs to monitor and check input provided by the ASR after the recognition of the utterance rather than to make a manual input (callsign, clr, hdg etc.). The results obtained through Human Performance assessment of the PJ10-W2-96 ASR solution (TS/IRS Part IV,[8]) prove that the tasks to be performed by the controllers with the introduction of ASR system are feasible and acceptable given their nature and the conditions under which they are expected to be performed.

5.6 Process assurance of the Safe Design

The safety assurance activities applied are in line with the activities envisaged for V3 concept development phase, as defined in SRM [3].

The Safety Requirements (functionality & performance) at Design level (SRD) in normal and abnormal conditions of operation from the SRS (functionality & performance) were identified through the analysis of the operation of the design under normal and abnormal conditions of operations. Further to this, the Safety Requirements (functionality & performance) and Safety Requirements (integrity&reliability) at Design level (SRD) were identified from SRS (integrity/ reliability) through the assessment of the adequacy of the design in the case of internal failures and mitigation of the Solution operational hazards.

The complementary HAZID workshop was performed with the safety experts, human performance and the operational experts involved in the PJ10-W2-96 ASR solution. In addition, the safety requirements consolidation workshop was performed F2F with the entire project team (TS/IRS, HP and validation exercises leads and contributors).

Safety assessment event	Scope	Outcomes
HAZID workshop Hazard refinement	Technological Safety Requirements at Service Level	TSSR
F2F HP & SAF workshop	Refinement of Technical Safety requirements at Design level and their consolidation at solution level	TSRD Input to TS/IRS Part I

Table 9 Safety activities performed to derive TSRD.

The evidence to support the safety assessment was obtained through the four human-in-the-loop RTS conducted within representative operational environments with participation of licensed air traffic controllers. The obtained results represent the consolidation of the quantitative data recorded during the simulation and the subjective opinions of the participating controllers contributing to the operational significance of the evidence.

6 Demonstration of achievability of the Technical System Safety Specification

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

The following table presents the summary of results coming from the validation exercises.

	EXE-001	EXE-002	EXE-003	EXE-005	Sol.96 ASR
CRT-Sol.96ASR-TRL6-TVALP-0040.001	ATCOs agreed that the accuracy of the information provided by the ASR system was adequate to accomplish the operations although there were differences among ATCOs	As reported for CRT-Sol.96ASR-TRL6-TVALP-0020.001, the relevant command error rated stayed below 2.5%; the callsign error rate was around 0.5%. ATCOs confirmed that level and quality of information provided by the system (in the radar labels) were an acceptable level with an average score of 8.8 on a scale from 1 up to 10, i.e., 10 indicates the best rating option. ATCOs also confirmed that operating methods are	Controllers considered that the accuracy was not enough to support them	There are no indications that the results presented above regarding recognition rates affected safety	For some exercises ATCOs considered that the accuracy was not enough or just sufficient to support them, but for one exercise ATCOs confirmed that level and quality of information provided by the system (in the radar labels) were an acceptable level.

		clearly identified and consistent in all operating condition with an average score of 8.3 on a scale from 1 up to 10, i.e., 10 indicates the best rating option.			
CRT-Sol.96ASR-TRL6-TVALP-0040.002	ATCOs agreed that the timeliness of information was acceptable	ATCOs confirmed the timeliness of ASRU output in the aircraft radar labels with an average score of 8.5 on a scale from 1 up to 10, i.e., 10 indicates the best rating option.	Controllers considered that the timeliness of the callsign recognition at the beginning of the phrase should be higher. The timeliness of the callsign at the end of the utterance and event recognition was enough although could be improved.	There are no indications that the results presented above regarding response times rates affected safety	The timeliness of the ASR output was confirmed and in some cases wished to be higher.
CRT-Sol.96ASR-TRL6-TVALP-0040.003	33% of ATCOs either agreed or strongly agreed that ASR did not increase potential for human error compared to current operations, whereas 17% of ATCOs disagreed, and the rest (50%)	ATCOs confirmed that ASR did NOT increase the potential for human errors with an average score of 3 on a scale from 1 up to 10, i.e., 10 indicates the worst rating option.	No error resulted from the introduction of the ASR	There are no indications of errors resulting from the introduction of the ASR.	ATCOs confirmed that ASR did NOT increase the potential for human errors.

	were neutral about it.	Objective analysis even shows that the number of errors in the radar label cells, i.e., missing input is much less if ATCOs are supported by ASRU compared to enter everything manually with mouse ($\alpha < 10-7\%$).			
CRT-Sol.96ASR-TRL6-TVALP-0040.004	All ATCOs were in agreement that the 'Hook' function improves situational awareness and could also be used as a safety barrier for avoiding confusion between inbound flights with similar callsigns.	ATCOs confirmed that their situational awareness is maintained at acceptable level with ASRU with an average score of 8.9 on a scale from 1 up to 10, i.e., 10 indicates the best rating option.	All ATCOs saw their situational awareness was increased or unaffected with the introduction of the ASR system.	The use of ASR did not affect the SA negatively. This is also supported by the interviews, where no ATCOs expressed that the SA was decreased when using ASR.	ATCOs stated that the situational awareness was increased or unaffected with the introduction of the ASR system.
CRT-Sol.96ASR-TRL6-TVALP-0040.005	Solution scenarios can be considered homogeneous, with no significant peaks in workload. most ATCO responses (90%)	The secondary task for objective workload measurement (Stroop test) showed a statistically significant decrease ($\alpha = 0.2\%$) of	ATCOs stated that the workload did not change or was decreased using the ASR technology.	the WL level were slightly higher for the ATCOs using ASR than the ones not using it, but this may just as well be explained by	ATCOs stated that the workload did not change or was decreased using the ASR technology. For one exercise a secondary

	indicated an acceptable level of WL	workload when ATCos are supported by ASRU. The ATCo-self-rated ISA score confirmed this with the same statistical significance ($\alpha=0.2\%$). In the final questionnaire, ATCos confirmed that ASRU supported them in maintaining workload at acceptable level with an average score of 7.9 on a scale from 1 up to 10, i.e., 10 indicates the best rating option.		a combination of differences in the dispatch of traffic between the sessions and the unbalance between the workload between the sectors in parts of the sessions.	task was performed for objective workload measurement (Stroop test) and showed a statistically significant decrease ($\alpha=0.2\%$) of workload when ATCos are supported by ASRU.
--	--	---	--	--	--

Table 10 Summary of Safety Success Criteria Results

7 Acronyms and Terminology

Acronym	Definition
ABSR	Assistant Based Speech Recognition
ACC	Area Control Centre
AI	Artificial Intelligence
ANSP	Air Navigation Service Provider
APP	Approach
ASR	Automatic Speech Recognition
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATM	Air Traffic Management
ATS	Air Traffic Services
ASW	Air Situation Window
CC	Capability Configuration
CHMI	Controller HMI
CLAM	Cleared Level Adherence Monitoring
CPDLC	Controller-Pilot Data Link Communications
CR	Change Request
CWP	Controller Working Position
DAC	Dynamic Airspace Configuration
EATMA	European Air Traffic Management Architecture
EC	Executive Controller
ENVAR	Environmental Assessment Report
ER	En-Route
EUROCAE	European Organisation for Civil Aviation Equipment
HF	High Frequency
HLOR	High Level Operational Requirements
HMI	Human Machine Interface
HPAR	Human Performance Assessment Report
ICAO	International Civil Aviation Organisation
ID	Identifier

IRS	Interface Requirements Specification
MTI	Multi-Touch-Input
MONA	Monitoring Aids
NSV	NATO System View
PC	Planning Controller
POI	Performance Operational Improvement
PTT	Push To Talk
RAM	Route Adherence Monitoring
SAR	Safety Assessment Report
SeAR	Security Assessment Report
SDD	Service Description Document
SESAR	Single European Sky ATM Research
SFPL	System Flight Plan
SRS	Safety Requirement at Service Level
S3JU	SESAR 3 Joint Undertaking (Agency of the European Commission)
TLA	Target Location Assistance
TMA	Terminal Manoeuvring Area
TRL	Technology Readiness Level
TS	Technical Specification
TSSR	Technical Specification Safety Requirement
TSRD	Technical Specification Requirement at Design Level
UC	Use Case
VCS	Voice Communication System
VHF	Very High Frequency
VoIP	Voice over IP

Table 11: Acronyms

Term		Definition
Automatic Recognition	Speech	An Automatic Speech Recognition (ASR) system gets an audio signal as input and transforms it into a sequence of words, i.e. “speech-to-text” following the recognition process. The sequence of words is transcribed into a sequence of ATC concepts (“text-to-concepts”) using an ontology. E.g: The word sequence “lufthansa two alpha altitude four thousand feet on qnh one zero one four reduce one eight zero knots or less turn left heading two six zero” is transcribed into “DLH2A ALTITUDE 4000 ft, DLH2A INFORMATION

	QNH 1014, DLH2A REDUCE 180 OR_LESS, DLH2A HEADING 260 LEFT". The resulting concepts can be used for further applications such as visualization on an HMI.
Command Recognition Rate	The number of controller commands which are correctly recognized by ASR and are not rejected divided by number of total given commands; in other words: the percentage of given commands correctly shown on the controllers' HMI. $CRR = \frac{\text{correctly recognised controller commands}}{\text{controller commands}} \cdot 100$
Command (Recognition) Error Rate	The number of controller commands which are wrongly recognized by ASR and which are not rejected divided by number of total given commands; in other words: the percentage of given commands wrongly shown on the controllers' HMI. $CER = \frac{\text{wrongly recognised controller commands}}{\text{controller commands}} \cdot 100$
Command Hypotheses Predictor	Components needed for Assistant Based Speech Recognition which predicts a set of possible commands.
Command Prediction Error Rate	The number of controller commands which are not predicted by the Command Hypotheses Predictor divided by number of total given commands. $CPER = \frac{\text{not predicted commands}}{\text{controller commands}} \cdot 100$
Command (Recognition) Rejection Rate	The number of recognized controller commands which are correctly or wrongly rejected (plus number of given controller commands which are not recognized at all) divided by number of total given commands. $CRejR = \frac{\text{rejected commands} + \text{not recognised commands}}{\text{controller commands}} \cdot 100$
Functional Block	A logical and cohesive grouping of automated Functions in a Technical System
Assistant Based Speech Recognition (ABSR)	Automatic Speech Recognition system that benefits from input from an assistance system (e.g. arrival manager) to generate probable commands and improve speech recognition.
Ontology	An internal dictionary to Automatic Speech Recognition, containing the relation between regular spoken utterances and events they refer to in a logical way, i.e. the translation between human and machine languages.

Table 12: Glossary of terms

8 References

Safety

- [1] (EU) No 2017/373 laying down common requirements for service providers and the oversight in air traffic management/air navigation services and other air traffic management network functions, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011 and (EU) No 1035/2011 and amending Regulation (EU) No 677/2011 (and associated AMC and GM)
- [2] SAM EUROCONTROL Safety Assessment Methodology, Edition 2.0
- [3] SESAR Safety Reference Material, Ed. 00.04.01, 14 December 2018
- [4] Guidance to Apply SESAR Safety Reference Material D.0.050 14 December 2018 Ed.00.03.01

Human Performance

- [5] Human Performance Guidance Reference Material v00.03.01

Project documentation

- [6] SESAR Solution PJ.10-W2- 96 ASR Final TS/IRS for TRL6
- [7] SESAR Solution PJ.10-W2-96 ASR -Final TVALR
- [8] SESAR Solution PJ.10-W2-96 ASR Human Performance Assessment Report
- [9] D1-1: MALORCA Operational Concept Document (edition 3.00), The Horizon 2020 SESAR project MALORCA (Machine Learning of Speech Recognition Models for Controller Assistance) partly funded by SESAR Joint Undertaking (Grant Number 698824)

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

A.1 Define TSSRs for Normal and Abnormal conditions

A.1.1 Static analysis of the technical specification

The static analysis of the ASR system behaviour at the interface with the operational user (i.e. controller) was performed for each of the PJ10-W2-96 ASR solution use cases (section 3.1.1.2 of the TS/IRS Part I [6]) to identify TSSRs (functionality and performance).

ID	Description	Use Case
TSSR-96-01	A callsign recognised by ASR from pilot's utterance shall be highlighted in the CWP HMI.	UC 1
TSSR-96-02	A callsign recognised by ASR from ATCO's utterance shall be highlighted in the CWP HMI.	UC 2 UC 3 UC 4 UC 8
TSSR-96-04	The controller's utterance shall be transformed into a sequence of ATC commands.	UC 2 UC 3 UC 4 UC 8
TSSR-96-05	A command recognized as part of an ATCO's utterance shall be displayed in the CWP HMI.	UC 3 UC 4 UC 8
TSSR-96-06	The command recognized and displayed by ASR shall be accepted if correct, automatically by the system or manually by the controller.	UC 4 UC 8
TSSR-96-07	If a command recognised by ASR is identified as incorrect by the controller, he/she shall be able to correct it.	UC 4 UC 8
TSSR-96-08	ATCO shall be able to reject the command incorrectly identified by ASR and displayed.	UC 4 UC 8
TSSR-96-10	An upcoming layout of sectors recognised by ASR from ATCO's utterance shall be highlighted in the CWP HMI.	UC 5 UC 7
TSSR-96-11	The relevant flights shall be highlighted in the CWP HMI from ATCO's utterance to highlight the flights affected by the upcoming sectorization change.	UC 6
TSSR-96-12	ATCO shall be able to navigate 3D visualization of the airspace.	UC 7
TSSR-96-13	ASR shall be able to process the ATCO utterances containing less frequent phraseology / way points with the same level of performance as for normal operations.	Abnormal conditions

A.1.2 Dynamic analysis of the technical specification

ID	Description	Use Case
----	-------------	----------

TSSR-96-03	A callsign recognised by ASR from ATCO's utterance shall be displayed on CWP HMI in the form of a historical annotation.	UC 3
TSSR-96-09	A sector recognised by ASR from ATCO's utterance shall be highlighted in the CWP HMI.	UC 5

A.2 Define TSSRs addressing failure conditions

A.2.1 FHA Workshop

The TSSRs for failure conditions might specify mitigation preventing the operational hazards to occur or might be expressed as the acceptable frequency (or probability on demand) of the Functionality Hazard. Therefore, for TSSR derivation, the link between ASR Functionality Hazards and potential operational hazard has been established via Fault Tree (see Figure 1 Operational Hazard fault tree below).

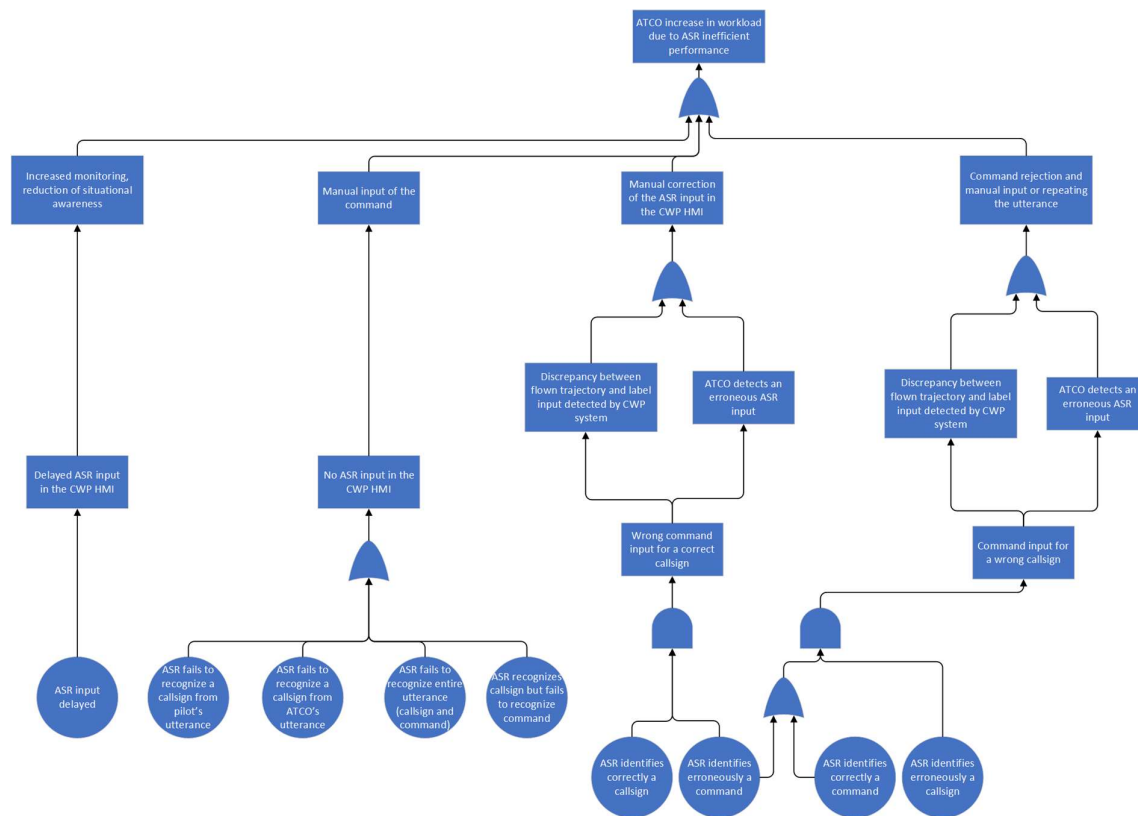


Figure 1 Operational Hazard fault tree

Through the FHA, it has been recognised that the impact of the ASR functional hazards is not significant from the safety point of view. The impact of the ASR inefficient performance might result in situations which are also present in current way of working impacting negatively human performance, i.e. increase in workload, but with the support of clearance monitoring tools already used in current operations (such as CLAM, RAM, MONA, etc.), these events will not escalate into safety relevant events.

In the Table 12 below are provided a list of causes, the assessed operational effect, the mitigations taken into account for defining the operational effect (protecting against the functionality hazard effects propagation), both those external to the technical system scope and those provided by the technical system (covering already identified during the identification of TSSRs functionality and performance and new mitigations which are further formalized as new TSSRs functionality and performance), as well as functional hazards of the ASR system.

Two types of TSSRs have been derived from this process:

- Additional TSSRs (functionality and performance) to mitigate against functionality hazard effects (protective mitigations)
- TSSRs addressing integrity/reliability in order to limit the frequency with which functionality hazards are allowed to occur (effect propagating mitigations).

Use Case	Potential causes	Operational effect	Mitigations protecting against propagation of effects	Functionality hazard & Severity
General application of ASR (applicable to all UCs)	Design issue ASR provides delayed output	If the use of ASR introduces delays in the usage of speech information (display of inputs, identification of aircraft, etc.) this may cause the ATCo to focus on specific flight/area of the AoR until they can verify that the action induced by ASR has been correctly processed and displayed. This may have negative impact on ATCo situational awareness.	Contingency measure to switch off ASR	FHz#01 Significant delay in ASR command recognition and/or display. No safety issue
UC 1 Highlight of callsigns on the CWP from pilot utterances.	Pilot utters a not understandable callsign Pilot utters a legal and understandable callsign, but ASR fails to recognize it	If pilot performs the radio call and the flight is not highlighted ATCo may have to scan the AoR to locate the aircraft. No difference to current operating method. However, if ASR functionality to highlight the callsign is defined in the new operating method, there is a default expectation by the ATCo that it is functional and assisting in locating aircraft, resulting in minor workload increase and situational awareness reduction.	ATCo may have to scan the AoR to locate the aircraft. No difference to current operating method.	FHz#02 ASR fails to identify an aircraft from pilot's utterance – no aircraft is highlighted No safety issue

Use Case	Potential causes	Operational effect	Mitigations protecting against propagation of effects	Functionality hazard & Severity
UC 2 Highlight of callsigns on the CWP from controllers utterances.	ATCO utters an illegal/not understandable callsign ATCO utters a legal and understandable callsign, but ASR fails to recognize it.	If ATCo performs the radio call it is assumed the impact is minor as the ATCo attention is focused on the aircraft being called and the impact is negligible.	No difference to current operating method.	FHz#03 ASR fails to identify an aircraft from controller's utterance—no aircraft is highlighted No safety issue
UC 1 Highlight of callsigns on the CWP from pilot utterances.	Pilot utters an not understandable callsign Pilot utters a legal and understandable callsign, but ASR recognizes an existing wrong callsign. Pilot utters a legal and understandable callsign, but ASR recognizes a wrong callsign not matching to callsigns considered by the system.	If pilot performs the radio call and erroneous flight is highlighted, the ATCo may focus on the highlighted aircraft and issue the clearance intended for the calling aircraft to the wrong flight. The difference to current operating method is that while occasional callsign confusion may occur between similar callsigns, now the ASR system is enforcing the ATCos perception of issuing the clearance to what is expected to be the correct flight. If the confusion is not clarified through read-back and hear-back procedure or with the assistance of the planning controller, issued clearance to the wrongly highlighted aircraft may result in an unintended trajectory change. From safety perspective this is not	If the confidence level of the callsign recognition is not sufficiently high, it is not highlighted. For lower confidence levels to highlight with different color to emphasize the uncertainty of correct recognition. If the erroneous recognition persists, ATCO switches off the ASR and continues working as in today's operations.	FHz#04 ASR erroneously identifies an aircraft from pilot's utterance – wrong aircraft is highlighted No safety issue

Use Case	Potential causes	Operational effect	Mitigations protecting against propagation of effects	Functionality hazard & Severity
		significantly different from current operating method.		
UC 2 Highlight of callsigns on the CWP from controllers utterances.	ATCO utters an illegal/not understandable callsign ATCO utters a legal and understandable callsign, but ASR recognizes an existing wrong callsign. ATCO utters a legal and understandable callsign, but ASR recognizes a wrong callsign not matching to callsigns considered by the system.	If ATCO performs the radio call and erroneous flight is highlighted, it is assumed the impact is minor as the ATCO's attention is on the aircraft being called and the impact of erroneous highlight is negligible.	If the confidence level of the callsign recognition is not sufficiently high, it is not highlighted. For lower confidence levels to highlight with different color to emphasize the uncertainty of correct recognition.	FHz#05 ASR erroneously identifies an aircraft from controller's utterance – wrong aircraft is highlighted No safety issue
UC 3 Annotation of controllers commands UC 4 Pre-filling of commands in the CWP UC 8 Prefilling of Datalink commands	ATCO utters an illegal/not understandable command ATCO utters a legal and understandable command, but ASR fails to recognize it	The failure of ASR to identify a complete command forces ATCO to manually make the input. In such cases the negative impact on ATCO workload and situational awareness increases is expected, as in the new operating method there is a default expectation by the ATCO that ASR is functional and assisting in inputting commands in the labels.	ATCO inputs command manually. If the failure of ASR to recognize commands persists, ATCO switches off the ASR and continues working as in today's operations.	FHz#06 ASR fails to identify a command from controller's utterance. No safety issue

Use Case	Potential causes	Operational effect	Mitigations protecting against propagation of effects	Functionality hazard & Severity
UC 3 Annotation of controllers commands UC 4 Pre-filling of commands in the CWP UC 8 Prefilling of Datalink commands	ATCO utters an illegal/not understandable command ATCO utters a legal and understandable command, but ASR recognizes the incorrect command and wrong command is displayed in the CWP HMI.	In cases where inputs are provided but are erroneous the ATCo will have to recognize the error and change information already input into the system. Depending on the ATM-system, some parts of correcting the clearance, etc. route change, may require manipulation of the FPL route data to input the correction. In such cases the impact on ATCo workload and potential disruption to the ATCo workflow may be higher than in cases where only missing data needs to be input to complete the clearance.	ATCO corrects ASR input manually for the intended callsign. If the failure of ASR to recognize commands correctly persists, ATCO switches off the ASR and continues working as in today's operations.	FHz#07 ASR erroneously identifies a command from controller's utterance No safety issue
UC 3 Annotation of controllers commands UC 4 Pre-filling of commands in the CWP UC 8 Prefilling of Datalink commands	ATCO utters a legal and understandable command, but ASR recognizes an incorrect callsign, which is being considered by the system, and the command is displayed for the incorrect flight in the CWP HMI.	In cases where inputs are provided but are erroneous (i.e. command input for wrong aircraft), ATCo will have to recognize the error and change information already input into the system. If the error is not recognized by the controller, the contacted pilot will nevertheless follow the clearance issued by controller on the frequency. The erroneous input in the label	If ATCO recognizes the error, he/she rejects and either repeats the clearance or inputs it manually directly into the label of the correct aircraft. If ATCO does not recognize the error, monitoring aids will detect the discrepancy between the flown trajectory and the command inserted in the label of the erroneous aircraft.	FHz#08 ASR recognizes an incorrect callsign, and the command is displayed for the incorrect flight in the CWP HMI. No safety issue

Use Case	Potential causes	Operational effect	Mitigations protecting against propagation of effects	Functionality hazard & Severity
		of another aircraft will soon be detected by clearance monitoring aids (e.g. CLAM, RAM, MONA)		
UC 5 Voice commands for highlighting an upcoming sectorization change in the CWP UC 6 Voice commands for highlighting the fights that will be affected by an upcoming sectorization change in the CWP	ATCO utters an illegal/not understandable command ATCO utters a legal and understandable command, but ASR fails to recognize it	This may cause to controller to get an erroneous understanding of how the sector being controlled will change. The system highlights wrong set of flights based on wrongly recognised controller utterance resulting in erroneous understanding of which flights will be affected by the changes in the sector being controlled.	An error message is briefly shown, and the ATCO needs to say the command again This will be clarified when the sectorization change is effectuated.	FHz#09 ASR erroneously identifies the sector from controller's utterance – wrong sector/layout/flights is/are highlighted No safety impact
UC 7 Voice commands for navigating the 3D visualization of the air space in the CWP	ATCO utters a legal and understandable command addressing a sector that is not part of the ACC ATCO utters an illegal/not understandable command ATCO utters a legal and understandable command, but ASR fails to recognize it	In the new operating method there is a default expectation by the ATCo that ASR is functional and assisting in navigating the 3D visualization of the airspace, resulting in minor workload increase.	An error message is briefly shown, and the ATCO needs to say the command again ATCO navigates manually the 3D visualization of the air space in the CWP	FHz#10 ASR erroneously identifies the command for navigating the 3D visualization of the air space in the CWP. No safety issue

Table 13 FHA working table

A.2.2 FHA Participation List

Name	Company	Role
Mirta Mestrovic	CCL/COOPANS	HF Expert
Alexandra Ghita	Deep Blue/Leonardo	HF Expert
Hartmut Helmke	DLR	EXE002 Lead
Raquel Garcia Lasheras	CRIDA/ENAIRE	EXE003 Lead
Erik G. Nilsson	SINTEF	EXE005 Lead
Sara Mansi	Leonardo	EXE001 Lead, Solution Lead
Jelena Dokic	Integra/ANS CR	Safety Expert

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

B.1 Deriving TSRDs from TSSRs

Table 14 below shows how the Technical Specification Safety Requirements (TSSRs) for normal and abnormal conditions of operation derived in section 4.2 map onto the related elements of the Design Model (i.e. NSV-4 models) and derived relevant Technical Safety Requirements at Design level (TSRDs) (functionality and performance).

The Safety Requirement identifiers in Table 14 below are the same as or consistent (for newly identified TRSDs) with the ones defined in Section 4 of the TS/IRS Part I. The consolidated list of TSRDs for normal and abnormal conditions of operation is included in section 5.3.1 of this document.

TSSR for Normal&Abnormal Operation (ID & content)	Technical Safety Requirement at Design level ⁴ (TSRD) or Assumption	Maps onto
TSSR-96-01 A callsign recognised by ASR from pilot's utterance shall be highlighted in the CWP HMI.	REQ-10.96-01-TS-HMI.0010 The HMI shall highlight the Track Label or part of it (or the track symbol) after recognizing the corresponding callsign.	[NSV-4] Display and highlight with Automatic Speech Recognition Element: Controller HMI Management
TSSR-96-02 A callsign recognised by ASR from ATCO's utterance shall be highlighted in the CWP HMI.	REQ-10.96-01-TS-HMI.0010 The HMI shall highlight the Track Label or part of it (or the track symbol) after recognizing the corresponding callsign.	[NSV-4] Display and highlight with Automatic Speech Recognition Element: Controller HMI Management
TSSR-96-04 The controller's utterance shall be transformed into a sequence of ATC commands.	REQ-10.96-01-TS-SF.0090: The voice flow (spoken words) shall be analysed and transformed into a text string. REQ-10.96-01-TS-SF.0100: The Apply Ontology and Logical Check function shall analyse the text string and transform it into the corresponding ATC concepts (following the Ontology) and	[NSV-4] Display and highlight with Automatic Speech Recognition [NSV-4] Prefilling of commands with Automatic Speech Recognition Element: Automatic Speech Recognition

⁴ iTSRD for the initial design or rTSRD for the refined design

	perform a logical check to discard incoherent commands.	
TSSR-96-05 A command recognized as part of an ATCO's utterance shall be displayed in the CWP HMI.	REQ-10.96-01-TS-HMI.0020 The HMI shall present the recognized (and validated) command types together with the command values in the radar label.	[NSV-4] Display and highlight with Automatic Speech Recognition [NSV-4] Prefilling of commands with Automatic Speech Recognition Element: Controller HMI Management
TSSR-96-06 The command recognized and displayed by ASR shall be accepted if correct, automatically by the system or manually by the controller.	REQ-10.96-01-TS-HMI.0030 The HMI shall enable acceptance of automatically inserted values by ATCo clicking on the value, by clicking on confirmation button in the dialogue line or by enabling automatic acceptance of recognized command values if the controller does not correct them within a predefined time frame (e.g. 10 seconds).	[NSV-4] Prefilling of commands with Automatic Speech Recognition Element: Manual acceptance: ATC Executive Controller Automatic acceptance: Automatic Speech Recognition
TSSR-96-07 If a command recognised by ASR is identified as incorrect by the controller, he/she shall be able to correct it.	REQ-10.96-01-TS-HMI.0040 The HMI shall enable manual correction/update of automatically proposed command value/type.	[NSV-4] Prefilling of commands with Automatic Speech Recognition Element: ATC Executive Controller
TSSR-96-08 ATCO shall be able to reject the command incorrectly identified by ASR and displayed.	REQ-10.96-01-TS-SF.0110: The HMI associated with ASR shall enable the ATCO to reject recognized command values for pre-filling radar label values by clicking on a rejection button.	[NSV-4] Prefilling of commands with Automatic Speech Recognition Element: ATC Executive Controller
TSSR-96-10 An upcoming layout of sectors recognised by ASR from ATCO's utterance shall be highlighted in the CWP HMI.	REQ-10.96-01-TS-HMI.0070 The HMI shall enable the ATCOs to give special commands for highlighting upcoming changes to the sectorization.	[NSV-4] Display and highlight with Automatic Speech Recognition Element: Controller HMI Management
TSSR-96-11 The relevant flights shall be highlighted in the CWP HMI	REQ-10.96-01-TS-HMI.0080 The HMI shall enable the ATCOs to give special commands for	[NSV-4] Display and highlight with Automatic Speech Recognition

from ATCO's utterance to highlight the flights affected by the upcoming sectorization change.	highlighting how upcoming changes to the sectorization will affect the flights being controlled by an ATCO.	<i>Element: Controller HMI Management</i>
TSSR-96-12 ATCO shall be able to navigate 3D visualization of the airspace.	REQ-10.96-01-TS-HMI.0090 The HMI shall enable the ATCOs to give special commands for navigating the 3D visualization of the air space.	<i>[NSV-4] Display and highlight with Automatic Speech Recognition</i> <i>Element: Controller HMI Management</i>
TSSR-96-13 ASR shall be able to process the ATCO utterances containing less frequent phraseology / way points with the same level of performance as for normal operations.	REQ-10.96-01-TS-SF.0120: ASR shall be able to process and recognize less used phraseology/ waypoints.	<i>[NSV-4] Prefilling of commands with Automatic Speech Recognition</i> <i>Element: Automatic Speech Recognition</i>

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

N/A

B.3 Dynamic analysis of the technical system

The TSRDs provided in the Table 15 have been identified through dynamic analysis (validation exercises performed as real-time simulations).

TSSR for Normal&Abnormal Operation (ID & content)	Technical Safety Requirement at Design level⁵ (TSRD) or Assumption	Maps onto
TSSR-96-03 A callsign recognised by ASR from ATCO's utterance shall be displayed on CWP HMI in the form of a historical annotation.	REQ-10.96-01-TS-SF.0130: The HMI shall display a callsign recognised by ASR from ATCO's utterance in the form of a historical annotation to the ATCO.	<i>[NSV-4] Display and highlight with Automatic Speech Recognition</i> <i>Element: Controller HMI Management</i>
TSSR-96-09 A sector recognised by ASR from ATCO's utterance shall be highlighted in the CWP HMI.	REQ-10.96-01-TS-SF.0140: The HMI shall enable the ATCOs to give special commands for highlighting a sector of interest.	<i>[NSV-4] Display and highlight with Automatic Speech Recognition</i>

⁵ iTSRD for the initial design or rTSRD for the refined design

		Element: Controller HMI Management
--	--	--

Table 15 Additional TSRDs derived through dynamic analysis

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)

The purpose is to derive from the TSSR (integrity/reliability) that have been identified in Section 4.3:

- TSRD (functionality and performance) in order to provide adequate mitigations to reduce the likelihood that specific failures would propagate up to the functionality hazard
- TSRD (integrity/ reliability) to limit the frequency with which failure of modified/new equipment elements in the Solution technical system could be allowed to occur.

C.1.1 Top-down causal analysis

In order to identify for each functionality hazard its causes and the associated mitigations a top-down causal analysis has been performed.

The identified mitigations refer to preventive mitigations for the functionality hazard, but they either prevent a basic cause to occur or they protect against the propagation of the basic cause effect up to the functionality hazard occurrence.

TSRD (functionality&performance) already provided in Section 4.2 might play a mitigation role, but additional TSRD (functionality&performance) have been derived here in order to ensure the satisfaction of the TSSR (integrity/reliability) associated to the functionality hazard.

TSRD (integrity/reliability) associated to internal system failures have been derived from the TSSR (integrity/reliability), driven by the causal analysis of each functionality hazard, accounting for the existing or new proposed preventive mitigations and with due consideration of any potential common cause failure.

Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
FHz#01: Significant delay in ASR command recognition and/or display	ASR provides delayed output	One or more of the ASR components is not performing as expected and causing the delay in the ASR output display.	REQ-10.96-01-TS-HMI.0060 The ASR system should provide the functionality to be switched off and switched on when necessary. REQ-10.96-01-TS-ReTi.0020 For 99.9% of the ATCo utterances except callsign itself, the system shall be able to give the output in less than two seconds after the ATCo has released the push-to-talk button.
FHz#02 ASR fails to identify an	Pilot utters a not understandable callsign	Pilot performs the radio call and the flight is not	REQ-10.96-01-TS-SF.0150 (new)

aircraft from pilot's utterance – no aircraft is highlighted	Pilot utters a legal and understandable callsign, but ASR fails to recognize it	highlighted in the CWP HMI.	If the confidence level of the callsign recognition is not sufficiently high, it shall not be highlighted.
FHz#03 ASR fails to identify an aircraft from controller's utterance– no aircraft is highlighted	ATCO utters an illegal/not understandable callsign ATCO utters a legal and understandable callsign, but ASR fails to recognize it.	ATCO performs the radio call and the flight is not highlighted in the CWP HMI.	REQ-10.96-01-TS-SF.0150 If the confidence level of the callsign recognition is not sufficiently high, it shall not be highlighted.
FHz#04 ASR erroneously identifies an aircraft from pilot's utterance – wrong aircraft is highlighted	Pilot utters an not understandable callsign. Pilot utters a legal and understandable callsign, but ASR recognizes an existing wrong callsign. Pilot utters a legal and understandable callsign, but ASR recognizes a wrong callsign not matching to callsigns considered by the system.	ATCo focuses on the highlighted aircraft and issue the clearance intended for the calling aircraft to the wrong flight. If the ATCo issues the clearance to the wrongly highlighted aircraft and may result in an unintended trajectory change.	REQ-10.96-01-TS-Perf.0030 The Command Recognition Error Rate of ASR SHOULD be less than 5% for pilots REQ-10.96-01-TS-Perf.0050 The Command Recognition Rate of ASR for pilots SHOULD be higher than 75%. REQ-10.96-01-TS-SF.0150 If the confidence level of the callsign recognition is not sufficiently high, it shall not be highlighted.
FHz#05: ASR erroneously identifies an aircraft from controller's utterance – wrong aircraft is highlighted	ATCO utters an illegal/not understandable callsign ATCO utters a legal and understandable callsign, but ASR recognizes an existing wrong callsign. ATCO utters a legal and	ATCo may get confused and issue a wrong clearance. If the ATCo issues the clearance to the wrongly highlighted aircraft, it may result in an unintended trajectory change.	Assumption A001: ATCOs will use standard phraseology as per ICAO Doc.4444. REQ-10.96-01-TS-Perf.0010 The Command Recognition Error Rate of ASR should be less than 2.5% for ATCos. REQ-10.96-01-TS-Perf.0040 The Command Recognition Rate of ASR of ATCos should be higher than 85%. REQ-10.96-01-TS-SF.0150 (new)

	understandable callsign, but ASR recognizes a wrong callsign not matching to callsigns considered by the system.		If the confidence level of the callsign recognition is not sufficiently high, it shall not be highlighted.
FHz#06: ASR fails to identify a command from controller's utterance	ATCO utters an illegal/not understandable command ATCO utters a legal and understandable command, but ASR fails to recognize it.	ATCo manually makes the input resulting in workflow disruptions and workload increase and situational awareness reduction.	REQ-10.96-01-TS-HMI.0040 The HMI shall enable manual correction/update of automatically proposed command value/type. REQ-10.96-01-TS-HMI.0060 The ASR system should provide the functionality to be switched off and switched on when necessary. REQ-10.96-01-TS-Perf.0040 The Command Recognition Rate of ASR of ATCos should be higher than 85%.
FHz#07: ASR erroneously identifies a command from controller's utterance	ATCO utters an illegal/not understandable command ATCO utters a legal and understandable command, but ASR recognizes an incorrect callsign, which is being considered by the system, and the command is displayed for the incorrect flight in the CWP HMI ATCO utters a legal and understandable command, but ASR recognizes the incorrect command and wrong command is displayed in the CWP HMI.	ATCo will have to change information already input into the system. Depending on the ATM- system, some parts of correcting the clearance, etc. route change, may require manipulation of the FPL route data to input the correction.	REQ-10.96-01-TS-HMI.0040 The HMI shall enable manual correction/update of automatically proposed command value/type. REQ-10.96-01-TS-SF.0110: The HMI associated with ASR shall enable the ATCO to reject recognized command values for pre-filling radar label values by clicking on a rejection button. REQ-10.96-01-TS-HMI.0060 The ASR system should provide the functionality to be switched off and switched on when necessary. REQ-10.96-01-TS-Perf.0010 The Command Recognition Error Rate of ASR should be less than 2.5% for ATCos.
FHz#08	ATCO utters an illegal/not	ATCO utters a legal and understandable	REQ-10.96-01-TS-Perf.0010

ASR recognizes an incorrect callsign, and the command is displayed for the incorrect flight in the CWP HMI.	understandable callsign followed by a command ATCO utters a legal and understandable callsign and a command, but ASR recognizes the incorrect callsign.	command, but ASR recognizes an incorrect callsign, which is being considered by the system, and the command is displayed for the incorrect flight in the CWP HMI.	The Command Recognition Error Rate of ASR should be less than 2.5% for ATCos. REQ-10.96-01-TS-Perf.0040 The Command Recognition Rate of ASR of ATCos should be higher than 85%. Assumption A003: ATCO is supported by the Clearance monitoring aids as in today's operations.
FHz#09 ASR erroneously identifies the sector from controller's utterance – wrong sector/layout/ flights is/are highlighted	ATCO utters an illegal/not understandable command ATCO utters a legal and understandable command, but ASR fails to recognize it	Wrong sector/layout/ flights is highlighted	REQ-10.96-01-TS-Perf.0010 The Command Recognition Error Rate of ASR should be less than 2.5% for ATCos. REQ-10.96-01-TS-SF.0110 The HMI associated with ASR shall enable the ATCO to reject recognized command values for pre-filling radar label values by clicking on a rejection button.
FHz#10 ASR erroneously identifies the command for navigating the 3D visualization of the air space in the CWP	ATCO utters a legal and understandable command addressing a sector that is not part of the ACC ATCO utters an illegal/not understandable command ATCO utters a legal and understandable command, but ASR fails to recognize it	Erroneous navigation in 3D visualizations of the air space sectorisation	REQ-10.96-01-TS-Perf.0010 The Command Recognition Error Rate of ASR should be less than 2.5% for ATCos. REQ-10.96-01-TS-SF.0110 The HMI associated with ASR shall enable the ATCO to reject recognized command values for pre-filling radar label values by clicking on a rejection button.

Table 16. Detailing the fault tree causes and associated preventive mitigations (TSRD)

C.1.2 Bottom-up failure modes and effects analysis

The bottom-up analysis of the failure modes of the ASR elements / element-to-element interfaces and of their effects has been performed in order to determine potential common cause failures but also in order to allow a more in depth causal analysis of certain parts of the technical system design.

Technical system element	Failure mode	Effects	Mitigation/Safety Requirement	Functionality hazard
Command Prediction	Fails to forecast possible future controller commands. Failure to receive external data required for forecast of future controller commands (external data can be radar data, flight plan data, weather data, airspace data, and also historic data of those types).	The speech recognizer relies on the input of the predicted commands. Commands, which are not predicted (normally), cannot be recognized. So if command prediction accuracy is worse than recognition accuracy itself, the command prediction functionality might have no benefits for the recognition engine any more.	REQ-10.96-01-TS-Perf.0020 If ASR is used, the Command Prediction Error Rate should not be higher than 10% and also not be higher than 50% of the opposite command recognition rate (i.e. 100% minus the command recognition rate), without using the checker.	FHz#05: ASR erroneously identifies an aircraft from controller's utterance – wrong aircraft is highlighted FHz#06: ASR fails to identify a command from controller's utterance FHz#07: ASR erroneously identifies a command from controller's utterance FHz#08 ASR recognizes an incorrect callsign, and the command is displayed for the incorrect flight in the CWP HMI.
Recognise Voice Words	Fails to analyse the voice flow and to transform into a text string. Does not receive the Voice Flow.	No callsign or command is recognised by ASR and displayed on the CWP HMI.	Assumption A002: If ASR does not provide an input, ATCO proceeds as in current operations (manual input and with no highlight of the callsign).	FHz#06: ASR fails to identify a command from controller's utterance
Apply Ontology and Logical check	Fails to analyse the text string and to transform into a set of predefined commands to discard incoherent commands.	The ASR output is erroneous and incoherent.	REQ-10.96-01-TS.0020 The ASR shall recognize commands of different command categories.	FHz#01: Significant delay in ASR command recognition and/or display FHz#06: ASR erroneously identifies an aircraft from controller's utterance – wrong aircraft is highlighted FHz#07: ASR erroneously identifies a

				command from controller's utterance
--	--	--	--	-------------------------------------

Table 17. FMEA (Failure Modes and Effects Analysis) table

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

The purpose is to derive TSRD (functionality&performance) from the TSSRs (functionality&performance) that have been derived in Appendix A.2 to provide mitigation against functionality hazard effects (protective mitigation), with due consideration of the potential common cause failures that might affect the functionality hazard causes and its protective mitigation.

In Table 10 below is shown how the TSSRs (functionality&performance) for protective mitigation of functionality hazards map onto the related elements of the Technical Design Model (technical system components or interactions/data flows).

The additional TSRDs (functionality and performance) for addressing internal system failures have been derive by the mapping of the TSSR onto the related elements of the Design Model.

The Safety Requirement identifiers in 10 below are consistent with the ones defined in Section 4 of the TS/IRS Part I. The new derived TSRDs (functionality&performance) for addressing internal system failures are included in section 5.4.2 of this document.

TSSR for Protective mitigation (ID & content)	Technical Safety Requirement at Design level ⁶ (TSRD) or Assumption	Maps onto
TSSR-96-14 The time needed to display command recognized by ASR shall be optimised to support controller's task execution.	REQ-10.96-01-TS-ReTi.0010 ASR should send not later than 1.0 second a recognized callsign to the cooperating ATC system when the controller has pressed the push-to-talk-button and fully said the callsign (aircraft identifier). REQ-10.96-01-TS-ReTi.0020 For 99.9% of the ATCO utterances except callsign itself, the system shall be able to give the output in less than two seconds after the ATCO has released the push-to-talk button.	<i>[NSV-4] Display and highlight with Automatic Speech Recognition</i> <i>[NSV-4] Prefilling of commands with Automatic Speech Recognition</i> <i>Elements:</i> <i>Automatic Speech Recognition</i> <i>Controller HMI Management</i>
TSSR-96-15 Required callsign recognition rate from pilot's utterance shall be set to a level appropriate for the application used and shall	REQ-10.96-01-TS-Perf.0050 The Command Recognition Rate of ASR for pilots SHOULD be higher than 75%.	<i>[NSV-4] Display and highlight with Automatic Speech Recognition</i> <i>Elements:</i>

⁶ iTSRD for the initial design or rTSRD for the refined design

be high enough to ensure that occasional ASR errors do not disrupt ATCo task execution.		Automatic Speech Recognition Controller HMI Management
TSSR-96-16 Required callsign recognition rate from ATCO's utterance shall be set to a level appropriate for the application used and shall be high enough to ensure that occasional ASR errors do not disrupt ATCo task execution.	REQ-10.96-01-TS-Perf.0040 The Command Recognition Rate of ASR of ATCOs should be higher than 85%.	<i>[NSV-4] Display and highlight with Automatic Speech Recognition</i> <i>Elements:</i> Automatic Speech Recognition Controller HMI Management
TSSR-96-17 Required callsign recognition error rate from pilot's utterance shall be set to a level appropriate for the application used and shall be low enough to ensure that occasional ASR errors do not disrupt ATCo task execution.	REQ-10.96-01-TS-Perf.0030 The Command Recognition Error Rate of ASR SHOULD be less than 5% for pilots	<i>[NSV-4] Display and highlight with Automatic Speech Recognition</i> <i>Elements:</i> Automatic Speech Recognition Controller HMI Management
TSSR-96-18 Required callsign recognition error rate from ATCO's utterance shall be set to a level appropriate for the application used and shall be low enough to ensure that occasional ASR errors do not disrupt ATCo task execution.	REQ-10.96-01-TS-Perf.0010 The Command Recognition Error Rate of ASR should be less than 2.5% for ATCOs.	<i>[NSV-4] Display and highlight with Automatic Speech Recognition</i> <i>Elements:</i> Automatic Speech Recognition Controller HMI Management
TSSR-96-19 Required command recognition rate from ATCO's utterance shall be set to a level appropriate for the application used and shall be high enough to ensure that occasional ASR errors do not disrupt ATCo task execution.	REQ-10.96-01-TS-Perf.0040 The Command Recognition Rate of ASR of ATCOs should be higher than 85%.	<i>[NSV-4] Prefilling of commands with Automatic Speech Recognition</i> <i>Elements:</i> Automatic Speech Recognition Controller HMI Management
TSSR-96-20 Required command recognition error rate from ATCO's utterance shall be set to a level	REQ-10.96-01-TS-Perf.0010 The Command Recognition Error Rate of ASR should be less than 2.5% for ATCOs.	<i>[NSV-4] Prefilling of commands with Automatic Speech Recognition</i>

appropriate for the application used and shall be low enough to ensure that occasional ASR errors do not disrupt ATCo task execution.		<i>Elements:</i> <i>Automatic Speech Recognition</i> <i>Controller HMI Management</i>
---	--	---

Table 18: TSRDs derived by mapping TSSRs for Protective mitigation of functionality hazard to Design Model Elements

Appendix D Assumptions, Safety Issues & Limitations

D.1 Assumptions log

In Table 19 below are provided the Assumptions that were raised in deriving the above Safety Requirements. The identified assumptions are considered as out of scope of the current solution, as they refer to the currently existing operating methods.

Ref	Assumption
A001	ATCOs will use standard phraseology as per ICAO Doc.4444.
A002	If ASR does not provide an input, ATCO proceeds as in current operations (manual input and with no highlight of the callsign).
A003	ATCO is supported by the clearance monitoring and conflict detection aids as in today's operations.

Table 19: Assumptions log

D.2 Safety Issues log

N/A

D.3 Operational Limitations log

N/A

-END OF DOCUMENT-

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