



SESAR Solution PJ07-03 SPR-INTEROP/OSED for V3 - Part II - Safety Assessment Report

Deliverable ID:	D4.2.010
Dissemination Level:	PU
Project Acronym:	PJ07 OAUO
Grant:	733020
Call:	H2020-SESAR-2015-2
Topic:	SESAR.IR-VLD.Wave1-09-2015
Consortium Coordinator:	EUROCONTROL
Edition Date:	23 September 2019
Edition:	00.01.04
Template Edition:	02.00.01

Founding Members



EUROPEAN UNION



EUROCONTROL



Authoring & Approval

Authors of the document

Name/Beneficiary	Position/Title	Date
Hugo MANSO TORRES EUROCONTROL	PJ07-03 member/Safety Expert	23/09/2019
Nicolas FOTA EUROCONTROL	PJ07-03 member/Safety Expert	23/09/2019

Reviewers internal to the project

Name/Beneficiary	Position/Title	Date
Frank Jelinek ECTL	Exercise Lead	18/09/2019
Kris Delcourte ECTL	Project Manager PJ07	18/09/2019
BLOCHING, Oliver AIRBUS	EXE Coordinator ATC	18/09/2019
KUPSCH, Norbert Airbus	Solution Contributor	18/09/2019
PLEVKA, Jan ANS CR (B4)	EXE Coordinator ATC	18/09/2019
HOVANCIK, Lumir ANS CR (B4)	Solution Contributor	18/09/2019
CIZEK, Vladimir ANS CR (B4)	Solution Contributor	18/09/2019
MARVAN, Vaclav ANS CR (B4)	Solution Contributor	18/09/2019
REUBER, Edgar EUROCONTROL CMC	Solution Contribution (former PJ.18-01a)	18/09/2019
KUREN, Igor EUROCONTROL CMC	Solution Contributor	18/09/2019
BREIVIK, Kim EUROCONTROL NM	Solution Contributor	18/09/2019
NECULAE, Cezar EUROCONTROL NM	Solution Contributor	18/09/2019

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

Name/Beneficiary	Position/Title	Date
DEL COURTE, Kris EUROCONTROL	Project Manager PJ07	27/09/2019
HERMANN, Klaus Dieter AIRBUS Defence and Space	Solution Lead PJ.07-03	27/09/2019
HOUSEK, Petr ANS CR (B4)	Solution Contribution Lead	27/09/2019

Rejected By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date

Document History

Edition	Date	Status	Author	Justification
00.00.01	02/05/2018	Draft proposed for Project review	Hugo MANSO TORRES Nicolas FOTA / EUROCONTROL	Creation of the Safety Assessment Report at operational (OSED) level (i.e. up to Section 3), distributed for Project internal review
00.01.00	31/05/2018	Consolidated version for V2 phase	Hugo MANSO TORRES / EUROCONTROL Nicolas FOTA / EUROCONTROL	Document updated with the comments from internal Project review
00.01.01	30/05/2019	Draft initial V3 phase for Project review	Hugo MANSO TORRES Nicolas FOTA / EUROCONTROL	Addition of the section 4 "Safe design" (SPR and TS levels)
00.01.02	30/06/2019	Draft document	Hugo MANSO TORRES Nicolas FOTA / EUROCONTROL	Update of section 4.5.1 after Safety Workshop
00.01.03	09/09/2019	Final draft proposed for Project review	Hugo MANSO TORRES Nicolas FOTA / EUROCONTROL	Update of the document accounting for updated SPR-INTEROP/OSED and provided TS/IR and VALR
00.01.04	23/09/2019	Final proposed for Delivery for submission to SJU	Hugo MANSO TORRES Nicolas FOTA / EUROCONTROL	Update of the document after project internal review

Copyright Statement © – 2019 – PJ.07-03 Partners: EUROCONTROL, AIRBUS Defence and Space and ANS CR (B4).

All rights reserved. Licensed to the SESAR Joint Undertaking under conditions

PJ07 OAUO

PJ07 OPTIMISED AIRSPACE USERS OPERATIONS

This Safety Assessment Report (SAR) is part of a project that has received funding from the SESAR Joint Undertaking under grant agreement No 733020 under European Union's Horizon 2020 research and innovation programme.



Abstract

This document specifies the results of the safety assessments carried out in SESAR 2020 Wave 1 by Project PJ.07 on the Mission Trajectory Driven Processes supported by Project PJ.18-Solution 01 (Mission Trajectories) by the European Organisation for the Safety of Air Navigation (EUROCONTROL).

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

Table of Contents

Abstract	4
1 Executive Summary.....	9
2 Introduction.....	11
2.1 Background	11
2.1.1 Solution objectives and scope.....	11
2.1.2 Outline of the change.....	12
2.2 General Approach to Safety Assessment	16
2.3 Scope of the Safety Assessment	17
2.4 Layout of the Document	18
3 Safety specifications at the operational level.....	19
3.1 Scope	19
3.2 Solution Operational Environment and Key Properties	20
3.2.1 Airspace Characteristics	20
3.2.2 Airspace Users – Flight Rules.....	20
3.2.3 Aircraft ATM capabilities	20
3.2.4 Ground ATM/ATFCM capabilities.....	20
3.3 Stakeholders’ expectations which impact Safety	21
3.4 Relevant Pre-existing Hazards	22
3.5 Safety Criteria	23
3.6 Mitigation of the Pre-existing Risks – Normal Operations	29
3.6.1 Operational Services to Address the Pre-existing Hazards	29
3.6.2 Derivation of Safety Objectives (Functionality & Performance – success approach) for Normal Operations.....	30
3.7 Solution Operations under Abnormal Conditions.....	35
3.7.1 Identification of Abnormal Conditions.....	35
3.7.2 Potential Mitigations of Abnormal Conditions.....	35
3.8 Mitigation of System-generated Risks (failure approach)	37
3.8.1 Identification and Analysis of System-generated Operational Hazards.....	37
3.8.2 Derivation of Safety Objectives (integrity/reliability)	42
3.9 Impacts of Mission Trajectory Driven Processes Solution operations on adjacent airspace or on neighbouring ATM Systems.....	44
3.10 Achievability of the Safety Criteria – Safety validation objectives.....	44
3.11 Validation & Verification of the Safety Specification	44
4 Safe Design (SPR and TS level).....	45
4.1 Scope	45

4.2	The initial design level Model & Safety Requirements derivation – Normal Operational conditions	45
4.2.1	Description of the initial design level Model	46
4.2.2	Task Analysis	46
4.2.3	Derivation of Safety Requirements (Functionality and Performance – success approach)	46
4.3	Analysis of the initial design level Model – Normal Operational Conditions	57
4.3.1	Scenarios for Normal Operations	57
4.3.2	Thread Analysis of the SPR-level Model – Normal Operations	58
4.3.3	Effects on Safety Nets – Normal Operational Conditions	58
4.3.4	Dynamic Analysis of the initial design level Model – Normal Operational Conditions	59
4.3.5	Additional Safety Requirements (functionality and performance) – Normal Operational Conditions	59
4.4	Analysis of the SPR-level Model – Abnormal Operational Conditions	59
4.5	Design Analysis – Case of Internal System Failures	59
4.5.1	Causal Analysis	60
4.5.1.1	Hz 01: Undetected incorrect traffic load data provided by Regional ATFCM to users	61
4.5.1.2	Hz 02: MIL flight inbound a sector with short notice (from adjacent sector)	69
4.5.1.3	Hz 03: ATFCM measures not implemented or implemented partially by local ATFCM	74
4.5.1.4	Hz 04: Conflict-inducing lateral deviation due to ground-airborne iRMT inconsistency	75
4.5.1.5	Hz 05: Uncoordinated ARES exit leading to imminent separation infringement	79
4.5.2	Common Cause Analysis	80
4.5.3	Formalization of Mitigations	80
4.5.4	Safety Requirements (integrity/reliability)	86
4.6	Achievability of the SAFETY Criteria – Safety validation results	86
4.7	Realism of the SPR-level Design	86
4.7.1	Achievability of Safety Requirements / Assumptions	86
4.7.2	“Testability” of Safety Requirements	86
4.8	Validation & Verification of the Safe Design at SPR Level	87
5	Acronyms and Terminology	88
6	References	91
Appendix A Derivation of Safety Objectives (Functionality & Performance – success approach) for Normal Operations		92
A.1	EATMA Process Models	92
A.2	Derivation of Safety Objectives for Normal Operations driven by EATMA Process Models	99
Appendix B HAZID Workshop Results		111
Appendix C Consolidated List of Safety Requirements		131
C.1	Safety Requirements (Functionality and Performance)	131
C.2	Safety Requirements (Integrity)	142
Appendix D Assumptions, Safety Issues & Limitations		143
D.1	Assumptions log	143

D.2	Safety Issues log	143
D.3	Operational Limitations log.....	143

List of Tables

Table 1	Pre-existing hazards relevant for AU Processes for Trajectory Definition	22
Table 2:	Operational services and Pre-existing Hazards	29
Table 3:	List of Safety Objectives (success approach) for Normal Operations	34
Table 4:	Additional Safety Objectives (success approach) for Abnormal Conditions	37
Table 5:	System-Generated Operational Hazards and Analysis.....	40
Table 6:	Safety Objectives (integrity/reliability).....	44
Table 7:	Derivation of Safety Requirements (functionality and performance) from Safety Objectives	56
Table 8	Causal Analysis for Hazard 01	68
Table 9	Causal Analysis for Hazard 02	73
Table 10	Causal Analysis for Hazard 03	74
Table 11	Causal Analysis for Hazard 04.....	78
Table 12	Causal Analysis for Hazard 05.....	79
Table 13	Safety Requirements formalizing the mitigations preventing the operational hazards occurrence (the ones added to the existing set of SPR-INTEROP/OSED or TS/IRS requirements are highlighted in bold)	85
Table 14:	Acronyms and terminology	90
Table 15:	Solution Operational Services & Safety Objectives (success approach)	110
Table 16	Full HAZID Working table.....	130
Table 17	Safety Requirements (functionality and performance) from the “success approach”	140
Table 18	Safety requirements (functionality and performance) from the “failure approach”	142
Table 19:	Assumptions log	143
Table 20:	Safety Issues log.....	143
Table 21:	Operational Limitations log	143



List of Figures

Figure 1 Simplified Mid-Air Collision (MAC) En Route (ENR) Accident Incident Model (AIM) & SACs allocation.....	24
Figure 2 Simplified Mid-Air Collision (MAC) TMA Accident Incident Model (AIM) & SACs allocation..	25



1 Executive Summary

This document contains the Safety Assessment for a typical application of Mission Trajectory Driven Processes supported by SESAR Activity PJ.18-01a (Mission Trajectories) and represents the Part II of the SPR-INTEROP/OSED.

The report has been generated by the safety assessment activities in support of the Design and Validation activities and in this version it presents the assurance that the Safety Requirements for the V1-V2 and V3 phases (when applicable, see below) are complete, correct and realistic, thereby providing all material to adequately inform the PJ.07-03 Solution OSED/SPR/INTEROP and TS/IRS.

The current version covers the operational specification level (OSD level) -incorporating the definition of the Safety Criteria and the derivation of the Safety Objectives- and the initial design level including the derivation of the Safety Requirements at SPR and TS level.

The Mission Trajectory Driven Processes addresses the following OIs:

- **AOM-0303: Pan-European OAT Transit Service (V3/TRL6)**
- **AOM-0304-A: Improved and Harmonised OAT Flight Plan (V3/TRL6)**
- **AUO-0215: Sharing iSMT through improved OAT flight plan (V3/TRL6)**
- AUO-0210: Participation in CDM through iSMT and Target Time (TTO) negotiation (not V3/TRL6)
- AUO 0211: WOC Management of iRMT via improved OAT FPL (not V3/TRL6)
- AUO-0228: Agreed iRMT (not V3/TRL6)

The activity PJ.18-01a focused on the technology by addressing the enablers related to the above OI steps.

From the OI steps above, only **AOM-0303, AOM-0304-A and AUO-0215 have completed V3/TRL6** and are under the scope of solution **PJ.07-03 “Sharing mission trajectory data with NM and ATC via an improved OAT Flight Plan (iOAT FPL)”**. This solution has been developed in the context of the validation of the wider “Mission Trajectory Driven Processes”, which also covered the rest of the OI steps. Solution PJ.07-03 captures those elements that were validated to V3/TRL6 in the context of SESAR 2020 Wave 1:

- The management of mission trajectory (MT) with variable profile areas (VPA) type of airspace reservations (ARES) as shared via iOAT FPL in **the planning phase**.
- The ARES conceptual evolution allowing more precise identification of ARES Entry and Exit location and time, to support the increased quality of the trajectory prediction in the corresponding wing operations centre (WOC), network manager (NM) and ATC systems. This includes the evolutions of the VPA module reference as integral part of the evolved iOAT FPL syntax & concept.



- The B2B services for iOAT FPL filing from WOC to NM as well as for the iOAT FPL distribution from NM to ATC. B2B services were as well successfully validated to connect Regional ATFCM (NM) and local ATC FMP systems.

2 Introduction

2.1 Background

2.1.1 Solution objectives and scope

Mission Trajectory Driven Processes solution refer, through a full integration of the Wing Operations Centre (WOC) within the ATM system, to the updating of WOC processes for the management of the shared and reference mission trajectory (SMT/RMT). These processes will respond to the need to accommodate individual military airspace user needs and priorities without compromising optimum ATM system outcome and the performances of all stakeholders.

The Mission trajectory driven processes, develop requirements and validate initial mission trajectory iMT integration into ATM network operations through exchange of iOAT FPL between Wing Operation Centres (WOCs), Regional ATFCM (IFPS) and ATC in close collaboration with airspace management (ASM). Continuity in iMT data sharing via iOAT FPL shared between all actors concerned will increase predictability and overall situation awareness on AU demand and contribute to the performance expectations of the ATM network.

Focus is laid on the management of the iSMT, represented by the iOAT FPL in the planning phase, (from the time of initial publication of the Shared Mission Trajectory SMT), and the management of the iRMT using the iOAT FPL format in the execution phase (until the flight termination).

Note: AFUA aspects and related CDM processes are out of scope of solution PJ.07-03 as these have been already developed and validated V3 in SESAR 1 programme. This project will be based on the results from SESAR 1 work packages contributing to the relevant OFA03.01.04: Business and Mission Trajectory.

The following Mission Trajectory Operating Methods (as they are called in the SPR-INTEROP/OSED [5] where they are further detailed through Use Cases) represent the areas of interest:

- iSMT Management in Short Term Planning Phase
- iRMT Management in Execution Phase
- iRMT Revision triggered by WOC
- iRMT Revision triggered by ATC
- iRMT Revision triggered by Flight Deck.

From the OI steps allocated to the mission trajectory driven processes, only AOM-0303, AOM-0304-A and AUO-0215 have completed V3/TRL6 and are under the scope of solution PJ.07-03 “Sharing mission trajectory data with NM and ATC via an improved OAT Flight Plan (iOAT FPL)”. The “Mission Trajectory Driven Processes” scope is wider and include in addition the rest of the OI steps. Solution PJ.07-03 captures those elements that were validated to V3/TRL6 in the context of SESAR 2020 Wave 1:

- The management of mission trajectory (MT) with variable profile areas (VPA) type of airspace reservations (ARES) as shared via iOAT FPL in the planning phase.

- The ARES conceptual evolution allowing more precise identification of ARES Entry and Exit location and time, to support the increased quality of the trajectory prediction in the corresponding wing operations centre (WOC), network manager (NM) and ATC systems. This includes the evolutions of the VPA module reference as integral part of the evolved iOAT FPL syntax & concept.
- The B2B services for iOAT FPL filing from WOC to NM as well as for the iOAT FPL distribution from NM to ATC. B2B services were as well successfully validated to connect Regional ATFCM (NM) and local ATC FMP systems.\

The scope of solution **PJ.07-03 “Sharing mission trajectory data with NM and ATC via an improved OAT Flight Plan (iOAT FPL)”** is limited to the OI steps that have completed V3/TRL6: **AOM-0303, AOM-0304-A and AUO-0215.**

2.1.2 Outline of the change

The **baseline** for the Safety Assessment will be, as declared in the SPR-INTEROP/OSED [5], “a combination of methods defined at national level applicable to state airspace users (military, police, custom, etc.), and new operating methods defined within the scope of SESAR 1 with V3 maturity level.”

From an operational point of view the **baseline** involves:

- With regards to ASM, AFUA and related CDM:
 - Automated Support for strategic, pre-tactical and tactical Civil-Military Coordination in Airspace Management (ASM)
 - Sharing in real time status of ARES (RTSA), encompassing interface between ASM and ATC systems delineating ARES on CWP
 - Europe-wide Shared Use of Military Training Areas
 - Flexible and modular ARES in accordance with the VPA design principle.
- With regards to FPL:
 - FPLs are filed (when applicable) by military in accordance with national regulations and procedures as laid down in National aeronautical publications (civil/military) (restricting the access to sensible flight related data for the ATM network).
 - FPLs are filed by military for GAT, mixed OAT/GAT flights as well as for pure OAT flights. For GAT and mixed OAT/GAT flights the FPL filing adheres to the maximum extent possible to the ICAO FPL format with due regard to the EUROCONTROL NMOC/IFPS provisions. For pure OAT flights (IFR and/or VFR) specific shortened formats may still be in use and their promulgation may be limited to military ATS, Air Defence (AD) and Command & Control (C2) units only.
 - Typical OAT FPLs (particularly related to fast jet operations) are currently not acceptable in NM IFPS owing to the incompatibility of data and formats used by military.

- OAT flights, as not being under European regulation, are exempted from ATFCM measures, whilst mixed OAT/GAT flights may be subject to measures unless individually exempted.
- EFPL (Extended Flight Plan as per SESAR 1 Solutions catalogue) is available: including additional information in relation to an aircraft's planned four-dimensional trajectory which supports an airspace environment where aircraft can fly their preferred flight paths. This four-dimensional flight plan data is integrated into the Network Manager Flight Planning acceptance and distribution system.
- With regards to ATC:
 - A unique ATC unit is in charge of both GAT and OAT flights in its area of responsibility (integrated civil-military ATS provision within one airspace continuum for all civil and military airspace users).

From a functional system point of view, the **Baseline** includes:

- ASM support tools automation
- Shared airspace planning information (ASM tools to ATFCM systems)
- Real time airspace status update (local ASM to Regional ATFCM systems; ASM systems to ATC systems)
- ASM support system interface for ASM data exchange between AMC, ATC, WOC and Regional ATFCM systems (see solution #31 in Baseline/SESAR 1 catalogue)
- Data exchange between WOC and IFPS to submit/update OAT Flight Plan (validated in SESAR 1 VP-789 and VP-790, which have been partially conducted up to V3)
- WOC Mission support tool (enabling the development of mission trajectory)
- NOP updated with airspace status info & route re-allocation
- Static and dynamic Airspace data in a standardised AIXM format
- Pan-European OAT-IFR Transit Service (OATTS) and IFR rules for OAT flights are available

The main operational change brought in by the new concept with regard to this Baseline is the introduction of the improved OAT Flight Plan (iOAT FPL), as a harmonized format proposed to be used by all military AUs in the IFPZ.

Only a harmonized format allows the central validation of the iOAT FPL and its management by Regional ATFCM and the sharing of the trajectory information between WOC, Regional ATFCM and ATC. It is a prerequisite to deploy the MT concept with the CDM process supporting the evolution of a flight intent becoming a SMT and finally a RMT.

In general, as ICAO2012 FPLs for GAT, iOAT FPL for OAT will be compliant with the full set of ATM Network rules and be subject of ATFCM Measures. Where, for mission needs this is not possible, existing exemption mechanism can be used. The iOAT FPL does not differentiate between GAT and

OAT sections anymore. Compared to the ICAO2012 FPL format, the iOAT FPL contains certain military specific information related to ARES and VPA use.

The aim is the integration of initial Mission Trajectory iMT into ATM network operations through exchange of iOAT FPL between Wing Operation Centres (WOCs), Regional ATFCM (IFPS) and ATC in close collaboration with airspace management ASM. Continuity in iMT data sharing via iOAT FPL between all actors concerned is expected to increase predictability and overall situation awareness on AU demand and contribute to the performance expectations of the ATM network.

A majority of Military Airspace Users will submit iOAT Flight Plans to Regional ATFCM, thus ensure visibility of OAT flight intentions to the network. These iOAT FPLs will be validated by Regional ATFCM and, if valid, distributed to ATC. WOC will be able to update them both in the planning and in the execution phase. Revisions to the iRMT can be initiated not only by the ATC and WOC but also by the Flight Deck.

With regards to Regional Airspace Management (at NM level) the military part of the environmental database will need to be integrated, involving a high extension of volume of data to be managed/maintained leading to increased complexity (input into CACD). The data structure might need to be adapted (e.g. account for MIL A/C performance), relying on the IR (Implementing Rule) setting up harmonization of MIL airspace data (e.g. move from 3 to 5 letter name convention) in order to assure compliance to ICAO naming conventions and to avoid important NMOC system adaptations (ETFMS, IFPS, CACD, ADR).

With regards to Regional Air Traffic Flow and Capacity Management, the additional iOAT FPLs need to be processed both in planning and in execution phase.

With regards to ATC, the Extended ATC Planner (EAP) and the Sector Planning Controller will have as new task the monitoring of the evolution of the updated RMT (e.g. evolving characteristics of planned ARES), for which new HMI functionalities will be needed.

With regards to Wing Operations Centre, with the new operating method WOC will send the iSMT to Regional ATFCM for impact assessment purposes and validation. If a mission change request is needed during the execution phase, WOC will be able to send it to ATC while previously it was done via the crew who coordinated with ATC. The Flight Data Operator will have a new task due to the potential need to correct/act upon NM responses. The Mission Observer might need to adapt the working methods with the use of ATC radar data sharing.

Note that the following are out of scope (not addressed within Wave 1):

- DMA 1 and 2
- En-route AAR operation (Air-to-Air Refueling)
- Formation flight.

The main system changes within the scope are:

- ATC FDPS systems receiving (from NM) & processing iOAT Flight Plan updates
- WOC and En-route / App exchange via B2B SWIM. The ATC system shall enable sharing the used surveillance data with WOC and receive WOC Trajectory revision request directly.



- New WOC system functionalities (format adaptation, interaction with ATC related to RMT revisions, ...)
- New ATC system functionalities (interaction with WOC related to RMT revisions...).

2.2 General Approach to Safety Assessment

A Broader approach

The safety assessment has been conducted in accordance with the SESAR Safety Reference Material (SRM) [2] and associated Guidance [3]. The SRM is based on a twofold approach:

- a new *success approach* which is concerned with the safety of the Solution operations (i.e. Mission Trajectory Driven Processes), in the absence of failure within the Functional System in the Solution scope; and
- a conventional *failure approach* which is concerned with the safety of the Solution operations in the event of failure within the Functional System in the Solution scope.

These two approaches are applied to the derivation of safety properties at each of two successive stages of the development of the new operating method, as follows:

Safety specification at the operational (OSED) Level

This is defined as what are the safety-relevant new or modified aspects that the Solution has to achieve at the ATM operational level in order to satisfy the requirements of the Airspace Users - *i.e.* it takes a “black-box” view of the Functional System in the Solution scope.

From a safety perspective, the user requirements are expressed in the form of Safety Criteria (SAC) and the Specification is expressed in the form of Safety Objectives (functionality & performance and integrity/reliability properties), which are derived during the V1 and V2 phases of the development lifecycle. The purpose is to check the completeness of the OSED Use Cases, to identify possibly additional safety-relevant validation objectives to be revealed by the safety analysis in view of their inclusion in the Validation plans and to prepare the derivation of Safety Requirements (performed at the next stage *i.e.* SPR level).

Safe Design (at SPR and TS Level)

This describes what the Functional System in the Solution scope itself is actually like internally and includes all those system properties that are not directly required by the Airspace Users but are implicitly necessary in order to fulfil the specification and thereby satisfy the User requirements. Design is essentially an internal, or “white-box”, view of the Functional System in the Solution scope. This is more generally called the logical design (or SPR and TS level) Model and is expressed in terms of human and machine “actors” that deliver the functionality.

From a safety perspective, the Design is expressed in the form of Safety Requirements (sub-divided into functionality & performance and integrity/reliability properties), which are derived during the V2 and V3 phases of the development lifecycle. The purpose here is to check the completeness of the SPR-INTEROP and TS design requirements, and, if relevant, inform the SPR-INTEROP/OSED and the TS/IRS (in accordance to Project maturity) with additional safety requirements that will be revealed by the safety analysis. Furthermore, if relevant, interact with the validation exercises so as to include additional validation objectives and obtain validation feedback regarding certain proposed safety requirements.

2.3 Scope of the Safety Assessment

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

- **V1** - through initial identification of safety implications of the Change and the definition of Safety Criteria
- **V2 & V3** - through establishing Safety Objectives (**at operational level**) to deliver the Safety Criteria and the derivation of Safety Requirements for the design up to V3 (**at design level, i.e. SPR and TS**, in accordance with Project maturity level) for part of the scope of Mission trajectory driven processes to satisfy the Safety Objectives (based on combined safety analysis of the design, and safety-related measurements, observations and debriefing of the validation exercises where applicable). The safety assessment for Safety Requirements derivation will align with the design maturity. The safety assessment will be conducted to the level of granularity decided by the Project for the OSED/SPR/INTEROP and TS/IRS documents for the design of the Functional system for the Solution as per V3 for the planning phase and initial V3 for the execution phase (encompassing people, procedures & airspace and equipment).

The current version of the SAR covers the Operating Methods and related Use Cases included in the OSED [5] of the PJ.07 Solution 03, supported by the system elements designed under PJ.18-01a.

The Solution focuses on the management of the Mission Trajectory by means of the iOAT FPL from the time of publishing the Initial Shared Mission Trajectory (iSMT) the first time until flight termination. Depending on the time frame and the different roles that can trigger a revision of the Mission Trajectory, the following Operating Methods (OM) are addressed within the PJ.07-03 OSED (note that in the OSED each Operating Method is further detailed through a set of Use Cases dedicated to each entity/actor):

- Operating Method 1: Mission Trajectory Management in the Short Term Planning Phase (creation and update, submission, validation and distribution of an iSMT by means of an improved OAT Flight Plan and transitions to the iRMT upon decision of the WOC after agreement of all involved stakeholders on the MT). This has completed V3/TRL6;
- Operating Method 2: Mission Trajectory Management in the Execution Phase (nominal execution of a MT, which may include an ARES reference, which is executed as stated in the iRMT). Not V3/TRL6;
- Operating Method 3: iRMT Revision triggered by WOC (WOC revision of iRMT after departure due to operational needs). Not V3/TRL6;
- Operating Method 4: iRMT Revision triggered by ATC (ATC revision of iRMT after departure due to operational needs). Not V3/TRL6;
- Operating Method 5: iRMT Revision triggered by Flight Deck (FD revision of iRMT after departure due to operational needs). Not V3/TRL6.

The Safety assurance activities have been conducted in line with the SESAR 2020 Safety Policy [1], SESAR Safety Reference Material (SRM) [2] and accompanying Guidance [3].

Finally, since the properties of the operational environment (OE) are crucial to the safety assessment, this assessment cannot be generic – it has to be specific to the Solution OE defined in section 3.2 and consequently, the term ‘specimen’ safety assessment should be used.

2.4 Layout of the Document

Section 1 presents the executive summary of the document

Section 2 provides background information related to the Mission Trajectory Driven Processes concept and outlines the related change, presents the principles of the safety assessment in SESAR Programme and the scope of this safety assessment

Section 3 addresses the safety specification at the operational level, through the definition of Safety Criteria (SAC), the determination of Safety Objectives (SO) and the link to safety validation objectives

Section 4 addresses the safe design (at SPR and TS level), through the derivation of Safety Requirements (SR) and link to validation results

Section 5 is dedicated to acronyms and specific terminology employed in this Safety Assessment Report

Section 6 lists the documents referred to in this Safety Assessment Report

Appendix A presents the EATMA models within the operational layer (process models) used to carry out the Safety Assessment at the operational level and the working table used to derive the Safety Objectives (Functionality & Performance) for normal operations

Appendix B presents the results of the HAZID Workshop

Appendix C provides a consolidated list of the Safety Requirements

Appendix D lists all the Assumptions, Safety Issues & Operational Limitations that arose during the safety assessment documented herein

3 Safety specifications at the operational level

3.1 Scope

Based on safety activities defined in the Safety Plan [4] this section addresses the following activities:

- Description of the key properties of the Solution Operational Environment which are relevant to the safety assessment – section 3.2
- Description of the Airspace Users' expectations – section 3.3. **Error! Reference source not found.**
- Identification of the pre-existing aviation hazards that affect traffic in the relevant operational environment (airspace, airport) and the risks which are reasonably expected to be mitigated to some degree and extent by the operational services provided by the Solution – section 0
- Setting of the SAFety Criteria (from the Solution Safety Plan [4]) – section 0
- Comprehensive determination of the operational services that are provided by the Solution to address the relevant pre-existing aviation hazards, understanding, throughout the Operating Methods/Use Cases, the Change brought in by the Solution and derivation of Safety Objectives (success approach) in order to mitigate the pre-existing risks under normal operational conditions – section 0
- Assessment of the adequacy of the operational services provided by the Solution under abnormal conditions of the Operational Environment – section 3.7
- Assessment of the adequacy of the operational services provided by the Solution in the case of internal failures and mitigation of the System-generated hazards (derivation of Safety Objectives -failure approach) – section 3.8
- Achievability of the SAFety Criteria – section 3.10
- Validation & verification of the safety specification – section 3.11

3.2 Solution Operational Environment and Key Properties

This sub-section describes the key properties of the Operational Environment that are relevant to the safety assessment of PJ07-03 supported by PJ18-01 (information summarized from PJ07.03 OSED/SPR/INTEROP section 3.2 [5]).

3.2.1 Airspace Characteristics

Managed airspace, both En-Route and TMA with high, medium and low complexity are considered.

The ENR and TMA managed airspaces are characterized by:

- Military airbases and airbases collocated with co-use by civil aviation
- TMA with military and mixed operations handling and transit service for OAT and GAT
- Control area (CTA) with military areas of responsibility
- Pilot briefing (ARO) on WOC side, handling and transit service for OAT and GAT
- ARES with tactical control and transit service for GAT

Airspace layout: current ICAO ATS airspace classifications (controlled airspace), regulations and applicable rules.

Free Routing Airspace is out of the scope for Wave 1. That will be tackled in Wave 2.

3.2.2 Airspace Users – Flight Rules

Operational Air Traffic (OAT) and General Air Traffic (GAT), both flying under IFR.

3.2.3 Aircraft ATM capabilities

Nothing new compared to current operations (however, enhancement in the application of the new method could be derived from the use of Data-Link services).

3.2.4 Ground ATM/ATFCM capabilities

Current Ground ATM capabilities:

- IFPS
- FDPS
- Initial SWIM (as per SESAR 1 Solutions catalogue) enabling Ground-ground interconnection
- AFUA
- ASM
- WOC Mission support tool
- ETFMS
- CACD

Founding Members

New Ground ATM capabilities:

- New enablers needed for PJ.07-03 which are out of the PJ.07-03 and PJ.18-01A solutions scope remain still to be identified e.g. for Regional and Local ATFCM systems.

The new enablers inside the PJ.07-03 and PJ.18-01A solutions scope (and as such not part of the operational environment) have been listed at §2.1.2.

3.3 Stakeholders' expectations which impact Safety

According to the SPR/INTEROP-OSED §6.1 and the Validation Plan §4.2 [8], the following benefits are expected for the Solution PJ.07-03 supported by PJ.18-01:

With relevance for the safety assessment:

Capacity: expected increase for ENR; thanks to the increased awareness of MIL demand, the sector capacity buffer aimed in current operations at mitigating the capacity shortfalls related to the limited availability of MIL demand will be reduced (the D4.2 Validation Targets 2019 [6] displays for PJ.07-03 an En-Route Capacity increase of +0.505% for any type of airspace complexity).

Safety: Safety will not be degraded compared to current operations and traffic levels despite the capacity increase. Potential to further improving Safety by reducing complexity (thanks to the enhanced traffic prediction).

Other benefits:

Predictability: expected to increase, thanks to better planning and traffic ordering; but also through allowing Military airspace users to have evidence of a significant improvement of mission efficiency via the integrated planning of trajectories by the users (WOC and FOC) and through allowing Airspace Users to choose the preferred way of integrating ATM constraints when required.

Cost efficiency: expected to increase, as a result of more efficient planning of staff allocation thanks to better collaboration and sharing of up to date data between actors.

MIL operations: significant improvement of mission efficiency through the integrated planning of trajectories by the users.

3.4 Relevant Pre-existing Hazards

A pre-condition for performing the safety assessment for the introduction of a new Concept is to understand the impact it would have in the overall ATM risk picture. The SRM Guidance D and E [3] provide a set of Accident Incident Models (AIM - one per each type of accident) which represent an integrated risk picture with respect to ATM contribution to aviation accidents.

In order to determine which AIM models are relevant for the PJ.07-03 supported by PJ.18-01a, this sub-section presents the relevant aviation hazards (that pre-exist in the operational environment before any form of ATM planning or de-confliction has taken place) that were identified within the HP&SAF scoping & change assessment session (using Guidance F.2.2 of [3]). The relevant pre-existing hazards, together with the corresponding ATM-related accident types and AIM models are presented in Table 1 below.

Pre-existing Hazards [Hp]	ATM-related accident type& AIM model
<p>Hp#1: Situation in which the intended trajectories of two or more aircraft are in conflict</p> <p>Encompassing:</p> <ul style="list-style-type: none"> • Conflicts between GAT IFR aircraft (e.g. as a side effect of traffic re-organisation related to ARES activation/de-activation) • Conflicts between GAT-OAT in civil-military mixed operations 	Mid-Air Collision (MAC) En Route & TMA AIM models
<p>Hp#2. Incursion In/ Excursion Out of ARES</p> <p>Encompassing:</p> <ul style="list-style-type: none"> • ARES infringement by non-participating IFR traffic • ARES borders excursion by MIL/CIV traffic using it 	<p>Mid-Air Collision or aircraft shot down- No AIM model available.</p> <p>Mid-Air Collision (MAC) En Route & TMA AIM models</p>
<p>Hp#3: Encounters with adverse weather</p>	Loss of control in flight due to adverse weather encounter - No AIM model available
<p>Hp#4. Fuel shortage - the potential contribution of the Concept to this aviation hazard is not in the focus of PJ07-03 supported by 18-01</p>	Loss of airframe due to fuel shortage- No AIM model available

Table 1 Pre-existing hazards relevant for AU Processes for Trajectory Definition

3.5 Safety Criteria

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

The SAC setting is driven by the analysis of the impact of the Change on the relevant AIM models, where available (at §0 the MAC En Route & TMA AIM model have been identified – see their simplified versions at Figure 1 and Figure 2), or otherwise is based on the analysis of the safety implications supported by operational expertise.

The set of SACs need to be consistent with the SESAR safety performance targets defined by PJ.19-04 in [6]. For PJ.07-03 the Safety Validation Targets are:

The reduction in the total number of MAC accidents per year of **-0.95% in En Route**¹, due to SESAR 2020 improvements with respect to a hypothetical “do nothing” scenario, in which no changes are made to ATM safety of the Baseline (2005) while traffic is allowed to increase until it reaches the capacity level targeted for SESAR in 2035.

¹ The PJ19: Validation Targets (2019) contains erroneous information regarding the safety improvement -0.18% in TMA (whilst no Capacity improvement in TMA is brought in by PJ07.03).

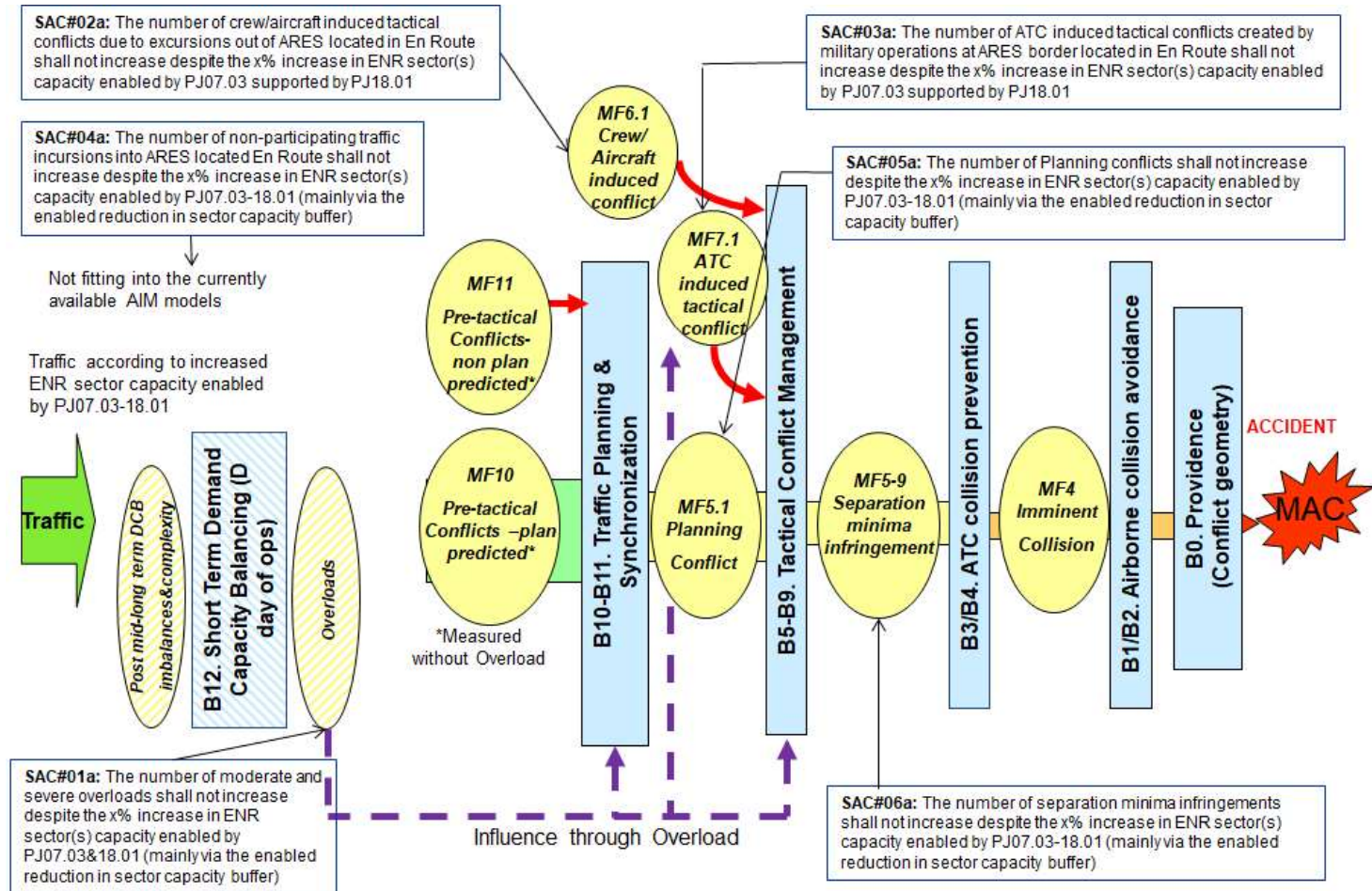


Figure 1 Simplified Mid-Air Collision (MAC) En Route (ENR) Accident Incident Model (AIM) & SACs allocation

Founding Members



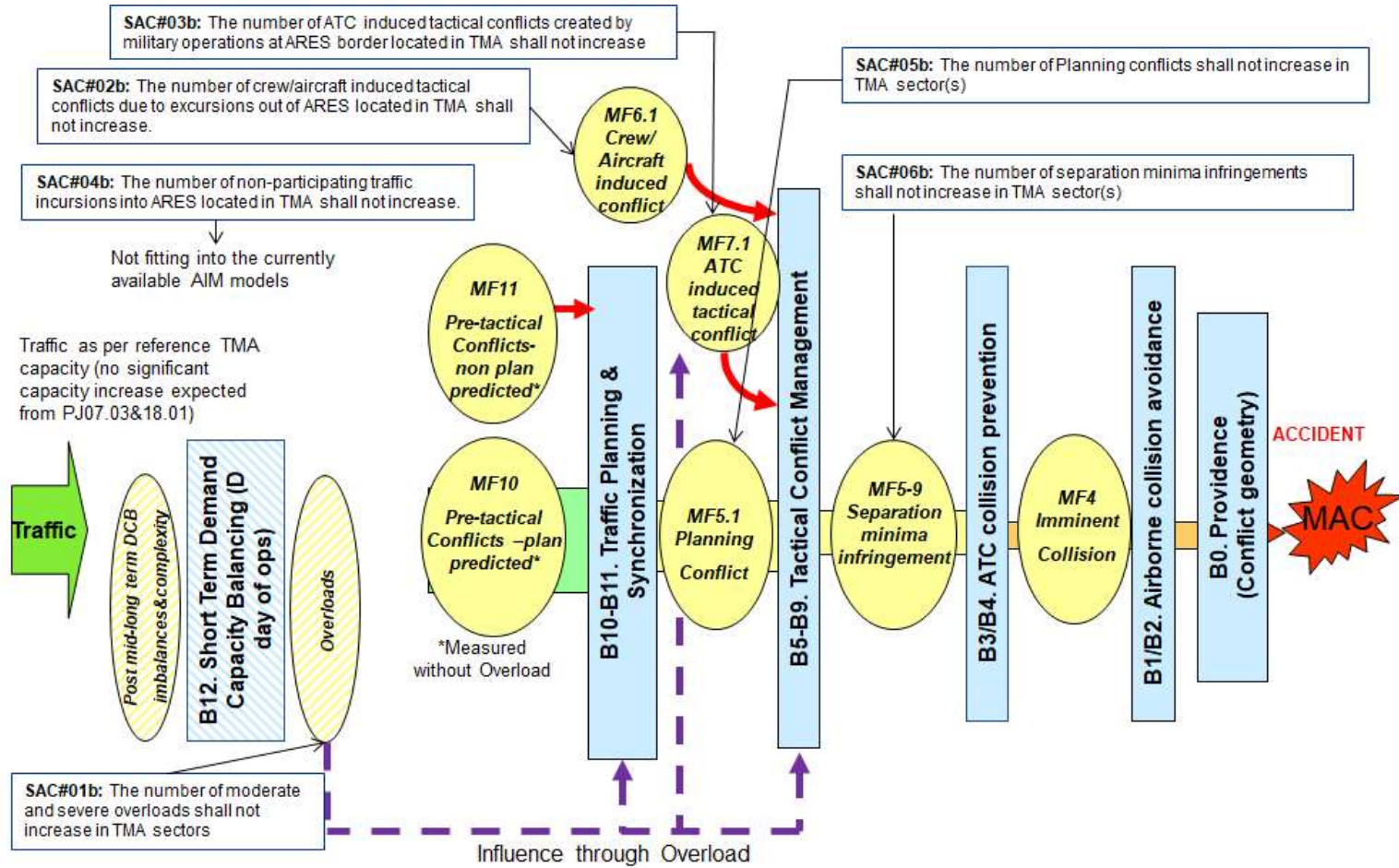


Figure 2 Simplified Mid-Air Collision (MAC) TMA Accident Incident Model (AIM) & SACs allocation

Founding Members



The following safety considerations can be drawn in relation to the Solution impact on the B12: Short Term Demand Capacity Balancing (in AIM MAC ENR & TMA models –see simplified versions in Figure 1 and Figure 2) which further on has an influence on the efficiency of the Tactical Planning and Tactical Conflict Management barriers:

- Safety impact through DCB: improvement of demand prediction thanks to the improved OAT flight plan i.e. of OAT prediction. Meanwhile, as the change will involve adaptation of certain functionalities in NM, WOC, ASM and ATC systems there is a need to control risk via specifying safety requirements for the functional system changes/developments (“functional system” encompassing people, procedures, equipment).

The following SACs are derived from the above consideration (with regards to the impact on Barrier B12 “Short Term Demand Balancing” -see *MB12²: Ineffective Short-term Demand/Capacity Balancing Resulting in Overloads* and subsequently the causes of ineffective Capacity management which will be impacted by the Solution):

SAC#01a: The number of moderate and severe overloads shall not increase despite the x% increase in ENR sector(s) capacity enabled by PJ.07-03 supported by PJ.18-01a (mainly via the enabled reduction in sector capacity buffer).

SAC#01b: The number of moderate and severe overloads shall not increase in TMA sector(s).

The following safety considerations can be drawn in relation to the Solution impact on the *MF6.1: Crew/Aircraft induced conflict* and *MF7.1: ATC Induced Tactical conflict* (in AIM MAC ENR & TMA models –see simplified versions in Figure 1 and Figure 2):

- There is a need to control risk related to Flight Plan data inconsistency (between CACD and ATC system), e.g. ARES exit points or exit times. The current mitigations will remain (e.g. crosscheck by WOC operator, then at tactical level), however need safety requirements for the system changes/developments.

The following SACs are derived from the above consideration, with regards to the tactical conflicts due to excursions out of ARES induced by crew/aircraft (see MF6.1.1.1.1² above: Airspace infringement by OAT/MIL traffic) and induced by ATC (see MF7.1.2.2²: Conflict created by Military operations at ARES border for ENR and MF7.1.3: Conflict with military A/C in own airspace created by ATC or MIL Unit):

SAC#02a: The number of crew/aircraft induced tactical conflicts due to excursions out of ARES located in En Route shall not increase despite the x% increase in ENR sector(s) capacity enabled by PJ.07-03 supported by PJ.18-01a

SAC#02b: The number of crew/aircraft induced tactical conflicts due to excursions out of ARES located in TMA shall not increase

² See detailed ENR and TMA AIM available on STELLAR -> Coordination Group – ATM Performance Assessment (APA) -> DOCUMENTS -> 05-Safety -> reference_documents -> AIM2017_Sept-17_Visio (1.2)

SAC#03a: The number of ATC induced tactical conflicts created by military operations at ARES border located in En Route shall not increase despite the x% increase in ENR sector(s) capacity enabled by PJ.07-03 supported by PJ.18-01a

SAC#03b: The number of ATC induced tactical conflicts created by military operations at ARES border located in TMA shall not increase

The following safety considerations can be drawn in relation to the incursions of non-participating traffic into ARES (no AIM model available):

- Non-participating traffic shall circumnavigate ARES. In addition to the non-participating CIV flights, the non-participating MIL flights become subject to DCB measures, flight-planning and tactical control to circumnavigate the ARES.

The following SAC is derived from the above consideration (with regards to the incursions of non-participating traffic into ARES):

SAC#04a: The number of non-participating traffic incursions into ARES located En Route shall not increase despite the x% increase in ENR sector(s) capacity enabled by PJ.07-03-PJ.18-01a (mainly via the enabled reduction in sector capacity buffer).

SAC#04b: The number of non-participating traffic incursions into ARES located in TMA shall not increase.

The following safety considerations can be drawn in relation to the Solution impact on the *B5: Plan Induced Conflict Management*, *B6: Crew/AC Induced Conflict Management*, *B9: VRF-IFR Conflict Management*, *B10: Traffic Planning and Synchronisation for plan predicted conflicts*, *B11: Traffic Planning and Synchronisation for non plan-predicted conflicts* and *MF7.1: ATC Induced conflict* (in AIM MAC ENR & TMA models –see simplified versions in Figure 1 and Figure 2):

- It shall be ensured that in ENR airspace the PLN and EXE ATCOs will be able to safely accommodate the enabled capacity increase in ENR, i.e. the possibility to reduce the sector capacity buffer (thanks to increased predictability with improved OAT plans).
- There will be several extra features that ATCO have to cope with: ARES part of flight plan; [*the following remain to be addressed in Wave 2: formation flight, En-Route AAR operation (Air-to-Air Refuelling)*]. It shall be ensured that these extra features do not adversely affect the current level of performance of the ATCOs safety-related tasks both in ENR and TMA.

Note: With PJ.07-03-PJ.18-01a, all aircraft in an airspace volume are provided with ATC service by the CIV or a MIL ATC unit which has the responsibility for that airspace volume. That might have an impact on the current version of the AIM MAC (ENR, TMA).

The following SACs are derived from the above considerations:

- With regards to the potential impact on the Planning ATCO tasks & workload -see MB10 Ineffective Traffic Planning or Synchronisation.

SAC#05a: The number of Planning conflicts shall not increase despite the x% increase in ENR sector(s) capacity enabled by PJ.07-03-PJ.18-01a (mainly via the enabled reduction in sector capacity buffer).

SAC#05b: The number of Planning conflicts shall not increase in TMA sector(s).

- With regards to the potential impact on the Executive ATCO tasks & workload (see B5: Plan Induced Conflict Management, B6: Crew/AC Induced Conflict Management, B9: VFR-IFR Conflict Management and MF7.1 ATC Induced Conflict).

SAC#06a: The number of separation minima infringements shall not increase despite the x% increase in ENR sector(s) capacity enabled by PJ.07-03-PJ.18-01a (mainly via the enabled reduction in sector capacity buffer).

SAC#06b: The number of separation minima infringements shall not increase in TMA sector(s)

Regarding the aviation hazard “Encounters with adverse weather”:

- the solution accounts for the potential adverse weather in the medium/short term planning phase, because according to OSED §3.2.2.6: “In the medium/short term planning phase, the ATS collects and integrates MET data into the trajectory profile definition for the SMT. Using this, plus other ATM-related data, the WOC identifies one or several geographical locations able to accommodate the trajectory profile part/s associated to the ARES type with the mission requirements, in order to minimise any impact of the MET phenomena on the execution of the mission. Furthermore, the WOC may develop several trajectory profiles for each mission, taking into consideration the operational requirements, priorities and safeguard clauses defined by military authorities, the MET data and other ATM constraints.” However, the safety impact concerns only the execution phase where the adverse weather is avoided tactically as per current operations. Consequently no specific Safety Criteria is derived to mitigate this aviation hazard.

3.6 Mitigation of the Pre-existing Risks – Normal Operations

3.6.1 Operational Services to Address the Pre-existing Hazards

Table 2 shows the list of ATM/ANS operational services, within the scope of PJ07-03 operations, provided to the Airspace Users to address the pre-existing aviation hazards.

ID	Operational Service	Pre-existing Hazards [Hp xx]
FPL#1	Flight plan preparation, filing, validation and distribution (focusing on Mission Trajectory, (including ARES cross check) in planning phase)	<p>Hp#1 (MAC risk)</p> <p>Hp#2 (ARES incursion/excursion risk)</p> <p>Hp#3 (Encounters with adverse weather)</p>
FPL#2	Flight plan revision (focusing on MT revision in execution phase)	<p>Hp#1 (MAC risk)</p> <p>Hp#2 (ARES incursion/excursion risk)</p> <p>Hp#3 (Encounters with adverse weather)</p>
ASM#1	Adjust the Capacity (to the extent where it is available) to fit the predicted Demand	<p>Hp#1 (MAC risk)</p> <p>Hp#2 (ARES incursion/excursion risk)</p>
ASM#2	Airspace reservation and management	<p>Hp#1 (MAC risk)</p> <p>Hp#2 (ARES incursion/excursion risk)</p>
DCB	Balance the predicted Demand against the available Capacity	<p>Hp#1 (MAC risk)</p> <p>Hp#2 (ARES incursion/excursion risk)</p>
ATC	<p>ATC services</p> <ul style="list-style-type: none"> • Planning & Coordination • Arrival sequencing, Metering, Holding • Maintain separation between aircraft • Handle request from AC (level, routing) • Manage trajectory • Lateral / vertical Deviation Detection & Resolution • Prevent unauthorized entry into restricted airspace • Prevent unauthorized exit from restricted airspace 	<p>Hp#1 (MAC risk)</p> <p>Hp#2 (ARES incursion/excursion risk)</p> <p>Hp#3 (Encounters with adverse weather)</p>

Table 2: Operational services and Pre-existing Hazards

3.6.2 Derivation of Safety Objectives (Functionality & Performance – success approach) for Normal Operations

The purpose of this section is to derive functionality & performance Safety Objectives (as part of the success approach) in order to mitigate the pre-existing aviation risks under normal operational conditions (i.e. those conditions that are expected to occur on a day-to-day basis) such as to meet the defined Safety Criteria.

That comes to interpret, from a safety perspective, the OSED Operational Concept specification (i.e. how the PJ.07-03 concept -supported by PJ.18-01a- contributes to the aviation safety) following and making use of the EATMA representation as per the Operational layer (each Operating Method being modelled through a process model made up of activities interacting via information flows).

The analysis of the concept is performed for a Mission trajectory definition and modification as specified via the OSED Operating Methods further detailed through Use Cases. The purpose is to derive a complete list of Safety Objectives, allowing to specify the Change involved by the Concept at the operational service level, by considering the management of a Mission trajectory definition and modification (i.e. the Function Processes dealing with the iSMT and iRMT generation by WOC with support from NM) as a continuous process. That allows to show how the Safety Objectives participate in the achievement of the relevant operational services and contribute to safety barriers (in the relevant AIM models) i.e. how they contribute to meeting the Safety Criteria.

This analysis is performed following and making use of the OSED Operating Methods and their representation through EATMA Process Models as defined by the PJ.07-03 OSED [5].

The following working method has been applied to derive the functionality & performance Safety Objectives (as part of the success approach) for Normal operations:

Step 1:

- For each Operating Method (described via an EATMA Process Model):
 - For each Activity:
 - Identify to **which operational service(s)** that Activity contributes to,
 - Identify whether the Activity is **new or modified**, and what is the change,
 - Whether necessary, refine the information by highlighting specific information flows produced or consumed by the Activity,
 - Based on the findings above (i.e. new or modified Activity), retain (or not) the Activity and the related information as a relevant input to the Safety Objectives derivation.

Step 2:

- Consolidate the information outcome from Step 1 above according to Operating Methods and Operational services
- For each Operating Method:
 - For each Operational service:
 - Check whether the identified change(s) **is (are) safety relevant** (i.e. could the change impact the efficiency of a safety barrier or the occurrence of a safety precursor? the previously identified operational services are a necessary but not sufficient indication, given their link to the AIM models),
 - Derive one or several Safety Objectives in order to describe the safety-relevant changes in the delivery of that operational service by the Solution.

The detailed application to PJ.07-03 of the method presented above is provided in Appendix A.

The rules used for codifying the different activities and flows, as well as for showing for each activity to which operational services it contributes to and whether it involves a change, are detailed in the same Appendix A.

The Table 3 below presents the list of functionality & performance Safety Objectives under normal operational conditions derived in Appendix A for PJ.07-03 supported by PJ.18-01a in accordance with the method described above. For each Safety Objective (SO), the link to the driving Safety Criteria is shown in the last column, via the relevant Operating Method and operational service that are concerned with the change and allowed the SO derivation (knowing that each operational service contributes to a safety barrier or precursor in the AIM models, and that the SACs have been defined in §0 at the level of the precursors of the AIM models).



ID	Safety Objective <i>(success approach)</i>	EATMA <i>OM-Activity or Flow</i>	Operational service	Related SAC# (AIM Barrier or Precursor)
SO 001	WOC shall submit (and resubmit if any update is needed) iSMT in time for enabling reliable traffic prediction	OM1-a1 OM1-a4	Flight plan preparation, filing, validation and distribution (focusing on Mission Trajectory (including ARES cross check) in planning phase,)	SAC#01a, SAC#01b (B12: Short Term DCB)
SO 002	Regional ATFCM shall validate iSMT in accordance with the applicable ATM constraints	OM1-a5	As above	SAC#01a, SAC#01b (B12: Short Term DCB)
SO 003	WOC shall submit iRMT in full consistency with the validated trajectory	OM1-a10	As above	SAC#01a, SAC#01b (B12: Short Term DCB) SAC#02a, SAC#02b (MF6.1 Crew/aircraft induced conflict) SAC#04a, SAC#04b (No AIM available) SAC#05a, SAC#05b (B10-B11: Traffic Planning & Synchronization)
SO 004	Regional ATFCM shall distribute the iSMT to Sub-regional/local ATFCM and ENR/APP ATS and update demand forecast accordingly	OM1-a6 OM1-a8	Adjust the Capacity (to the extent where it is available) to fit the predicted Demand Balance the predicted Demand against the available Capacity	SAC#01a, SAC#01b (B12: Short Term DCB)





ID	Safety Objective <i>(success approach)</i>	EATMA <i>OM- Activity or Flow</i>	Operational service	Related SAC# (AIM Barrier or Precursor)
SO 005	Sub-regional/local ATFCM shall receive iSMT and integrate it in the local impact assessment in view of appropriate Capacity adjustment and Demand balancing	OM1-a7	As above	SAC#01a, SAC#01b (B12: Short Term DCB)
SO 006	Regional ATFCM shall distribute the iRMT to Sub-regional/local ATFCM in view of appropriate Demand balancing against available Capacity and to ENR/APP ATS in view of the provision of ATC services	OM1-a11	Balance the predicted Demand against the available Capacity ATC Services	SAC#01a, SAC#01b (B12: Short Term DCB) SAC#03a, SAC#03b (MF7.1 ATC induced tactical conflict) SAC#04a, SAC#04b (No AIM available) SAC#05a, SAC#05b (B10-B11: Traffic Planning & Synchronization) SAC#06a, SAC#06b (B5-B9: Tactical Conflict Management)
SO 007	ENR/APP ATS shall receive timely and accurate iRMT consistent with the allocated ARES (if applicable) in view of the provision of ATC services	OM1-a9 OM2-a3	ATC Services	SAC#03a, SAC#03b (MF7.1 ATC induced tactical conflict) SAC#04a, SAC#04b (No AIM available) SAC#05a, SAC#05b (B10-B11: Traffic Planning & Synchronization) SAC#06a, SAC#06b (B5-B9: Tactical Conflict Management)
SO 008	WOC shall receive Surveillance Data in view of an enhanced mission monitoring (e.g. to detect possible deviations from the expected trajectory)	OM2-a7 OM2-f1 OM4-a6 OM4-f1 OM5-a6 OM5-f1	Flight plan revision (focusing on MT revision in execution phase)	SAC#02a, SAC#02b (MF6.1 Crew/aircraft induced conflict) SAC#06a, SAC#06b (B5-B9: Tactical Conflict Management)





ID	Safety Objective <i>(success approach)</i>	EATMA <i>OM- Activity or Flow</i>	Operational service	Related SAC# (AIM Barrier or Precursor)
SO 009	iRMTs revised as agreed shall be shared whilst keeping consistency among all the following actors: ENR/APP ATS, Regional & Local ATFCM, Adjacent ENR/APP ATS, WOC and Flight Deck	OM3-a4 OM3-f1 OM3-f2 OM3-f3 OM3-f4 OM3-f5 OM3-f6 OM3-f7 OM3-a7 OM3-a10 OM4-a1 OM4-a3 OM4-a7 OM5-a3 OM5-a9	Flight plan revision (focusing on MT revision in execution phase) ATC services	SAC#02a, SAC#02b (MF6.1 Crew/aircraft induced conflict) SAC#03a, SAC#03b (MF7.1 ATC induced tactical conflict) SAC#04a, SAC#04b (No AIM available) SAC#05a, SAC#05b (B10-B11: Traffic Planning & Synchronization) SAC#06a, SAC#06b (B5-B9: Tactical Conflict Management)
SO 010	Regional ATFCM shall update the traffic demand in line with the latest updates of the iRMT	OM3-a6 OM4-a5 OM5-a5	Balance the predicted Demand against the available Capacity	SAC#01a, SAC#01b (B12: Short Term DCB)

Table 3: List of Safety Objectives (success approach) for Normal Operations

3.7 Solution Operations under Abnormal Conditions

The purpose of this section is to assess, at operational level, the ability of PJ.07-03 supported by PJ.18-01a concepts to work through (robustness), or at least recover from (resilience) any abnormal conditions, external to the Functional System in the Solution scope, that might be encountered relatively infrequently.

3.7.1 Identification of Abnormal Conditions

The following list of abnormal conditions has been identified within the PJ.07-03 & PJ.18-01a HAZID (HAZard IDentification) workshop involving relevant operational and technical experts (see list of participants in Appendix B):

- ABN1. Unforeseen airspace closure (e.g. Volcanic Ash, nuclear cloud ...)
- ABN2. Severe weather conditions (CBs, turbulences, icing)
- ABN3. Unplanned Aerodrome closure
- ABN4. Unplanned limitation in ATC capacity (e.g. due to ATC system failure)
- ABN5. FDPS failure (in one ACC)
- ABN6. Degradations of NM system (IFPS)
- ABN7. Civil or Military aircraft emergency
- ABN8. Industrial actions, e.g. strikes

3.7.2 Potential Mitigations of Abnormal Conditions

The Table 4 below assesses, for each abnormal condition, the immediate effect on MIL AU operations and, when applicable, it identifies the possible mitigations of the safety consequence of the operational effect with a reference to the Solution Safety Objectives already defined at §3.6.2 or to the means available in the operational environment. When necessary additional mitigation means might be specified in terms of new Solution Safety Objectives. Note that this analysis will be further refined in the next safety assessment step (at SPR and TS level) by integrating the more in-depth knowledge at design level.

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SO xx]
	Unforeseen airspace closure (e.g. Volcanic Ash, nuclear cloud ...)	<p>For iSMTs or iRMTs not yet airborne: mission modification or cancellation (note that last briefing before take-off -1 h before take-off at the latest- accounts for last developments)</p> <p>For mission being already airborne: mission abortion or degradation of mission performance (e.g. due to need to circumnavigate, involving iRMT revision).</p>	<p>SO 001 (Modification or cancellation of iSMT)</p> <p>SO 003 (Modification or abortion through an iRMT revision)</p>

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SO xx]
	Severe weather conditions (e.g. CBs, turbulences, icing)	<p>For iSMTs or iRMTs not yet airborne: similar to above (mission modification or cancellation)</p> <p>For mission being already airborne: potential degradation in mission performance due to temporary need to deviate from iRMT</p>	<p>iSMT/iRMT revision (SO 001, SO 003)</p> <p>If sufficient time available, either FD or ATC will trigger an iRMT revision. In worst case, if no time available for trajectory revision, the Pilot will deviate temporarily from the iRMT (following ATC radar vectoring, or avoiding based on flight information service provided and/or on weather radar, whilst informing ATC)</p>
	Unplanned Aerodrome closure	<p>For iSMTs or iRMTs not yet airborne: (mission delay or cancellation)</p> <p>Destination change (use the alternate airport) managed through iRMT revision, with potential degradation in mission performance</p>	<p>SO 001 (Modification or cancellation of iSMT)</p> <p>SO 003 (iRMT revision)</p>
ABN4	Unplanned limitation in ATC capacity (e.g. due to ATC system failure – e.g. radar failure resulting in single radar coverage)	Mission proceeds as per the filed iOAT FPL.	<p>No iRMT revision needed</p> <p>If necessary, MIL control unit will take over the tactical control of the impacted flight (ensuring coordination with ATC as appropriate)</p>
ABN5	FDPS failure (in one ACC)	<p>In case of an iRMT revision, need to ensure coordination/distribution of information to adjacent ACCs via telephone, implying significant workload increase and loss of ATC capacity.</p> <p>No impact on the mission performance</p>	Coordination/distribution of iRMT revision information to adjacent ACCs via telephone

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SO xx]
ABN6	Degradation of NM system (IFPS)	In the short term (less than 3 hours): no significant effect (iOAT FPL have already been distributed to ACCs). If degradation persists: current contingency procedure i.e. individual passing of FPL to concerned ACCs. No impact on the mission performance	Waiting for restoration to file new iOAT FPLs Current contingency procedure i.e. individual passing of FPL to concerned ACCs.
ABN7	Civil or Military aircraft emergency	Induces a sector capacity problem (due to need for dedicated frequency and possibly dedicated controller, etc.) Might induce an iRMT revision (to change the trajectory) and at worst, mission abortion	SO 003 (Modification or abortion through an iRMT revision)
ABN8	Industrial actions, e.g. strikes	No impact on military flights. The MIL control system will take over	Not needed

Table 4: Additional Safety Objectives (success approach) for Abnormal Conditions

After having carried out the assessment for each abnormal condition, no new Safety Objectives have been identified.

3.8 Mitigation of System-generated Risks (failure approach)

This section addresses the Mission Trajectory Driven Processes in the case of internal failures of the Functional System within the Solution scope. Before any conclusion can be reached concerning the adequacy of the safety specification of the Solution at the OSED level, it is necessary to assess:

- the possible adverse effects that failures internal to the end-to-end Trajectory Definition System might have upon the provision of the relevant operational services described in section 3.6.1
- and to derive safety objectives (failure approach) to mitigate against these effects.

3.8.1 Identification and Analysis of System-generated Operational Hazards

The identification and analysis of the system-generated operational hazards has been performed based on the analysis of the OSED Operating Methods/Use cases (represented through the EATMA Process Models) and a HAZID (HAZard IDentification) workshop, involving relevant operational and technical experts.

The analysis has been done through the following steps:

- Identification of the relevant operational failure modes at the level of the activities and/or information flows in the EATMA Process Model of each Operating Method;

- Immediate operational effect assessment;
- Identification of the possible mitigations of the safety consequence of the operational effect.
- Different failure modes leading to similar operational effects and displaying same mitigations of the safety consequence have been consolidated into Operational Hazards (OH).
- Assessment of severity of the effect from the operational hazard occurrence accounting for the mitigations of the safety consequence, as per the relevant Severity Classification Scheme(s) from Guidance E.3 of Reference [3].

The detailed organisation, process description and outcomes of the PJ07-03 & PJ18-01 HAZID workshop are provided in Appendix B, which includes:

- the list of participants,
- the working table used for recording and structuring the relevant information for the hazard identification and analysis.

Table 5 represents an extract of the full HAZID shown in Appendix B and it contains only the system-generated operational hazards, i.e. consolidated failure modes of the Functional System which were concluded to have a safety impact. The operational hazards were derived at the level of the Operating Methods specified in OSED (see References [5]) and formalized via the EATMA process models (Appendix A.1). The table is organised as follows:

- Column 1 indicates the operational hazard reference,
- Column 2 provides the description of the operational hazard,
- Column 3 indicates the related functionality & performance Safety Objective in normal conditions -success approach (the operational hazard has been originated by a mode of failure to meet that safety objective),
- Column 4 summarizes the operational effects of the hazard,
- Column 5 indicates the mitigations of hazard effects, in terms of available protective means once the operational hazard occurred,
- Column 6 indicates the AIM-based severity applicable to the hazard.



ID	Operational Description	Hazard	Related SO (success approach)	Operational Effects	Mitigations of Effects	Severity (most probable effect)
HZ 01	Undetected incorrect traffic load data provided by Regional ATFCM to users (new contributor to already existing HZ-04 and similar to failure mode FLM-05 from Network Operations Safety Report NOSR v1.1 11/2017)		SO 001 SO 002 SO 003 SO 004 SO 005 SO 006 SO 010	If multiple flights are affected, impact on NMF performance, with potential for not timely detecting a Hotspot that might result in sector overload (in the context where sector capacity buffer will be reduced thanks to this Concept implementation)	Planning & tactical tasks under overload	MAC-SC3 IM=0.4 Minoring factor accounting for the lesser proportion of iOAT FPLs compared to civil FPLs
HZ 02	MIL flight inbound a sector with short notice (from adjacent sector or ARES)		SO 003 SO 006 SO 007 SO 009	The lack of an iRMT might not be systematically detected at the first contact with ATC (case of MIL aircraft entering controlled airspace without preliminary notification/coordination. If undetected, potential for conflict not timely detected by PLN ATCO)	Tactical conflict resolution	MAC-SC4b
HZ 03	ATFM measures not implemented or implemented partially by local ATFCM (new contributor to already existing HZ-05 from Network Operations Safety Report NOSR v1.1 11/2017)		SO 005	If multiple flights are affected, potential for not timely detecting a Hotspot that might result in sector overload (in the context where sector capacity buffer will be reduced thanks to this Concept implementation)	Planning & tactical tasks under overload	MAC-SC4b IM=10 Majoring factor accounting for the multiple flights affected



ID	Operational Description	Hazard	Related SO (success approach)	Operational Effects	Mitigations of Effects	Severity (most probable effect)
Hz 04	Conflict-inducing lateral deviation due to ground-airborne inconsistency	aircraft due to iRMT	SO 006 SO 007 SO 008 SO 009	<p>Potential for conflict not timely detected by PLN ATCO (either MIL aircraft inbound sector from adjacent sector or MIL aircraft leaving ARES), due to Aircraft lateral deviation at a waypoint</p> <p>Proposed Safety Requirement: the CDM process shall be designed such as to avoid iRMT discrepancy</p>	<p>Trajectory conformance monitoring tool (RAM/CLAM)</p> <p>Tactical conflict resolution</p>	MAC-SC4a
Hz 05	Uncoordinated ARES exit leading to separation infringement		SO 006 SO 007 SO 009	<p>If an iRMT inconsistency goes undetected, risk for tactical conflict between MIL aircraft exiting ARES and aircraft flying at ARES borders (not predictable based on flight plan info)</p> <p>In order to allow iRMT inconsistency detection and more generally to prevent lack of coordination,</p> <p>Proposed safety requirement: MIL Flight coordination and transfer of responsibility from one AoR to the other (i.e. ARES to ATC sector or ATC to ARES) shall be executed as a system to system exchange in accordance with established standards & regulations</p>	ATC Collision prevention (STCA)	MAC-SC3

Table 5: System-Generated Operational Hazards and Analysis

Note 1: Several Safety Requirements have been proposed during the HAZID workshop in order to limit the occurrence of the operational hazards. They have been provisionally recorded in the previous table, within the “Operational Effects” column and will be further re-conducted in the safety assessment at the logical design (SPR and TS) level (Section 4).

Note 2: The IM=10 stands for the value assumed for the Impact Modification factor that will be used for the allocation of the Safety Objective associated to the operational hazard. It allows to allocate a more stringent safety objective to hazards involving sector overload compared to hazards displaying same severity but involving only individual flights.

3.8.2 Derivation of Safety Objectives (integrity/reliability)

This section derives Safety Objectives (addressing integrity/reliability) to limit the frequency with which the system-generated hazards could be allowed to occur using the Risk Classification Scheme for AIM MAC En-Route & TMA operational environments (from Guidance E of Reference [3]).

The Safety Objectives associated to the operational hazards Hz 01 and Hz 03 (with sector overload as a potential effect) need:

- to be expressed “per sector operational hour”, whilst the unit for the maximum tolerable frequency of occurrence in the Risk Classification Scheme is “per flight hour”.
- to be computed whilst accounting for an Impact Modification factor (IM=10, which stands for the value that allows to allocate a more stringent safety objective to hazards involving sector overload compared to hazards displaying same severity but involving only individual flights. The value IM=10 has been assumed based on rough expert-based considerations on the acceptable frequency of occurrence of similar operational hazards in current operations)

Conversion from “per flight hour” to “per sector operational hour”:

For one hazard occurrence per hour, the affected traffic corresponds to those flight hours flown during one hour within the impacted area (which might be either a high density En Route sector or a high density terminal area sector experiencing overload). The value used in RTCA/EUROCAE Operational Safety Assessments (e.g. the ADS-B RAD) is an average of 6 flight hours controlled per sector hour³ for both the high density En Route sector or the high density terminal area sector.

³ The ADS-B-RAD and the Reference systems support the ATC Service in the following traffic densities:

- For a medium density TMA airspace (ENVT-1), an average of 6 flight hours controlled per sector hour and a maximum of 15 instantaneous aircraft count in a sector

- For a high density en-route airspace (ENVT-2), a maximum of 6 flight hours controlled per sector hour and a maximum of 20 instantaneous count aircraft in a sector

- For a high density TMA airspace (ENVT-3), an average of 6 flight hours controlled per sector hour and a maximum of 15 instantaneous aircraft count in a sector

Note: For medium density TMA airspace, the figure is a result from combining a sector capacity with average flight time in sectors related to medium-density operations,

e.g. 30 flights per hour sector capacity with an average 12 minute flight length in sector, or another example could be 36 flights per hour sector capacity with a 10 minute average flight length.

Note: For high density en-route airspace, the figure is a result from combining a sector capacity with average flight time in sector related to high-density operations,

e.g. 60 flights per hour sector capacity with an average 6 minute flight length in sector, or another example could be 45 flights per hour sector capacity with an 8 minute average flight length.

Note: High density TMA by its nature contains more and smaller sectors than in the medium density TMA albeit with the same sector traffic throughput (i.e. 6 flight hours per sector hour) and therefore is by definition more dense.

Illustration of SO computation

The computation of the Safety Objectives (performed in accordance with Guidance E of Reference [3]) is illustrated via the example for Hz 01 below:

Hz 01: Corrupted traffic load data provided to users due to iOAT FPLs missing or not updated

As Hz 01 has been allocated severity MAC-SC3 (to which corresponds an MTfO = 1E-04 per flight hour), the safety objective is:

$$SO_{101} = \frac{MTfO_{relevant_severity_class}}{N \times IM} = \frac{1E-04}{25 \times 0.4} = 1E-05 \text{ [per flight*hour]} = 1E-05 \times 6 \text{ [per sector}$$

operational hour]= **6E-05 [per sector operational hour]**

Where:

N= 25 = overall number of operational hazards for the severity SC3 in the Risk Classification Schemes associated to AIM MAC ER & TMA models⁴,

IM= 0.4 = the Impact Modification factor considered herein (see explanation above, second bullet under first paragraph of current sub-section)

Note that the computation of the hazards which effect concerns a single flight (Hz 02, Hz 04 and Hz 05) does not need the conversion into “per sector operational hour” and does not use an IM (IM=1). The Max Tolerable Frequency of Occurrence (MTfO) and the overall number of operational hazards per accident type (N) have been taken from the §E.2.3.3 of SRM Guidance E [3]) as follows: MTfO=1E-2 and N=100 for Hz 02 (MAC-SC4b); MTfO=1E-3 and N=30 for Hz 04 (MAC-SC4a); MTfO=1E-4 and N=25 for Hz 05 (MAC-SC3).

The consolidated list of the derived integrity/reliability Safety Objectives (failure approach) is provided in Table 6 below.

ID	Safety Objectives <i>(failure approach)</i>	Related Hazard	Severity & IM
SO 101	The likelihood of undetected incorrect traffic load data provided by Regional ATFCM to users shall be no more than 6e-5 per sector operational hour	Hz 01	MAC-SC3 IM=0.4
SO 102	The likelihood that MIL flight inbound a sector with short notice (from adjacent sector or ARES) shall be no more than 1e-4 per flight hour	Hz 02	MAC-SC4b

⁴ An updated value (100 instead of 30) has been used for the Number of hazards per Severity class and Accident type (Table 5 in §E.2.3.3 of SRM Guidance E [3]). The updated SRM Guidance will be available in October 2018 (for additional information, please address to SESAR 2020 Safety Community of Practice)



SO 103	The likelihood of corrupted traffic load data provided to users due to incorrect accommodation of correctly received iSMT in local ATFCM shall be no more than 6e-5 per sector operational hour	Hz 03	MAC-SC4b IM=10
SO 104	The likelihood that a conflict-inducing aircraft lateral deviation occurs due to ground-airborne iRMT inconsistency shall be no more than 3.3e-5 per flight hour	Hz 04	MAC-SC4a
SO 105	The likelihood of an uncoordinated ARES exit leading to separation infringement shall be no more than 4e-6 per flight hour	Hz 05	MAC-SC3

Table 6: Safety Objectives (integrity/reliability)

3.9 Impacts of Mission Trajectory Driven Processes Solution operations on adjacent airspace or on neighbouring ATM Systems

N/A

3.10 Achievability of the Safety Criteria – Safety validation objectives

As specified in the Safety Plan [4], safety evidence will be collected from the validation exercises planned as per the Validation Plan [8]. The safety-related outcomes of the validation exercises will feed the Safety Criteria and will be traced back to the safety validation objectives. Decision for deriving (or not) Safety Requirements will be taken from these results.

Note: Safety validation objectives were not defined for the V2 validation exercise held January 2018, given that the conducted RTS was of limited operational relevance for the safety aspects. With regards to the V3 validation exercises, Safety validation objectives were not defined for the exercise related to the planning phase held in May 2019, given that the conducted Shadow Mode simulation was of limited operational relevance for the safety aspects. The solution that completed V3 was focused only on the planning phase. Moreover, further V3 validation exercises (including those related to the execution phase and involving relevant safety aspects) necessary to achieve the full V3 maturity level, will be part of SESAR Wave 2 solution 40.

3.11 Validation & Verification of the Safety Specification

This section describes the processes by which safety objectives were derived as well as details of the competencies of the personnel involved.

A HAZID workshop was organised in order to support the validation of the Safety Criteria, the confirmation of functionality & performance SOs (normal and abnormal conditions) and the identification of the system-generated hazards for the concept.

A description of the HAZID process and participation (people involved and competencies) is provided in Appendix B.

4 Safe Design (SPR and TS level)

4.1 Scope

In the light of the maturity reached for the Solution at the end of SESAR Wave 1, which is V3 for the planning phase and initial V3 for the execution phase, the safety assessment has been conducted at the initial design level. That comes to derive the full set of safety requirements for the SPR-INTEROP/OSED but to perform only an initial derivation for the TS/IRS, limiting the latter to the collection of the technical mitigations resulting from the causal analysis of the operational hazards.

This section is intended to address the following activities:

- Description of the initial design level model of the end-to-end Solution ATM System - section 4.2
- Analysis of the operation of the initial design under normal operational conditions – section 0
- Analysis of the operation of the initial design under abnormal conditions of the Operational Environment - section 4.4
- Assessment of the adequacy of the initial design in the case of internal failures and mitigation of the System-generated hazards - section 4.5
- Justification that the Safety Criteria are capable of being satisfied in a typical implementation - section 4.6
- Realism of the initial design - section 4.7
- Validation & Verification of the Specification - section 4.8

4.2 The initial design level Model & Safety Requirements derivation – Normal Operational conditions

The initial design level Model in this context is a high-level architectural representation of the Solution System design that leaves the door open to multiple alternatives for the eventual physical implementation of that design. It describes the main human roles or tasks, machine-based functions and airspace structures and explains what each of those “actors” provides in terms of functionality and performance. The initial design model normally does not provide the detailed functional description and necessary logical interfaces between functions & functional blocks, that remain to be described in the refined design level model (the one where the achievement of full V3 (TRL6) maturity has to be verified which authorises then the transition to Industrialisation and Deployment).

4.2.1 Description of the initial design level Model

For those elements at V3 maturity level, the EATMA Operational activity models (NOV-5 diagram Operational activity model – see Appendix A.1) used by the solution to specify the operational and interoperability requirements have been also used for the safety assessment at the initial design level, and have been considered sufficient for the scope validated at V3/TRL6 level (planning phase).

In next phases of the V3 maturity level, the safety assessment at the refined design level will be supported by more detailed EATMA models like NSV-4 diagram, System Functionality and Flow model etc.

4.2.2 Task Analysis

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

PJ.07-03 did not produce such a Task Analysis. However, in order to complement the Safety Assessment, several HP-relevant inputs from the HP Assessment Report [9], and from internal meetings involving the Human Performance team have been taken into account for the derivation and agreement of the Safety Requirements.

4.2.3 Derivation of Safety Requirements (Functionality and Performance – success approach)

According to the SRM methodology, the derivation of the safety requirements (functionality and performance- success approach) should be performed starting from the Safety Objectives (success approach). This derivation must be supported by the relevant design models and driven by the mapping of each Safety Objective (success approach) to the ATM/ANS functional system design elements (technical, human and procedural) whilst focusing on those design elements which are modified or new.

In the specific case of PJ.07-03, the solution has already accomplished a significant part of the “success approach” as the derivation of the SPR-INTEROP/OSED requirements has been driven by a complete set of EATMA process models (NOV 5 diagrams). That systematic requirements derivation represents the assurance that the resulting set of requirements (operational, interoperability, and to some extent safety and performance as well) display a rather high degree of completeness, correctness and are provided with the appropriate rationale.

In that context, the work related to the safety requirements derivation at the initial design level has been re-deployed (compared to the SRM-proposed methodology) according to the method explained below.

A Causal Analysis has been performed in the first place (see 4.5.1).

This allowed to seek for the origin of the various failure causes, for each operational hazard, and to identify which are the SPR-INTEROP/OSED requirements (derived by the Project) with potential for generating such failure scenarios. In case such a requirement were not satisfied, that would contribute

to an operational hazard and consequently that requirement is in the SAFETY category, i.e. it is a Safety Requirement (functionality and Performance). In some occasions this analysis allowed to spot missing “success case” requirements, in which case they were derived as safety requirements and proposed for inclusion in the SPR-INTEROP/OSED or in the TS/IRS. The new derived safety requirements (i.e. which are added to those requirements already existing in the SPR-INTEROP/OSED when the safety assessment at the design level was initiated) are highlighted in bold characters across the entire safety assessment report.

The new derived “success approach” safety requirements and those already existing SPR-INTEROP/OSED requirements that have been identified in the SAFETY category have been further traced to the related operational hazards and ultimately consolidated in the Table 7 below (in the last column of the table the related success SO is indicated for traceability purposes). In the meantime, the category *SAFETY* has been input to the “Category” field in the SPR-INTEROP/OSED requirements from section 4 of the SPR-INTEROP/OSED document.

Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-OP02.0002	Situational awareness to the Downstream En-Route/Approach ATS shall be provided about any updates to iRMT	Hz 02 Hz 04 Hz 05	SO 007 SO 009
REQ-07.03-SPRINTEROP-OP02.0003	The En-Route/Approach ATS shall have a possibility to revise iRMT	Hz 01 Hz 04	SO 006 SO 009
REQ-07.03-SPRINTEROP-OP02.0006	The En-Route/Approach ATS shall receive from Regional ATFCM iSMT/iRMT data based on latest validated iOAT FPL information (including modification messages) in order to allocate and manage the trajectories within respective AoR in execution phase via SWIM technical profile	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-OP02.1001	The ATC shall receive, process and develop requested iMT including demanded ARES configuration	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-OP02.1002	The ATC shall receive, process and develop requested iMT including demanded ARES configuration as ad-hoc ASM scenario with predefined ID	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 007 SO 009



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-OP02.1003	The ATC shall receive, process and develop requested iMT including the ARES flexible parameters in iMT profile description	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-OP02.1004	The ATC shall receive, to process and develop requested iMT profile irrespective of the GAT or OAT segments	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-OP02.1005	The ATC shall provide arrangements for NSF with WOC (AU)	Hz 02 Hz 04	
REQ-07.03-SPRINTEROP-IO02.0007	En-Route / Approach ATS shall be connected to all relevant ATM Nodes for iRMT Revisions distribution information exchange	Hz 02	SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO02.0008	En-Route / Approach ATS shall be connected to all relevant ATM Nodes for iRMT Revisions distribution information exchange. For any possible updates ADEXP/OLDI standards are used	Hz 02	SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO02.0009	En-Route / Approach ATS shall be connected to all relevant ATM Nodes for iRMT Revisions distribution information exchange during execution phase. Possible updates through SWIM technical profile	Hz 02	SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO02.0010	En-Route / Approach ATS shall be connected to receive iOAT FPL Mission Trajectory Data (iSMT/iRMT) and modification messages from Regional ATFCM	Hz 01 Hz 02 Hz 04	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO02.0011	En-Route / Approach ATS shall be connected to receive iOAT FPL Mission Trajectory Data (iSMT/iRMT) and modification messages from Regional ATFCM using improved OAT Flight Plan format	Hz 01 Hz 02 Hz 04	SO 004 SO 006 SO 007 SO 009



PJ07
OAUO



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-IO02.0012	En-Route / Approach ATS shall be connected to receive iOAT FPL Mission Trajectory Data (iSMT/iRMT) and modification messages from Regional ATFCM via SWIM technical profile	Hz 01 Hz 02 Hz 04	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO02.0016	The En-Route/Approach ATS shall connect to relevant systems to exchange initial Reference Mission Trajectory data including updates and revisions	Hz 01 Hz 04	SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO02.0017	The En-Route/Approach ATS shall exchange initial Reference Mission Trajectory data including updates and revisions. During transition for any trajectory updates ADEXP/OLDI standards are used	Hz 04	SO 009
REQ-07.03-SPRINTEROP-IE02.0001	iSMT - (Reception of Improved OAT-FPL information) Issuer <ul style="list-style-type: none"> Regional ATFCM (NMOC/IFPS) Intended Addressees <ul style="list-style-type: none"> Relevant civil & military (ATM, ATC) entities Information Element <ul style="list-style-type: none"> ATM Constraints ATM Environment Special Events (iOAT-FPL) Interaction Rules and Policy <ul style="list-style-type: none"> N/A Content Type <ul style="list-style-type: none"> Data Periodicity <ul style="list-style-type: none"> 24/24 On Demand Safety Criticality <ul style="list-style-type: none"> severe Maximum Latency <ul style="list-style-type: none"> Minutes (seconds) 	Hz 01	SO 002 SO 004





Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-IE02.0002	iRMT (Update of filed iOAT FPL information)	Hz 02	SO 006
	Issuer <ul style="list-style-type: none"> • Regional ATFCM (NMOC/IFPS) Intended Addressees <ul style="list-style-type: none"> • Relevant civil & military (ATM, ATC) entities Information Element <ul style="list-style-type: none"> • ATM Constraints • ATM Environment • Special Events (iOAT-FPL) Interaction Rules and Policy <ul style="list-style-type: none"> • N/A Content Type <ul style="list-style-type: none"> • Data Periodicity <ul style="list-style-type: none"> • 24/24 • On Demand Safety Criticality <ul style="list-style-type: none"> • severe Maximum Latency <ul style="list-style-type: none"> • Seconds 	Hz 04	SO 007 SO 009
REQ-07.03-SPRINTEROP-IE02.0004	Send iRMT Revision Issuer <ul style="list-style-type: none"> • EN-Route/Approach ATS Intended Addressees <ul style="list-style-type: none"> • Flight Deck and Relevant civil & military (ATM, ATC, WOC, AD/C2) entities Information Element <ul style="list-style-type: none"> • iRMT Interaction Rules and Policy <ul style="list-style-type: none"> • N/A Content Type <ul style="list-style-type: none"> • Voice/Data Periodicity <ul style="list-style-type: none"> • 24/24 Safety Criticality <ul style="list-style-type: none"> • severe Maximum Latency <ul style="list-style-type: none"> • Seconds 	Hz 02 Hz 04	SO 007



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-OP03.1001	The Regional ATFCM shall process iOAT FPL and associated messages	Hz 01	SO 002SO 010
REQ-07.03-SPRINTEROP-OP03.1003	Regional ATFCM shall distribute all accepted iOAT FPLs and associated messages to all relevant civil and military entities in the IFPZ as today implemented for GAT FPLs	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-OP03.1004	Regional ATFCM shall apply ATM Network rules (e.g. RAD checking, AIP) to iOAT FPLs to validate their compliance with them within the IFPZ as today for GAT flights	Hz 01	SO 002
REQ-07.03-SPRINTEROP-OP03.1008	Regional ATFCM shall cross check that ARES data in iOAT FPL comply with ARES allocated via ASM process	Hz 01 Hz 02 Hz 04	SO 002
REQ-07.03-SPRINTEROP-IO03.1001	The Regional ATFCM shall provide interface for the data exchange of iOAT FPL and associated messages	Hz 01 Hz 02 Hz 04	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO03.1002	The Regional ATFCM shall process all standard data formats (ADEXP, XML) applicable to iOAT FPL and associated messages	Hz 01 Hz 02 Hz 04	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO03.1003	The Regional ATFCM shall exchange iOAT FPL and associated messages data via SWIM	Hz 01 Hz 02 Hz 04	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO03.1004	The Regional ATFCM shall provide interface to all AU for the iOAT FPL filing and submission	Hz 01 Hz 02	SO 001 SO 003



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-IO03.1005	The Regional ATFCM shall process all standard data formats (ADEXP, XML) applicable to iOAT FPL	Hz 01 Hz 02 Hz 04	SO 002 SO 004 SO 006 SO 009
REQ-07.03-SPRINTEROP-IO03.1006	Regional ATFCM shall ensure integration of iOAT FPL data for filing and submission via SWIM technical profile	Hz 01 Hz 02	SO 001 SO 003
REQ-07.03-SPRINTEROP-IO03.1007	Regional ATFCM shall provide interface for distribution of iOAT FPL and associated messages data alike for GAT FPL	Hz 01 Hz 02 Hz 04	SO 004 SO 006 SO 009
REQ-07.03-SPRINTEROP-IO03.1008	The Regional ATFCM shall distribute iOAT FPL and associated messages in standard data formats (ADEXP, XML)	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 009
REQ-07.03-SPRINTEROP-IO03.1009	The Regional ATFCM shall distribute iOAT FPL and associated messages in standard data formats (ADEXP, XML) through SWIM technical profile	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 009
REQ-07.03-SPRINTEROP-IO03.1010	Regional ATFCM shall provide interface for iMT data exchange between Regional and Sub-Regional/Local ATFCM	Hz 01 Hz 02	SO 004 SO 005 SO 006
REQ-07.03-SPRINTEROP-IO03.1011	The Regional ATFCM shall exchange iMT data in standard data formats (ADEXP, XML)	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 009
REQ-07.03-SPRINTEROP-IO03.1012	The Regional ATFCM shall exchange iMT data with Sub regional/national ATFCM through SWIM technical profile	Hz 01 Hz 02	SO 004 SO 005 SO 006
REQ-07.03-SPRINTEROP-IO03.1013	Regional ATFCM shall provide interface for data exchange between environmental data and flight plan data processing systems	Hz 01	SO 002



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-IO03.1014	The Regional ATFCM shall apply data standards for exchange between environmental data and flight plan data processing systems	Hz 01	SO 002
REQ-07.03-SPRINTEROP-IO03.1015	The Regional ATFCM shall ensure exchange of data between environmental data and flight plan data processing systems via SWIM	Hz 01	SO 002
REQ-07.03-SPRINTEROP-IO03.0004	Regional ATFCM shall be connected to the WOC to receive Mission Trajectory data and answer with validation status	Hz 01 Hz 02	SO 001 SO 002 SO 003 SO 009
REQ-07.03-SPRINTEROP-IO03.0005	The WOC shall exchange Mission Trajectory data with Regional ATFCM using the improved OAT Flight Plan format	Hz 01 Hz 02	SO 001 SO 003
REQ-07.03-SPRINTEROP-IO03.0006	The WOC shall exchange Mission Trajectory data with Regional ATFCM through SWIM technical profile	Hz 01 Hz 02	SO 001 SO 003
REQ-07.03-SPRINTEROP-IE03.0001	<p>Submission of iOATFPL</p> <p>Issuer</p> <ul style="list-style-type: none"> • WOC or ATC in case of FPL revision in execution <p>Intended Addressees</p> <ul style="list-style-type: none"> • Regional ATFCM <p>Information Element</p> <ul style="list-style-type: none"> • iOAT FPL <p>Interaction Rules and Policy</p> <ul style="list-style-type: none"> • N/A <p>Content Type</p> <ul style="list-style-type: none"> • Data <p>Periodicity</p> <ul style="list-style-type: none"> • 24/24 <p>Safety Criticality</p> <ul style="list-style-type: none"> • severe <p>Maximum Latency</p> <ul style="list-style-type: none"> • Seconds 	Hz 01 Hz 02	SO 001 SO 003



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-IE03.0003	Distribution of improved OAT FPL Issuer <ul style="list-style-type: none"> Regional ATFCM Intended Addressees <ul style="list-style-type: none"> En-Route/Approach ATS(civil&military) Information Element <ul style="list-style-type: none"> iOAT FPL Interaction Rules and Policy <ul style="list-style-type: none"> N/A Content Type <ul style="list-style-type: none"> Data Periodicity <ul style="list-style-type: none"> 24/24 Safety Criticality <ul style="list-style-type: none"> severe Maximum Latency <ul style="list-style-type: none"> Seconds 	Hz 01 Hz 02 Hz 04 Hz 05	SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-SF03.0003	iOAT FPLs shall be taken into account for Demand forecast prediction	Hz 01	SO 002 SO 004 SO 006 SO 010
REQ-07.03-SPRINTEROP-OP04.0004	The Flight Data Operator in the WOC shall submit the iSMT based on latest available Mission Trajectory data to the Regional ATFCM	Hz 01	SO 001
REQ-07.03-SPRINTEROP-OP04.0005	If changes to the content of a submitted initial Shared Mission Trajectory are needed, the Flight Data Operator shall submit updated initial Shared Mission Trajectory to Regional ATFCM	Hz 01	SO 001
REQ-07.03-SPRINTEROP-OP04.0006	If conditions for transition from initial Shared Mission Trajectory to initial Referenced Mission Trajectory are met, the Flight Data Operator in the WOC shall submit the initial Referenced Mission Trajectory to Regional ATFCM	Hz 01 Hz 02	SO 003



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-OP04.0011	If revision of an initial Referenced Mission Trajectory is needed, the Flight Data Operator in the WOC shall update the Mission Trajectory data	Hz 01 Hz 02	SO 003
REQ-07.03-SPRINTEROP-OP04.0012	The Flight Data Operator in the WOC shall submit the initial Referenced Mission Trajectory Revision Request based on latest available Mission Trajectory data to En-Route/Approach ATS	Hz 04	SO 003
REQ-07.03-SPRINTEROP-OP04.1002	The WOC shall be able to define the ARES configuration as ad hoc ASM scenario with pre-defined ID	Hz 01	SO 001 SO 003
REQ-07.03-SPRINTEROP-OP04.1003	The WOC shall be able to integrate the ARES flexible parameters in iMT profile description	Hz 01	SO 001 SO 003
REQ-07.03-SPRINTEROP-OP04.1004	The WOC shall be able to define the iMT profile irrespective of the GAT or OAT segments and submit it to Regional ATFCM	Hz 01 Hz 02	SO 001 SO 003
REQ-07.03-SPRINTEROP-OP04.1005	The WOC shall pre-validate filed iOAT FPL through the NM validation mechanism before final submission	Hz 01	SO 002
REQ-07.03-SPRINTEROP-IO04.0002	The WOC shall send Mission data update to the Flight Deck with standard phraseology	Hz 04	SO 009
REQ-07.03-SPRINTEROP-IO04.0003	The WOC shall send Mission data update to the Flight Deck via State AU internal communication means	Hz 04	SO 009
REQ-07.03-SPRINTEROP-IO04.0007	The WOC shall be connected to En-Route/Approach ATS to exchange initial Referenced Mission Trajectory data during execution phase	Hz 02	SO 003 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO04.0008	The WOC shall exchange initial Referenced Mission Trajectory data with En-Route/Approach ATS using ADEXP/OLDI format	Hz 02	SO 003 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO04.0009	The WOC shall exchange initial Referenced Mission Trajectory data with En-Route/Approach ATS via AFTN	Hz 02	SO 003 SO 007 SO 009

Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-IO04.0018	The WOC shall be connected to Regional ATFCM to exchange Mission Trajectory data	Hz 01	SO 001 SO 003
REQ-07.03-SPRINTEROP-IO04.0019	The WOC shall exchange Mission Trajectory data with Regional ATFCM using the iOAT FPL format	Hz 01	SO 001 SO 003
REQ-07.03-SPRINTEROP-IO04.0020	The WOC shall exchange Mission Trajectory data with Regional ATFCM through SWIM technical profile	Hz 01	SO 001 SO 003
REQ-07.03-SPRINTEROP-IE04.0005	<p>Send iRMT</p> <p>Issuer</p> <ul style="list-style-type: none"> • WOC <p>Intended Addressees</p> <ul style="list-style-type: none"> • Regional ATFCM <p>Information Element</p> <ul style="list-style-type: none"> • iRMT <p>Interaction Rules and Policy</p> <ul style="list-style-type: none"> • N/A <p>Content Type</p> <ul style="list-style-type: none"> • Data <p>Periodicity</p> <ul style="list-style-type: none"> • On Demand <p>Safety Criticality</p> <ul style="list-style-type: none"> • Major <p>Maximum Latency</p> <ul style="list-style-type: none"> • Minutes 	Hz 02	SO 003

Table 7: Derivation of Safety Requirements (functionality and performance) from Safety Objectives

4.3 Analysis of the initial design level Model – Normal Operational Conditions

This section is concerned with ensuring that the design model is complete, correct and internally coherent with respect to the Safety Requirements (success approach) derived for the normal operating conditions that were used to develop the corresponding Safety Objectives (success approach) in section 3.6.2.

This involves an analysis aimed at proving the Safety Requirements (Functionality and Performance) from three perspectives:

- a static view of the System behaviour using a Thread Analysis technique, as described in sections 4.3.1 and 0,
- check that the System design operates in a way that does not have a negative effect on the operation of related ground-based and airborne safety nets, through static analysis and simulation - see section 4.3.3
- a dynamic view of the System behaviour using in particular Real-time simulations - see section 0

4.3.1 Scenarios for Normal Operations

In addition to the EATMA process Models shown in Appendix A and used in sections 3.6 (for SO derivation in success approach) and 4.2 (for SR derivation) the following scenario has been considered as safety relevant and consequently analysed in the next sub-section 4.3.2:

- ARES is published in the eAUP/eUUP for a defined period of time (e.g. from 09:00 to 17:00 hours)
- iOAT FPL information shows that the ARES will be really occupied for a shorter period of time (e.g. from 09:30 to 12:30 hours)
- ATC makes use of the time occupancy information included in the iOAT FPL and tactically makes use of ARES airspace in collaboration with AMC during the periods where no iOAT flights are expected to be inside the ARES.
- ATC receives a new iOAT FPL showing an updated occupancy of the ARES between 14:00 and 17 hours.
- ATC system notifies automatically to ATCO about ARES activation 15 minutes prior IOAT flight entry based on the iOAT FPL information.

4.3.2 Thread Analysis of the SPR-level Model – Normal Operations

The analysis of the above scenario does not justify the effort for a Thread Analysis.

The scenario described in the previous sub-section is assessed from a safety point of view (with regards to the impact that this scenario might have on the planning phase (leading to overloads) and in the tactical phase) below:

- With regards to the impact on the planning phase, INAP will work with the eAUP/eUUP information (considering the ARES activation for the whole period, from 09:00 to 17:00 in the example), and it will not take into account the periods where the ARES is temporarily deactivated, so no safety impact related to DCB has been identified.
- With regards to the impact on the tactical phase, ATC will know that the ARES needs to be reactivated thanks to the information included in the iOAT FPL as soon as it becomes available and consequently ATC will clear the area before ARES reactivation (as per current operations). Consequently, no safety impact related to the change has been identified.

4.3.3 Effects on Safety Nets – Normal Operational Conditions

This is about checking that the Solution System operates in a way that does not have a negative effect on the operation of related ground-based and airborne safety nets.

The safety nets relevant for the operational environment under consideration (ENR and TMA airspace) are STCA, ACAS and APW.

None of these safety nets make use of the planned aircraft trajectory, thus there is no foreseen impact from the initial mission trajectory iMT integration into ATM network operations.

4.3.4 Dynamic Analysis of the initial design level Model – Normal Operational Conditions

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

4.3.5 Additional Safety Requirements (functionality and performance) – Normal Operational Conditions

Considering the information included in the previous sub-sections, no additional Safety Requirements (Functionality and Performance) have been found.

4.4 Analysis of the SPR-level Model – Abnormal Operational Conditions

This section is aimed at ensuring that the SPR-level Design is complete, correct and internally coherent with respect to the Safety Requirements (Functionality and Performance) derived for the abnormal operating conditions.

No Safety Objective for Abnormal Conditions has been identified at §3.7.2, consequently no Safety Requirements has been further derived at the design level.

4.5 Design Analysis – Case of Internal System Failures

The objective of this analysis consists in determining how the ATM/ANS functional system architecture (encompassing people, procedures, airspace design, equipment) designed for the Mission Trajectory Driven Processes can be made acceptably safe in presence of internal functional system failures. The method consists in apportioning the Safety Objectives derived from each operational hazard into Safety Requirements for the functional system elements, driven by the analysis of the hazard causes.

According to the SRM methodology, the following main steps need to be conducted:

- Perform a causal analysis for each of the operational hazards identified,
- Identify and address as appropriate the potential common cause failures (affecting multiple operational hazards)
- Derive safety requirements in order to formalize the mitigations for reducing the likelihood that specific failures would propagate up to the operational hazard
- Set safety requirements (integrity/reliability) to limit the frequency with which each HW equipment failure could be allowed to occur.

4.5.1 Causal Analysis

The purpose of the causal analysis is to develop the risk mitigation strategy through the identification of all possible causes of the operational hazards. This way it will be possible to identify the corresponding Safety Requirements allowing to meet the Safety Objective of the Operational Hazard under consideration.

For each system-generated hazard (see chapter 3.8.1), a top-down identification of internal system failures that could cause the hazard was conducted.

This analysis has been conducted and recorded for each operational hazard in a causal analysis-dedicated table (see Table 8 as an example). The causal analysis has been initiated from the failure modes already identified as causing operational hazards during the HAZID Workshop (held at Prague Airport on 5th and 6th of March 2018 - see **Error! Reference source not found.**). The causes for operational hazards are included in the Column 1 of the causal analysis table.

Then, for each cause of operational hazard failure, the origins have been identified in terms of which were the SPR-INTEROP/OSED requirements (derived by the Project) with potential for generating such failures. In case such requirements were not satisfied, that would contribute to an operational hazard (and consequently that requirement is in the SAFETY category -i.e. it is a Safety Requirement-success approach that is also captured for being included in §4.2.3-). The causes' origins, in terms of contributing SPR-INTEROP/OSED requirements, are included in the Column 2 of the causal analysis table. In addition to the analysis of the SPR-INTEROP/OSED requirements already defined by the Project, the use cases description from the OSED and the available EATMA models (NOV-5: Operational activity models) have been used in order to identify any additional potential failure causes. That was performed through checking for elements of the change represented by the Solution that have not been sufficiently captured by the existing SPR-INTEROP/OSED requirements and that could have a safety contribution. If such element were identified, coordination with the Project OSED and TS teams was initiated in order to create the adequate Safety Requirement-success approach.

Based on the understanding of the potential causes for the operational hazard, the mitigations allowing to limit the occurrence of the cause or its propagation up to the occurrence of the operational hazard have been identified from the existing set of SPR-INTEROP/OSED requirements and have been allocated the category Safety. In case those mitigations were judged insufficient with regards to their efficiency, new mitigations have been defined and formalized as new safety requirements (proposed to be added to the existing set of SPR-INTEROP/OSED and TS requirements).

All the mitigations identified (both the new and the already existing ones) have been consolidated in the table from section 4.5.3.



4.5.1.1 Hz 01: Undetected incorrect traffic load data provided by Regional ATFCM to users

(Operational hazard already existing in baseline operations- see NOSR Hz-04, failure mode FLM-05; the PJ07-03 design changes are expected to introduce new hazard causes)

<i>Severity Class</i>	SC-4b	<i>IM factor</i>	0.4
<i>Safety Objective</i>	The likelihood of undetected incorrect traffic load data provided by Regional ATFCM to users shall be no more than 6e-5 per sector operational hour		

Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
WOC operator fails to timely submit iSMT (or re-submit, following NM rejection) for multiple iOAT flights	REQ-07.03-SPRINTEROP-OP04.0004 REQ-07.03-SPRINTEROP-OP04.0005	Current mitigation applies (case of nominal MIL flights that are scheduled): <ul style="list-style-type: none"> the time limit parameter for iSMT submission applies as for the legacy IFPS system (for current FPLs) if the time limit parameter is not respected, the iSMT will be rejected as per the legacy IFPS system procedures (for current FPLs)
Undetected WOC system or connection failure resulting in multiple iSMT not generated or not submitted or not re-submitted to NM	REQ-07.03-SPRINTEROP-IO03.1004 REQ-07.03-SPRINTEROP-IO03.1006 REQ-07.03-SPRINTEROP-IO03.0004 REQ-07.03-SPRINTEROP-IO03.0005 REQ-07.03-SPRINTEROP-IO03.0006 REQ-07.03-SPRINTEROP-IE03.0001 REQ-07.03-SPRINTEROP-IO04.0018 REQ-07.03-SPRINTEROP-IO04.0019 REQ-07.03-SPRINTEROP-IO04.0020	<p>REQ-07.03-SPRINTEROP-SF04.0001: In case of WOC system or connection failure preventing from iOAT FPL filing/updating, WOC operator shall file or update iOAT FPL by alternative means (e.g. phone, fax, mail etc.)</p> <p>REQ-07.03-SPRINTEROP-SF04.0002: WOC shall be alerted via a lack of acknowledgement message in case the submitted iSMT/iRMT has not been received by the Regional ATFCM system</p>



Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
<p>WOC operator fails to submit or submits late iRMT for multiple iOAT flights (updates of iSMT or last minute filing)</p>	<p>REQ-07.03-SPRINTEROP-OP04.0006 REQ-07.03-SPRINTEROP-OP04.0011</p>	<p>Current mitigation applies (case of nominal MIL flights that are scheduled):</p> <ul style="list-style-type: none"> • the time limit parameter for iRMT submission applies as for the legacy IFPS system (for current FPLs) • if the time limit parameter is not respected, the iRMT will be rejected as per the legacy IFPS system procedures (for current FPLs)
<p>Undetected WOC system or connection failure resulting in multiple iRMT not submitted or lately submitted to NM</p>	<p>REQ-07.03-SPRINTEROP-IO03.1004 REQ-07.03-SPRINTEROP-IO03.1006 REQ-07.03-SPRINTEROP-IO03.0004 REQ-07.03-SPRINTEROP-IO03.0005 REQ-07.03-SPRINTEROP-IO03.0006 REQ-07.03-SPRINTEROP-IE03.0001 REQ-07.03-SPRINTEROP-IO04.0018 REQ-07.03-SPRINTEROP-IO04.0019 REQ-07.03-SPRINTEROP-IO04.0020</p>	<p>REQ-07.03-SPRINTEROP-SF04.0001 REQ-07.03-SPRINTEROP-SF04.0002</p>





Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
NM (IFPS) system failure resulting in not detecting or not rejecting invalid iSMT	REQ-07.03-SPRINTEROP-OP03.1001 REQ-07.03-SPRINTEROP-OP03.1004 REQ-07.03-SPRINTEROP-OP03.1008 REQ-07.03-SPRINTEROP-IO03.1013 REQ-07.03-SPRINTEROP-IO03.1014 REQ-07.03-SPRINTEROP-IO03.1015 REQ-07.03-SPRINTEROP-OP04.1002 REQ-07.03-SPRINTEROP-OP04.1003 REQ-07.03-SPRINTEROP-OP04.1004 REQ-07.03-SPRINTEROP-OP04.1005	SR_TS_001: Adequate SW assurance shall be ensured for the IFPS reception, processing & validation of the iSMT/iRMT by NM system
NM (IFPS) system failure resulting in iSMT not published/distributed	REQ-07.03-SPRINTEROP-IO02.0010 REQ-07.03-SPRINTEROP-IO02.0011 REQ-07.03-SPRINTEROP-IO02.0012 REQ-07.03-SPRINTEROP-IE02.0001 REQ-07.03-SPRINTEROP-OP03.1003 REQ-07.03-SPRINTEROP-IO03.1001 REQ-07.03-SPRINTEROP-IO03.1002	REQ-07.03-SPRINTEROP-SF03.0001: Regional ATFCM operator shall be alerted in case of connection failure with the relevant entities SR_TS_002: Adequate SW assurance shall be ensured for the distribution of the iSMT/iRMT





Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
	REQ-07.03-SPRINTEROP-IO03.1003 REQ-07.03-SPRINTEROP-IO03.1005 REQ-07.03-SPRINTEROP-IO03.1007 REQ-07.03-SPRINTEROP-IO03.1008 REQ-07.03-SPRINTEROP-IO03.1009 REQ-07.03-SPRINTEROP-IO03.1010 REQ-07.03-SPRINTEROP-IO03.1011 REQ-07.03-SPRINTEROP-IO03.1012 REQ-07.03-SPRINTEROP-IE03.0003	
NM system error resulting in Demand forecast not enriched and published (based on iSMT)	REQ-07.03-SPRINTEROP-SF03.0003: iOAT FPLs shall be taken into account for Demand forecast prediction	SR_TS_003: Adequate SW assurance shall be ensured for the demand forecast computation accounting for the iSMT/iRMT
Local ATFCM system failure leading to iSMT not received	REQ-07.03-SPRINTEROP-IE02.0001	SR_TS_007: Adequate SW assurance shall be ensured for the reception and processing of the iSMT/iRMT by the Local ATFCM system





Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
ATC system failure leading to iSMT not received	REQ-07.03-SPRINTEROP-OP02.0006 REQ-07.03-SPRINTEROP-OP02.1001 REQ-07.03-SPRINTEROP-OP02.1002 REQ-07.03-SPRINTEROP-OP02.1003 REQ-07.03-SPRINTEROP-OP02.1004 REQ-07.03-SPRINTEROP-IO02.0010 REQ-07.03-SPRINTEROP-IO02.0011 REQ-07.03-SPRINTEROP-IO02.0012 REQ-07.03-SPRINTEROP-IE02.0001	SR_TS_004: Adequate SW assurance shall be ensured for the reception, update, processing and distribution of the iSMT/iRMT by the ATC system
NM system error resulting in wrong or inaccurate iSMT received by Local ATFCM	REQ-07.03-SPRINTEROP-OP03.1003 REQ-07.03-SPRINTEROP-IO03.1001 REQ-07.03-SPRINTEROP-IO03.1002 REQ-07.03-SPRINTEROP-IO03.1003 REQ-07.03-SPRINTEROP-IO03.1005 REQ-07.03-SPRINTEROP-IO03.1007 REQ-07.03-SPRINTEROP-IO03.1008 REQ-07.03-SPRINTEROP-IO03.1009 REQ-07.03-SPRINTEROP-IO03.1010 REQ-07.03-SPRINTEROP-IO03.1011 REQ-07.03-SPRINTEROP-IO03.1012 REQ-07.03-SPRINTEROP-IE03.0003	SR_TS_002





Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
NM system error resulting in wrong or inaccurate iSMT received by ATC	REQ-07.03-SPRINTEROP-IO02.0010 REQ-07.03-SPRINTEROP-IO02.0011 REQ-07.03-SPRINTEROP-IO02.0012 REQ-07.03-SPRINTEROP-IE02.0001 REQ-07.03-SPRINTEROP-OP03.1003 REQ-07.03-SPRINTEROP-IO03.1001 REQ-07.03-SPRINTEROP-IO03.1002 REQ-07.03-SPRINTEROP-IO03.1003 REQ-07.03-SPRINTEROP-IO03.1005 REQ-07.03-SPRINTEROP-IO03.1007 REQ-07.03-SPRINTEROP-IO03.1008 REQ-07.03-SPRINTEROP-IO03.1009 REQ-07.03-SPRINTEROP-IO03.1011 REQ-07.03-SPRINTEROP-IE03.0003	SR_TS_002
Local ATFCM system error resulting in wrong or inaccurate iSTM received by Local ATFCM		SR_TS_007





Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
ATC system error resulting in wrong or inaccurate iSMT received by ATC	REQ-07.03-SPRINTEROP-OP02.0006 REQ-07.03-SPRINTEROP-OP02.1001 REQ-07.03-SPRINTEROP-OP02.1002 REQ-07.03-SPRINTEROP-OP02.1003 REQ-07.03-SPRINTEROP-OP02.1004 REQ-07.03-SPRINTEROP-IO02.0010 REQ-07.03-SPRINTEROP-IO02.0011 REQ-07.03-SPRINTEROP-IO02.0012	SR_TS_004
NM (IFPS) system error resulting in iRMT not distributed to local ATFCM	REQ-07.03-SPRINTEROP-OP03.1003 REQ-07.03-SPRINTEROP-IO03.1001 REQ-07.03-SPRINTEROP-IO03.1002 REQ-07.03-SPRINTEROP-IO03.1003 REQ-07.03-SPRINTEROP-IO03.1005 REQ-07.03-SPRINTEROP-IO03.1007 REQ-07.03-SPRINTEROP-IO03.1008 REQ-07.03-SPRINTEROP-IO03.1009 REQ-07.03-SPRINTEROP-IO03.1010 REQ-07.03-SPRINTEROP-IO03.1011 REQ-07.03-SPRINTEROP-IO03.1012 REQ-07.03-SPRINTEROP-IE03.0003	REQ-07.03-SPRINTEROP-SF03.0001 SR_TS_002





Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
NM system error resulting in updated iRMT not received	REQ-07.03-SPRINTEROP-IO03.1001 REQ-07.03-SPRINTEROP-IO03.1004 REQ-07.03-SPRINTEROP-IO03.1011	REQ-07.03-SPRINTEROP-SF03.0001 SR_TS_001
ATC system error resulting in IRMT update not provided to NM	REQ-07.03-SPRINTEROP-IO02.0016 REQ-07.03-SPRINTEROP-IO02.0017 REQ-07.03-SPRINTEROP-IE02.0004 REQ-07.03-SPRINTEROP-IE03.0001	SR_TS_004
ATCO fails to update iRMT information	REQ-07.03-SPRINTEROP-OP02.0003	REQ-07.03-SPRINTEROP-SF02.0001: ATCO procedures shall reflect the proper management of the iRMT REQ-07.03-SPRINTEROP-SF02.0002: ATCO shall be properly trained in the management of the iRMT

Table 8 Causal Analysis for Hazard 01



4.5.1.2 Hz 02: MIL flight inbound a sector with short notice (from adjacent sector)

(Operational hazard already existing in baseline operations; the PJ07-03 design changes are expected to introduce new hazard causes)

<i>Severity Class</i>	SC-4b	<i>IM factor</i>	1
<i>Safety Objective</i>	The likelihood that MIL flight inbounds a sector with short notice (from adjacent sector or ARES) shall be no more than 1e-4 per sector operational hour		

Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
WOC operator fails to submit iRMT or fails to resubmit the updated iRMT	REQ-07.03-SPRINTEROP-OP02.1005 REQ-07.03-SPRINTEROP-OP04.0006 REQ-07.03-SPRINTEROP-OP04.0011	Safety Issue I001: To clarify system design & procedures such as to ensure that a mission will not fly without iRMT
Undetected WOC system or connection failure resulting in iRMT not generated or not submitted to NM	REQ-07.03-SPRINTEROP-IO03.1004 REQ-07.03-SPRINTEROP-IO03.1006 REQ-07.03-SPRINTEROP-IO03.0004 REQ-07.03-SPRINTEROP-IO03.0005 REQ-07.03-SPRINTEROP-IO03.0006 REQ-07.03-SPRINTEROP-IE03.0001 REQ-07.03-SPRINTEROP-OP04.1004 REQ-07.03-SPRINTEROP-IO04.0007 REQ-07.03-SPRINTEROP-IO04.0008 REQ-07.03-SPRINTEROP-IO04.0009 REQ-07.03-SPRINTEROP-IE04.0005	REQ-07.03-SPRINTEROP-OP03.1002: Regional ATFCM shall provide the same options for filing and submission of iOAT FPL as for civil GAT FPL REQ-07.03-SPRINTEROP-SC04.0003: The supporting IT infrastructure SWIM and PENS shall transfer Flight Plan data without error REQ-07.03-SPRINTEROP-SF04.0001: In case of WOC system or connection failure preventing from iOAT FPL filing/updating, WOC operator shall file or update iOAT FPL by alternative means (e.g. phone, fax, mail etc.) Safety Assumption A001: As per current operations, WOC is alerted via a lack of acknowledgement message in case the submitted iOAT FPL has not been received by the Regional ATFCM system



Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
NM (IFPS) system error resulting in iRMT not published/distributed	REQ-07.03-SPRINTEROP-IE02.0002 REQ-07.03-SPRINTEROP-OP03.1003 REQ-07.03-SPRINTEROP-IO03.1001 REQ-07.03-SPRINTEROP-IO03.1002 REQ-07.03-SPRINTEROP-IO03.1003 REQ-07.03-SPRINTEROP-IO03.1005 REQ-07.03-SPRINTEROP-IO03.1007 REQ-07.03-SPRINTEROP-IO03.1008 REQ-07.03-SPRINTEROP-IO03.1009 REQ-07.03-SPRINTEROP-IO03.1010 REQ-07.03-SPRINTEROP-IO03.1011 REQ-07.03-SPRINTEROP-IO03.1012 REQ-07.03-SPRINTEROP-IE03.0003	<p>SR_TS_002: Adequate SW assurance shall be ensured for the distribution of the iSMT/iRMT</p> <p>Current mitigation: Reception of trajectory information via advanced boundary information (OLDI message) from adjacent ACC</p>





Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
ATC system error resulting in iRMT not received	REQ-07.03-SPRINTEROP-OP02.0002	<p>SR_TS_004: Adequate SW assurance shall be ensured for the reception, update, processing and distribution of the iSMT/iRMT by the ATC system</p> <p>Current mitigation, valid only after the moment of ABI distribution: Reception of trajectory information via advanced boundary information (ABI OLDI message, before the activation message) from adjacent ACC</p> <p>Other current mitigation: The systematic reception by NM of e.g. CPR data, AFP (ATC FPL proposal) allows to mitigate the lack or inaccurate information distributed before</p>
	REQ-07.03-SPRINTEROP-OP02.0006	
	REQ-07.03-SPRINTEROP-OP02.1001	
	REQ-07.03-SPRINTEROP-OP02.1002	
	REQ-07.03-SPRINTEROP-OP02.1003	
	REQ-07.03-SPRINTEROP-OP02.1004	
	REQ-07.03-SPRINTEROP-IO02.0007	
	REQ-07.03-SPRINTEROP-IO02.0008	
	REQ-07.03-SPRINTEROP-IO02.0009	
	REQ-07.03-SPRINTEROP-IO02.0010	
	REQ-07.03-SPRINTEROP-IO02.0011	
	REQ-07.03-SPRINTEROP-IO02.0012	
	REQ-07.03-SPRINTEROP-IE02.0002	
	REQ-07.03-SPRINTEROP-IE02.0004	





Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
NM (IFPS) system error resulting in inaccurate or wrong iRMT published/distributed	REQ-07.03-SPRINTEROP-IO02.0010	In order to mitigate the iRMT mismatch with regards to the sectorisation: SR_TS_006: ATC system jointly with ASM system shall be able to identify any inaccurate iRMT distribution within the ATC system including the appropriate activated/deactivated ARES entry and exit points In order to mitigate the inconsistency between onboard and ground iRMT information: <ul style="list-style-type: none"> • as per current operations, the conformance monitoring function (where available) SR_TS_001: Adequate SW assurance shall be ensured for the IFPS reception, processing & validation of the iSMT/iRMT by NM system SR_TS_002
	REQ-07.03-SPRINTEROP-IO02.0011	
	REQ-07.03-SPRINTEROP-IO02.0012	
	REQ-07.03-SPRINTEROP-IE02.0002	
	REQ-07.03-SPRINTEROP-OP03.1003	
	REQ-07.03-SPRINTEROP-OP03.1008	
	REQ-07.03-SPRINTEROP-IO03.1001	
	REQ-07.03-SPRINTEROP-IO03.1002	
	REQ-07.03-SPRINTEROP-IO03.1003	
	REQ-07.03-SPRINTEROP-IO03.1005	
	REQ-07.03-SPRINTEROP-IO03.1007	
	REQ-07.03-SPRINTEROP-IO03.1008	
	REQ-07.03-SPRINTEROP-IO03.1009	
	REQ-07.03-SPRINTEROP-IO03.1010	
	REQ-07.03-SPRINTEROP-IO03.1011	
	REQ-07.03-SPRINTEROP-IO03.1012	
REQ-07.03-SPRINTEROP-IE03.0003		





Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
ATC system error resulting in inaccurate or wrong iRMT received by ATC	REQ-07.03-SPRINTEROP-OP02.0002 REQ-07.03-SPRINTEROP-OP02.0006 REQ-07.03-SPRINTEROP-OP02.1001 REQ-07.03-SPRINTEROP-OP02.1002 REQ-07.03-SPRINTEROP-OP02.1003 REQ-07.03-SPRINTEROP-OP02.1004	<p>REQ-07.03-SPRINTEROP-SF02.0003: Mission trajectory coordination and transfer of responsibility from one AoR to the other (i.e. ARES to ATC sector or ATC to ARES) shall be executed as a system to system –supported exchange in accordance with established standards & regulations (SYSCO)</p> <p>SR_TS_004: Adequate SW assurance shall be ensured for the reception, update, processing and distribution of the iSMT/iRMT by the ATC system</p>
ATC system error resulting in iRMT not timely displayed to PLN ATCO		<p>REQ-07.03-SPRINTEROP-SF02.0003</p> <p>SR_TS_004</p>

Table 9 Causal Analysis for Hazard 02



4.5.1.3 Hz 03: ATFCM measures not implemented or implemented partially by local ATFCM

(Operational hazard already existing in baseline operations- see NOSR Hz-05; the PJ07-03 design changes are expected to introduce new hazard causes)

<i>Severity Class</i>	SC-4b	<i>IM factor</i>	10
<i>Safety Objective</i>	The likelihood of corrupted traffic load data provided to users due to incorrect accommodation of correctly received iSMT in local ATFCM shall be no more than 6e-5 per sector operational hour		

Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
Local ATFCM fails to assess the local impact of multiple iSMT		REQ-07.03-SPRINTEROP-SF03.0002: Local ATFCM actor shall be trained in the proper impact assessment of the mission trajectories
Local ATFCM system error resulting in multiple iSMT local impact not assessed		SR_TS_007: Adequate SW assurance shall be ensured for the reception and processing of the iSMT/iRMT by the Local ATFCM system

Table 10 Causal Analysis for Hazard 03





4.5.1.4 Hz 04: Conflict-inducing lateral deviation due to ground-airborne iRMT inconsistency

(Operational hazard already existing in baseline operations; the PJ07-03 design changes are expected to introduce new hazard causes)

<i>Severity Class</i>	SC-4a	<i>IM factor</i>	1
<i>Safety Objective</i>	The likelihood that a conflict-inducing aircraft lateral deviation occurs due to ground-airborne iRMT inconsistency shall be no more than 3.3e-5 per sector operational hour		

Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
NM system error resulting in inaccurate or wrong iRMT published/distributed	REQ-07.03-SPRINTEROP-IO02.0010	In order to mitigate the inconsistency between onboard and ground iRMT information: <ul style="list-style-type: none"> as per current operations, the conformance monitoring function (where available) SR_TS_001: Adequate SW assurance shall be ensured for the IFPS reception, processing & validation of the iSMT/iRMT by NM system SR_TS_002: Adequate SW assurance shall be ensured for the distribution of the iSMT/iRMT
	REQ-07.03-SPRINTEROP-IO02.0011	
	REQ-07.03-SPRINTEROP-IO02.0012	
	REQ-07.03-SPRINTEROP-IE02.0002	
	REQ-07.03-SPRINTEROP-OP03.1003	
	REQ-07.03-SPRINTEROP-OP03.1008	
	REQ-07.03-SPRINTEROP-IO03.1001	
	REQ-07.03-SPRINTEROP-IO03.1002	
	REQ-07.03-SPRINTEROP-IO03.1003	
	REQ-07.03-SPRINTEROP-IO03.1005	
	REQ-07.03-SPRINTEROP-IO03.1007	
	REQ-07.03-SPRINTEROP-IO03.1008	
	REQ-07.03-SPRINTEROP-IO03.1009	
	REQ-07.03-SPRINTEROP-IO03.1011	
REQ-07.03-SPRINTEROP-IE03.0003		





Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
ATC system error resulting in inaccurate or wrong iRMT received by ATC	REQ-07.03-SPRINTEROP-OP02.0006 REQ-07.03-SPRINTEROP-OP02.1001 REQ-07.03-SPRINTEROP-OP02.1002 REQ-07.03-SPRINTEROP-OP02.1003 REQ-07.03-SPRINTEROP-OP02.1004 REQ-07.03-SPRINTEROP-IO02.0010 REQ-07.03-SPRINTEROP-IO02.0011 REQ-07.03-SPRINTEROP-IO02.0012	<p>REQ-07.03-SPRINTEROP-SF02.0003: Mission trajectory coordination and transfer of responsibility from one AoR to the other (i.e. ARES to ATC sector or ATC to ARES) shall be executed as a system to system –supported exchange in accordance with established standards & regulations (SYSCO)</p> <p>SR_TS_004: Adequate SW assurance shall be ensured for the reception, update, processing and distribution of the iSMT/iRMT by the ATC system</p>
ATC system error resulting in inconsistent information displayed to PLN ATCO with respect to FD one		<p>REQ-07.03-SPRINTEROP-SF02.0003</p> <p>SR_TS_004</p>
ATCO fails to update the iRMT information in the system		<p>In order to mitigate the inconsistency between onboard and ground iRMT information:</p> <ul style="list-style-type: none"> as per current operations, the ATC conformance monitoring function and reminders (where available) <p>REQ-07.03-SPRINTEROP-SF02.0001: ATCO procedures shall reflect the proper management of the iRMT</p> <p>REQ-07.03-SPRINTEROP-SF02.0002: ATCO shall be properly trained in the management of the iRMT</p>





Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
WOC system error after an iRMT revision, resulting in discrepancy between the iRMT agreed with ATC and the iRMT received by FD	REQ-07.03-SPRINTEROP-IO04.0003	In order to mitigate the inconsistency between onboard and ground iRMT information: <ul style="list-style-type: none"> as per current operations, the ATC conformance monitoring function and reminders (where available) <p>SR_TS_005: Adequate SW assurance shall be ensured for the processing and distribution of the iSMT/iRMT by the WOC system</p> <p>REQ-07.03-SPRINTEROP-SF04.0003: Final coordination with regards to iRMT update shall be always between FC and ATCO</p>
ATC system error resulting in discrepancy between the iRMT agreed between WOC and ATC and the iRMT received by FD	REQ-07.03-SPRINTEROP-OP02.1001 REQ-07.03-SPRINTEROP-OP02.1002 REQ-07.03-SPRINTEROP-OP02.1003 REQ-07.03-SPRINTEROP-OP02.1004	SR_TS_004
FD system error resulting in discrepancy between the iRMT agreed with ATC and the iRMT received by FD		FD system is out of the scope of PJ07-03
WOC operator fails to provide or provide erroneous revised iRMT agreed with ATC to the FD	REQ-07.03-SPRINTEROP-OP02.1005 REQ-07.03-SPRINTEROP-OP04.0012 REQ-07.03-SPRINTEROP-IO04.0002	REQ-07.03-SPRINTEROP-SF04.0003: Final coordination with regards to iRMT update shall be always between FC and ATCO



Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
ATCO fails to update or incorrectly updates iRMT with respect to the agreed iRMT with FD		<p>In order to mitigate the inconsistency between onboard and ground iRMT information:</p> <ul style="list-style-type: none"> as per current operations, the ATC conformance monitoring function and reminders (where available) <p>REQ-07.03-SPRINTEROP-SF02.0001: ATCO procedures shall reflect the proper management of the iRMT</p> <p>REQ-07.03-SPRINTEROP-SF02.0002: ATCO shall be properly trained in the management of the iRMT</p>
FC fails to appropriately update the iRMT in the aircraft		FC is out of the scope of PJ07-03
ATC system error leading to revised iRMT not provided to adjacent ACCs	<p>REQ-07.03-SPRINTEROP-OP02.0002</p> <p>REQ-07.03-SPRINTEROP-OP02.0003</p> <p>REQ-07.03-SPRINTEROP-OP02.0006</p> <p>REQ-07.03-SPRINTEROP-IO02.0016</p> <p>REQ-07.03-SPRINTEROP-IO02.0017</p> <p>REQ-07.03-SPRINTEROP-IE02.0004</p>	SR_TS_004
ATC system error leading to revised iRMT not received from adjacent ACCs	<p>REQ-07.03-SPRINTEROP-OP02.0003</p> <p>REQ-07.03-SPRINTEROP-OP02.0006</p> <p>REQ-07.03-SPRINTEROP-IO02.0016</p> <p>REQ-07.03-SPRINTEROP-IO02.0017</p>	SR_TS_004

Table 11 Causal Analysis for Hazard 04

Founding Members





4.5.1.5 Hz 05: Uncoordinated ARES exit leading to imminent separation infringement

(Operational hazard already existing in baseline operations; the PJ07-03 design changes are expected to introduce new hazard causes)

<i>Severity Class</i>	SC-3	<i>IM factor</i>	1
<i>Safety Objective</i>	The likelihood of an uncoordinated ARES exit leading to separation infringement shall be no more than 4e-6 per sector operational hour		

Causes	Origin of the cause (SAF REQ not satisfied)	Mitigations / Safety Requirements
NM (IFPS) system error resulting in inaccurate or wrong iRMT published/distributed	REQ-07.03-SPRINTEROP-OP03.1003 REQ-07.03-SPRINTEROP-OP03.1008 REQ-07.03-SPRINTEROP-IE03.0003 REQ-07.03-SPRINTEROP-IO03.1008 REQ-07.03-SPRINTEROP-IO03.1009 REQ-07.03-SPRINTEROP-IO03.1011	REQ-07.03-SPRINTEROP-SF02.0003: Mission trajectory coordination and transfer of responsibility from one AoR to the other (i.e. ARES to ATC sector or ATC to ARES) shall be executed as a system to system –supported exchange in accordance with established standards & regulations (SYSCO) SR_TS_002: Adequate SW assurance shall be ensured for the distribution of the iSMT/iRMT
ATC system error resulting in inaccurate or wrong iRMT received by ATC	REQ-07.03-SPRINTEROP-OP02.0002 REQ-07.03-SPRINTEROP-OP02.0006 REQ-07.03-SPRINTEROP-OP02.1001 REQ-07.03-SPRINTEROP-OP02.1002 REQ-07.03-SPRINTEROP-OP02.1003 REQ-07.03-SPRINTEROP-OP02.1004	REQ-07.03-SPRINTEROP-SF02.0003 SR_TS_004: Adequate SW assurance shall be ensured for the reception, update, processing and distribution of the iSMT/iRMT by the ATC system

Table 12 Causal Analysis for Hazard 05

4.5.2 Common Cause Analysis

For the time being, the specification regarding the systems that are expected to fulfil the operational requirements have not yet been provided at the right level of detail. Consequently, there is no possibility at this stage to perform a Common Cause Analysis. This analysis will remain to be done once the Technical Specification document will be enough matured (that would not be expected for Wave 1).

4.5.3 Formalization of Mitigations

Table 13 formalizes the mitigations in terms of either existing SPR-INTEROP/OSED Requirements (i.e. requirements already existing in the SPR-INTEROP/OSED when the safety assessment at the design level was initiated, which will need to be allocated the Safety category) or new derived Safety Requirements (the latter are highlighted in bold).

These mitigations have been formalised considering the outcome of the causal analysis (see section 4.5.1) and more particularly the hazard mitigations identified in the tables developed for each operational hazard (mitigations allowing to prevent the hazard occurrence, i.e. to either limit the occurrence of the cause or its propagation up to the occurrence of the operational hazard).



SO	SRs	SR Description	Allocated to Activity / Role
SO 101 The likelihood of undetected incorrect traffic load data provided by Regional ATFCM to users shall be no more than 6e-5 per sector operational hour	REQ-07.03-SPRINTEROP-SF02.0001	ATCO procedures shall reflect the proper management of the iRMT	As per PJ07-03 SPR-INTEROP/OSED document
	REQ-07.03-SPRINTEROP-SF02.0002	ATCO shall be properly trained in the management of the iRMT	As per PJ07-03 SPR-INTEROP/OSED document
	REQ-07.03-SPRINTEROP-SF03.0001	Regional ATFCM operator shall be alerted in case of connection failure with the relevant entities	As per PJ07-03 SPR-INTEROP/OSED document
	REQ-07.03-SPRINTEROP-SF04.0001	In case of WOC system or connection failure preventing from iOAT FPL filing/updating, WOC operator shall file or update iOAT FPL by alternative means (e.g. phone, fax, mail etc.)	As per PJ07-03 SPR-INTEROP/OSED document
	REQ-07.03-SPRINTEROP-SF04.0002	WOC shall be alerted via a lack of acknowledgement message in case the submitted iSMT/iRMT has not been received by the Regional ATFCM system	As per PJ07-03 SPR-INTEROP/OSED document
	SR_TS_001	Adequate SW assurance shall be ensured for the IFPS reception, processing & validation of the iSMT/iRMT by NM system”	As per PJ07-03 SPR-INTEROP/OSED document
	SR_TS_002	Adequate SW assurance shall be ensured for the distribution of the iSMT/iRMT	As per PJ07-03 SPR-INTEROP/OSED document
	SR_TS_003	Adequate SW assurance shall be ensured for the demand forecast computation accounting for the iSMT/iRMT	As per PJ07-03 SPR-INTEROP/OSED document
	SR_TS_004	Adequate SW assurance shall be ensured for the reception, update, processing and distribution of the iSMT/iRMT by the ATC system	As per PJ07-03 SPR-INTEROP/OSED document
SR_TS_007	Adequate SW assurance shall be ensured for the reception and processing of the iSMT/iRMT by the Local ATFCM system	As per PJ07-03 SPR-INTEROP/OSED document	





SO	SRs	SR Description	Allocated to Activity / Role
<p>SO 102</p> <p>The likelihood that MIL flight inbounds a sector with short notice (from adjacent sector or ARES) shall be no more than 1e-4 per flight hour</p>	REQ-07.03-SPRINTEROP-OP03.1002	Regional ATFCM shall provide the same options for filing and submission of iOAT FPL as for civil GAT FPL	As per PJ07-03 SPR-INTEROP/OSED document
	REQ-07.03-SPRINTEROP-SC04.0003	The supporting IT infrastructure SWIM and PENS shall transfer Flight Plan data without error	As per PJ07-03 SPR-INTEROP/OSED document
	REQ-07.03-SPRINTEROP-SF02.0003	Mission trajectory coordination and transfer of responsibility from one AoR to the other (i.e. ARES to ATC sector or ATC to ARES) shall be executed as a system to system –supported exchange in accordance with established standards & regulations (SYSCO)	As per PJ07-03 SPR-INTEROP/OSED document
	REQ-07.03-SPRINTEROP-SF04.0001	In case of WOC system or connection failure preventing from iOAT FPL filing/updating, WOC operator shall file or update iOAT FPL by alternative means (e.g. phone, fax, mail etc.)	As per PJ07-03 SPR-INTEROP/OSED document
	SR_TS_001	Adequate SW assurance shall be ensured for the IFPS reception, processing & validation of the iSMT/iRMT by NM system	As per PJ07-03 SPR-INTEROP/OSED document
	SR_TS_002	Adequate SW assurance shall be ensured for the distribution of the iSMT/iRMT	As per PJ07-03 SPR-INTEROP/OSED document
	SR_TS_004	Adequate SW assurance shall be ensured for the reception, update, processing and distribution of the iSMT/iRMT by the ATC system	As per PJ07-03 SPR-INTEROP/OSED document
	SR_TS_006	ATC system jointly with ASM system shall be able to identify any inaccurate iRMT distribution within the ATC system including the appropriate activated/deactivated ARES entry and exit points	As per PJ07-03 SPR-INTEROP/OSED document





SO	SRs	SR Description	Allocated to Activity / Role
<p>SO 103</p> <p>The likelihood of corrupted traffic load data provided to users due to incorrect accommodation of correctly received iSMT in local ATFCM shall be no more than 6e-5 per sector operational hour</p>	<p>REQ-07.03-SPRINTEROP-SF03.0002</p>	<p>Local ATFCM actor shall be trained in the proper impact assessment of the mission trajectories</p>	<p>As per PJ07-03 SPR-INTEROP/OSED document</p>
	<p>SR_TS_007</p>	<p>Adequate SW assurance shall be ensured for the reception and processing of the iSMT/iRMT by the Local ATFCM system</p>	<p>As per PJ07-03 SPR-INTEROP/OSED document</p>





SO	SRs	SR Description	Allocated to Activity / Role
<p>SO 104</p> <p>The likelihood that a conflict-inducing aircraft lateral deviation occurs due to ground-airborne iRMT inconsistency shall be no more than 3.3e-5 per flight hour</p>	REQ-07.03-SPRINTEROP-SF02.0001	ATCO procedures shall reflect the proper management of the iRMT	As per PJ07-03 SPR-INTEROP/OSED document
	REQ-07.03-SPRINTEROP-SF02.0002	ATCO shall be properly trained in the management of the iRMT	As per PJ07-03 SPR-INTEROP/OSED document
	REQ-07.03-SPRINTEROP-SF02.0003	Mission trajectory coordination and transfer of responsibility from one AoR to the other (i.e. ARES to ATC sector or ATC to ARES) shall be executed as a system to system –supported exchange in accordance with established standards & regulations (SYSCO)	As per PJ07-03 SPR-INTEROP/OSED document
	REQ-07.03-SPRINTEROP-SF04.0003	Final coordination with regards to iRMT update shall be always between FC and ATCO	As per PJ07-03 SPR-INTEROP/OSED document
	SR_TS_001	Adequate SW assurance shall be ensured for the IFPS reception, processing & validation of the iSMT/iRMT by NM system	As per PJ07-03 SPR-INTEROP/OSED document
	SR_TS_002	Adequate SW assurance shall be ensured for the distribution of the iSMT/iRMT	As per PJ07-03 SPR-INTEROP/OSED document
	SR_TS_004	Adequate SW assurance shall be ensured for the reception, update, processing and distribution of the iSMT/iRMT by the ATC system	As per PJ07-03 SPR-INTEROP/OSED document
	SR_TS_005	Adequate SW assurance shall be ensured for the processing and distribution of the iSMT/iRMT by the WOC system	As per PJ07-03 SPR-INTEROP/OSED document





SO	SRs	SR Description	Allocated to Activity / Role
SO 105 The likelihood of an uncoordinated ARES exit leading to separation infringement shall be no more than 4e-6 per flight hour	REQ-07.03-SPRINTEROP-SF02.0003	Mission trajectory coordination and transfer of responsibility from one AoR to the other (i.e. ARES to ATC sector or ATC to ARES) shall be executed as a system to system –supported exchange in accordance with established standards & regulations (SYSCO)	As per PJ07-03 SPR-INTEROP/OSED document
	SR_TS_002	Adequate SW assurance shall be ensured for the distribution of the iSMT/iRMT	As per PJ07-03 SPR-INTEROP/OSED document
	SR_TS_004	Adequate SW assurance shall be ensured for the reception, update, processing and distribution of the iSMT/iRMT by the ATC system	As per PJ07-03 SPR-INTEROP/OSED document

Table 13 Safety Requirements formalizing the mitigations preventing the operational hazards occurrence (the ones added to the existing set of SPR-INTEROP/OSED or TS/IRS requirements are highlighted in bold)



4.5.4 Safety Requirements (integrity/reliability)

According to the SRM this section is aimed at setting Safety Requirements to limit the frequency with which each identified failure of the HW elements/parts of the system could be allowed to occur, taking account of the above mitigations, such that the residual risk is within the specified numeric values as per section 0 above.

The Safety Requirements (integrity/reliability) for the execution phase will be subject to more in-depth safety assessment in further lifecycle steps outside the scope of initial V3 (as a refined design needs to be specified in the V3 TS/IRS and the associated NSV-4 EATMA models).

4.6 Achievability of the Safety Criteria – Safety validation results

Safety validation objectives were not defined for the exercise related to the planning phase held in May 2019, given that the conducted Shadow Mode simulation was of limited operational relevance for the safety aspects. In addition, the results collected in the VALR [10] have not shown any safety related outcome.

Further V3 validation exercises (including those related to the execution phase and involving relevant safety aspects) necessary to achieve the full V3 maturity level, will be part of SESAR Wave 2 solution 40

4.7 Realism of the SPR-level Design

The development and safety analysis of the design would be seriously undermined if it were found in the subsequent Implementation phase that the Safety Requirements were either not ‘testable’ or impossible to satisfy (i.e. not achievable), and / or that some of the assumptions were in fact incorrect.

This is not relevant for the initial design but will need to be performed for the refined design in further V3 assessments.

4.7.1 Achievability of Safety Requirements / Assumptions

N/A

4.7.2 “Testability” of Safety Requirements

N/A

4.8 Validation & Verification of the Safe Design at SPR Level

This section describes the processes by which safety requirements were derived as well as details of the competencies of the personnel involved.

The causal analysis and the related safety requirements derivation have been conducted in a Safety Workshop in which the analysis undertaken by the safety assessment team has been progressively validated, involving the following PJ07-03/PJ18-01 design and operational experts.

WebEx meeting 17/06/2019

Name	Surname	Company
Igor	KUREN	EUROCONTROL
Edgar	REUBER	EUROCONTROL
Frank	JELINEK	EUROCONTROL
Norbert	KUPSCH	AIRBUS
Jan	PLEVKA	ANS CR (B4)
Milos	ZIDEK	ANS CR (B4)

The validation has been further complemented by submitting the results (as documented in this safety assessment report) to the internal validation by a panel of PJ07-03/PJ18-01 operational, design and technical experts (see the list of reviewers internal to the project on the cover page of this safety assessment report).

5 Acronyms and Terminology

Term	Definition
ACAS	Airborne Collision Avoidance System
ACC	Area Control Centre or Area Control
ADR	Aeronautical Data Repository
AFUA	Advanced Flexible Use of Airspace
AIM	Accident Incident Model
AMC	Airspace Management Cell
ANS CR	Air Navigation Services – Czech Republic
APW	Area Proximity Warning
ARES	Airspace Reservation
ASM	Airspace Management
ATCO	Air Traffic Control Officer
ATFCM	Air Traffic Flow and Capacity Management
ATFM	Air Traffic Flow Management
ATM	Air Traffic Management
AU	Airspace User
AUP	Airspace Use Plan
CACD	Central Airspace and Capacity Database
CDM	Collaborative Decision Making
CNS	Communication Navigation and Surveillance
CONOPS	Concept of Operations
CR	Change Request
DMA	Dynamic Mobile Area
EAP	Extended ATC Planner
EATMA	European ATM Architecture
EOBT	Estimated Off Block time

ETFMS	Enhanced Tactical Flow Management System
FDPS	Flight Data Processing System
FHA	Functional Hazard Analysis
FMP	Flow Management Position
FOC	Flight Operations Centre
GAT	General Air Traffic
HAZID	Hazard IDentification
HMI	Human Machine Interface
HP	Human Performance
HPAR	Human Performance Assessment Report
IFPS	Integrated Initial Flight Plan Processing System
INTEROP	Interoperability Requirements
IOAT FPL	Improved Operational Air Traffic Flight Plan
iRMT	Initial Reference Mission Trajectory
iSMT	Initial Shared Mission Trajectory
IRS	Interface Requirement Specification
KPA	Key Performance Area
MAC	Mid-Air Collision Model (AIM)
MIL	Military
MT	Mission Trajectory
NM	Network Manager
NMF	Network Management Function
NMOC	Network Manager Operations Centre
NOP	Network Operations Plan
NOTAM	Notice to Airman
OAT	Operational Air Traffic
OAT FPL	Operational Air Traffic Flight Plan
OATTS	Operational Air Traffic Transit Service (Pan-European OAT-IFR Transit Service)
OAUO	Optimized Airspace User Operations

OI	Operational Improvement
OM	Operating Method
OSED	Operational Service and Environment Definition
PFP	Preliminary Flight Plan
PSSA	Preliminary System Safety Assessment
QoS	Quality of Service
RTSA	Real Time Status of ARES
SAC	Safety Criteria
SAR	Safety Assessment Report
SESAR	Single European Sky ATM Research Programme
SFPL	System Flight Plan
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SO	Safety Objective
SPR	Safety and Performance Requirements
SRM	SESAR Safety Reference Material
STAM	Short-Term ATFCM Measures
STCA	Short-Term Conflict Alert
SWIM	System Wide Information Model
TMA	Terminal Manoeuvring Area
TS	Technical Specification
TTA	Target Time of Arrival
TTO	Target Time Over
UC	Use Case
UUP	Updated Use Plan
V1, V2...	Validation Maturity Levels
VALR/P	Validation Report/Plan
WOC	Wing Operations Centre

Table 14: Acronyms and terminology

6 References

Safety

- [1] SESAR 2020 Safety Policy
- [2] SESAR, Safety Reference Material, Edition 00.04.01, December 2018
- [3] SESAR, Guidance to Apply the Safety Reference Material, Edition 00.03.01, December 2018
- [4] SESAR Solution PJ.07-03: Validation Plan (VALP) for V3 – Part II – Safety Assessment Plan, Edition 00.02.00, 29th July 2019
- [5] SESAR Solution PJ.07-03 SPR-INTEROP/OSED for initial V3, Edition 00.03.01 (Draft), 15th August 2019
- [6] PJ19: Validation Targets (2019), Ed.00.00.01, 23 January 2019
- [7] EATMA Portal
- [8] SESAR Solution PJ.07-03: Validation Plan (VALP) for V3 - Part I, Edition 00.01.01, 31st July 2019
- [9] SESAR Solution PJ.07-03 SPR/INTEROP-OSED V3 - Part IV - Human Performance Assessment Report Edition 00.01.02 August 2019
- [10] SESAR Solution PJ.07-03: Validation Report (VALR) for V3, Edition 00.00.04, 4th September 2019







Appendix A Derivation of Safety Objectives (Functionality & Performance – success approach) for Normal Operations

A.1 EATMA Process Models

The following EATMA Process Models (extracted from PJ07-03 OSED [5] and EATMA Portal [7]) addressed in this Safety Assessment Report have been taken into consideration for the elaboration of the Safety Assessment.

- Operating Method 1: Mission Trajectory Management in the Short Term Planning Phase
- Operating Method 2: Mission Trajectory Management in the Execution Phase
- Operating Method 3: iRMT Revision triggered by WOC
- Operating Method 4: iRMT Revision triggered by ATC
- Operating Method 5: iRMT Revision triggered by Flight Deck

The activities included in these models have been marked with the following coloured labels for traceability depending on the related Operational Services:

Legend	ID	Operational Service
	FPL#1	Flight plan preparation, filing, validation and distribution (focusing on Mission Trajectory in planning phase, including ARES cross check)
	FPL#2	Flight plan revision (focusing on MT revision in execution phase)
	ASM#1	Adjust the Capacity (to the extent where it is available) to fit the predicted Demand
	ASM#2	Airspace reservation and management
	DCB	Balance the predicted Demand against the available Capacity
	ATC	ATC services <ul style="list-style-type: none"> • Planning & Coordination • Arrival sequencing, Metering, Holding • Maintain separation between aircraft • Handle request from AC (level, routing) • Manage trajectory • Lateral / vertical Deviation Detection & Resolution • Prevent unauthorized entry into restricted airspace • Prevent unauthorized exit from restricted airspace

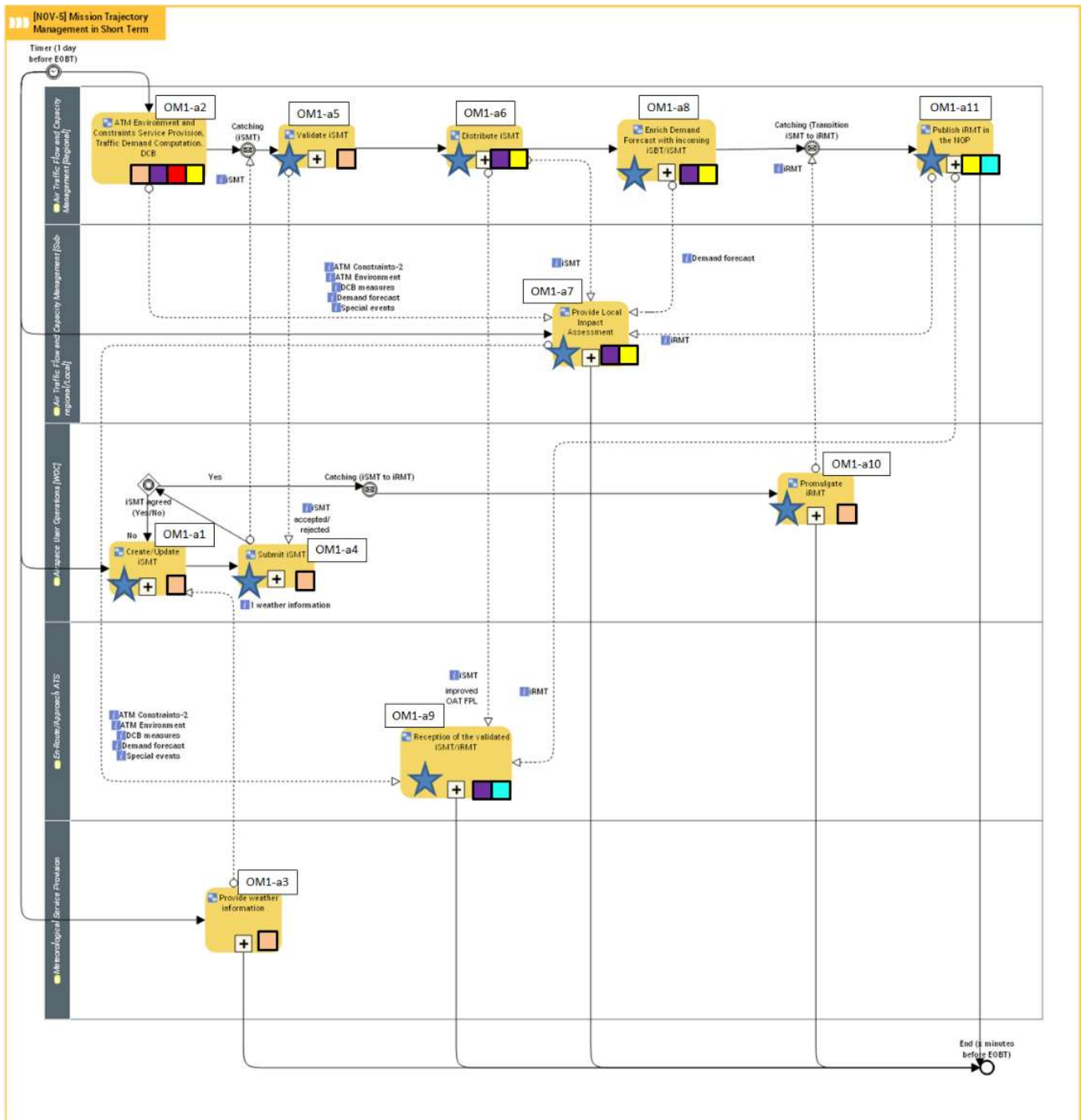
The activities and flows have been codified following the same principle:

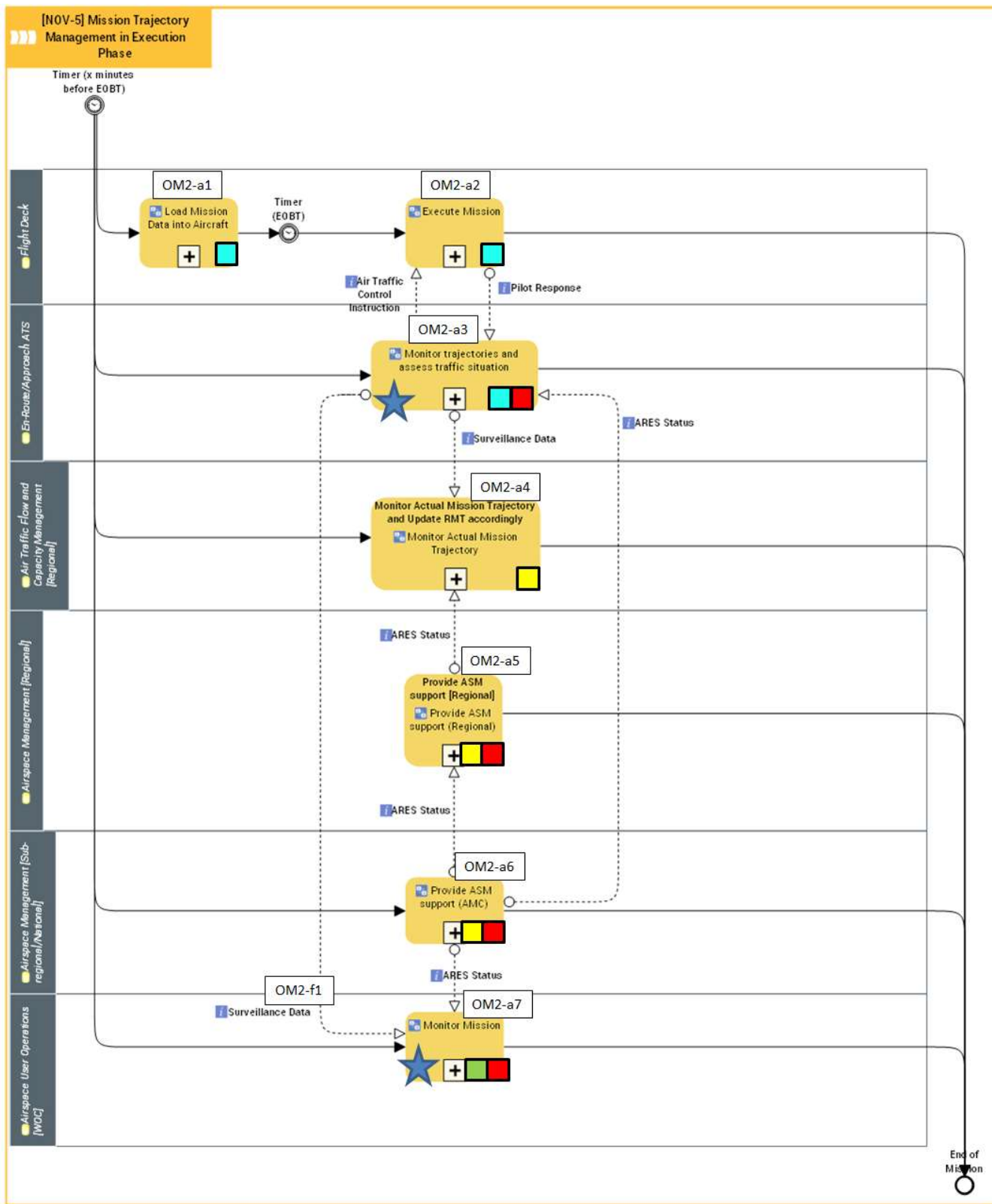
OMx-yz

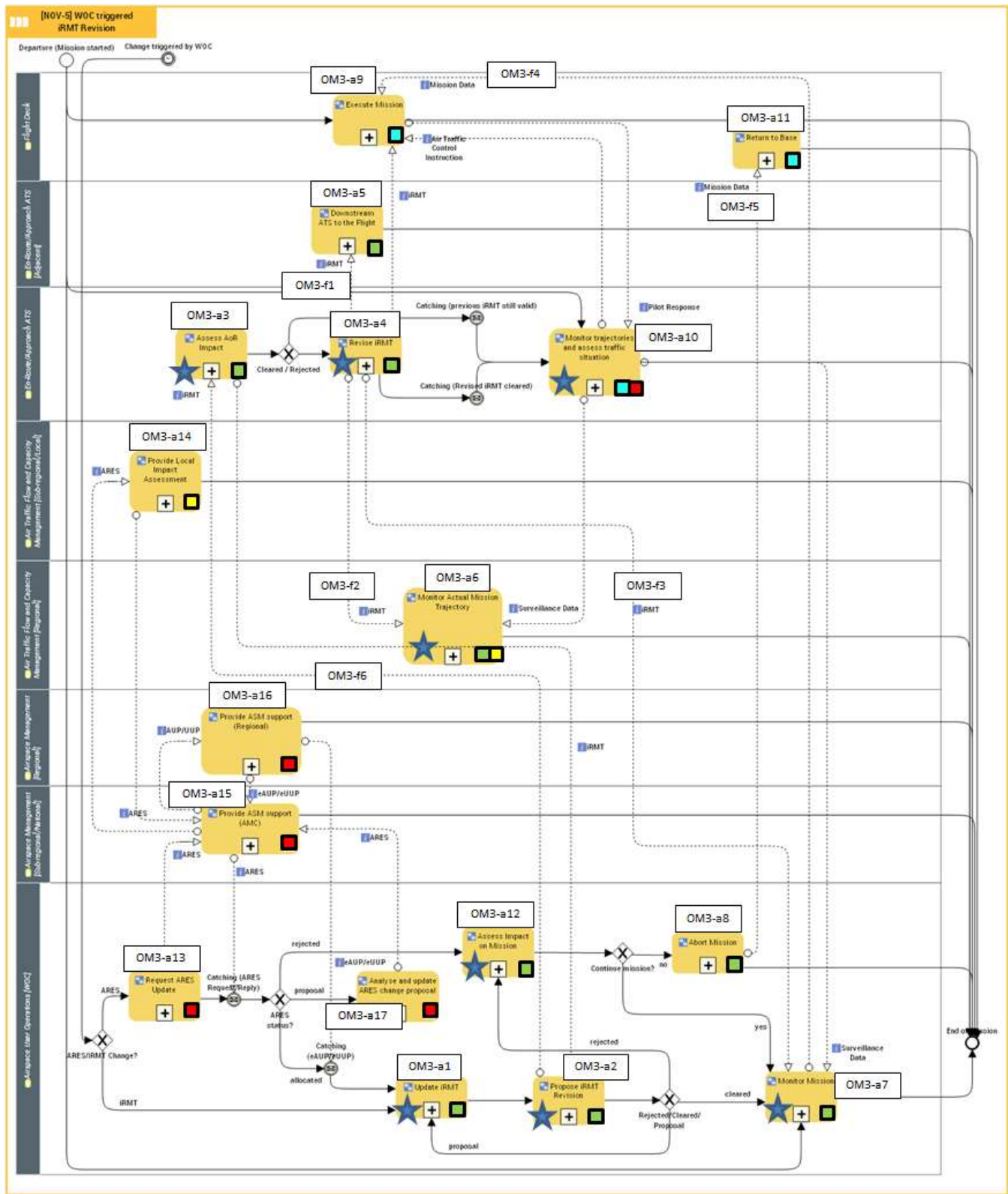
OMx	x corresponding to the number of the related Operating Method
y	y corresponding to an activity (a) or to a flow (f)
z	z corresponding to correlative numbers from 1 to n

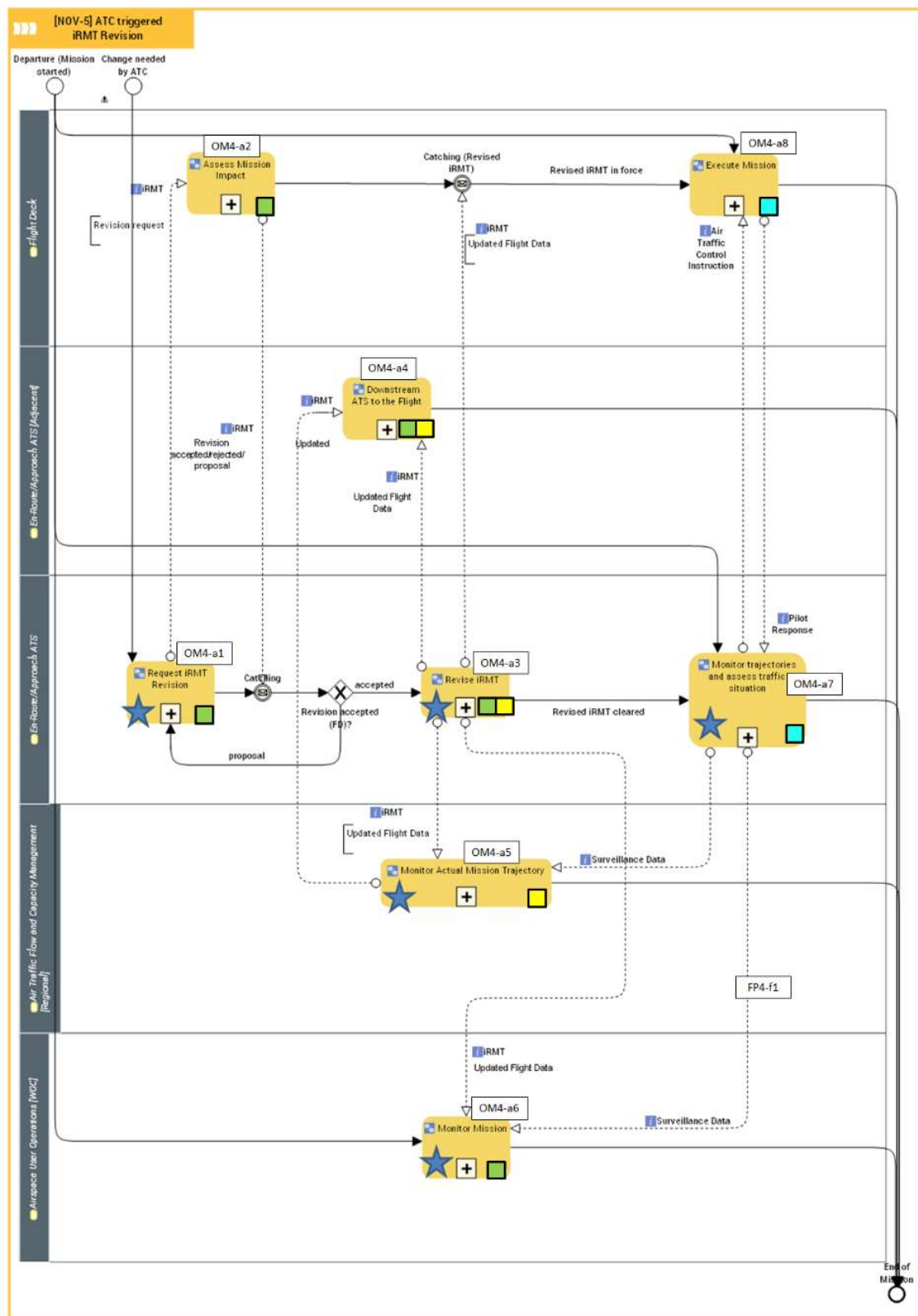
The activities identified as impacted by the change (i.e. either new or modified) have been highlighted in the EATMA Process Models with the following symbol: ★

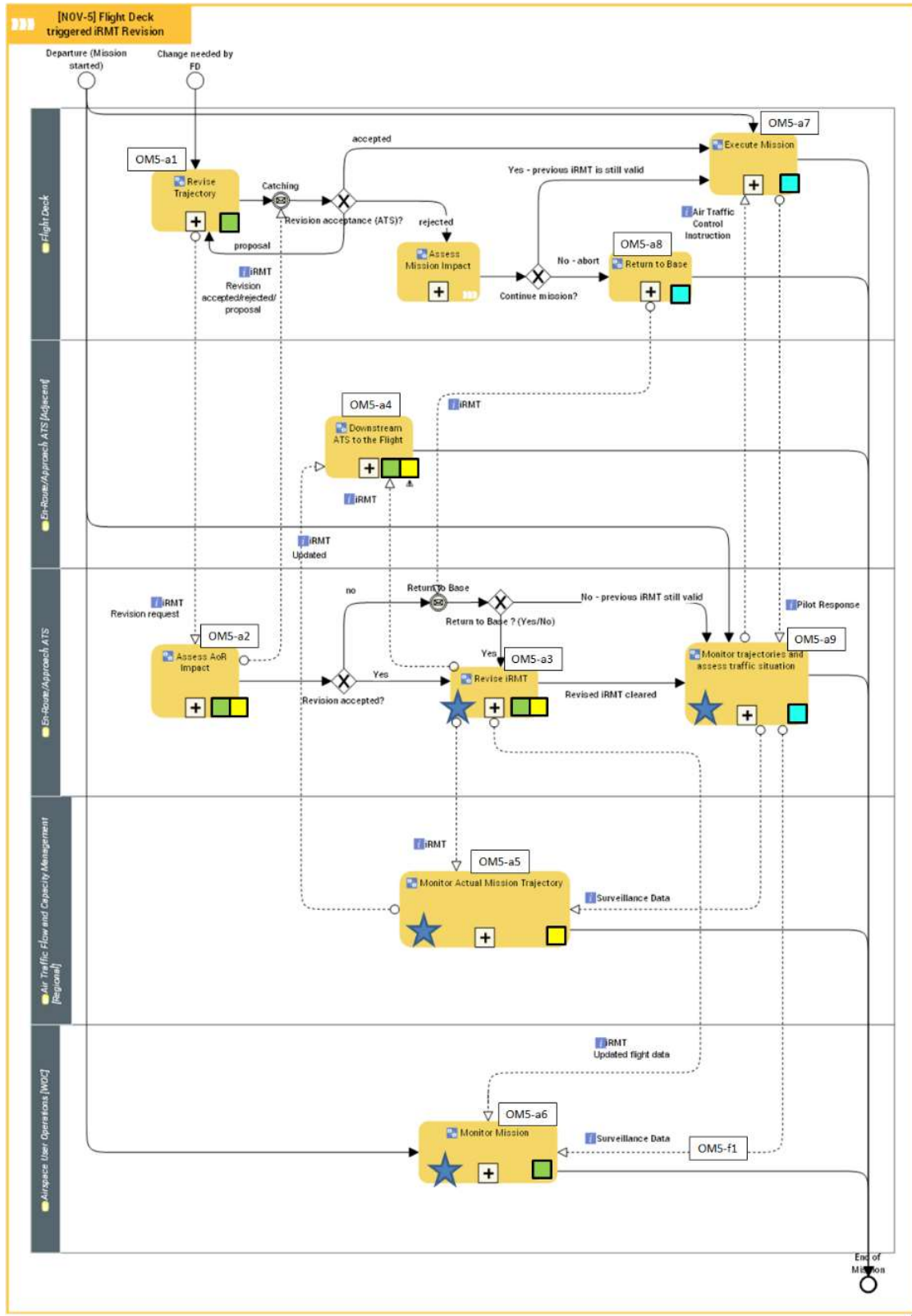
Note: Only the activities identified as impacted by the change (i.e. either new or modified) have been taken into account in the table for SO success derivation.











A.2 Derivation of Safety Objectives for Normal Operations driven by EATMA Process Models

The derivation of the functionality & performance Safety Objectives (as part of the success approach) is performed following and making use of the work done in the previous subsection (A.1).

The process carried out in this Step 2 is the following:

- Consolidate the information outcome from Step 1 above according to Operating Method and Operational services
- For each Operating Method:
 - For each Operational service:
 - Check whether the identified change(s) **is (are) safety relevant** (i.e. could the change impact the efficiency of a safety barrier or the occurrence of a safety precursor; the previously identified operational services are a necessary but not sufficient indication, given their link to the AIM models)
 - Derive one or several Safety Objectives in order to describe the safety-relevant changes in the delivery of that operational service by the Solution.

The rules used for codifying the different activities and flows, as well as for showing for each activity to which operational services it contributes to and whether it involves a change, are detailed in A.1.



Operational Service	EATMA Operating Method - Activity or Flow	Achieved by / Safety Objective [SO xx]	Related SAC# (AIM Barrier or Precursor)
---------------------	---	--	---

OM1: Mission Trajectory Management in Short Term Planning Phase

Flight plan preparation, filing, validation and distribution (focusing on Mission Trajectory (including ARES cross check) in planning phase)	Create/update iSMT	OM1-a1	SO 001: WOC shall submit (and resubmit if any update is needed) iSMT in time for enabling reliable traffic prediction	SAC#01a (B12: Short Term DCB)
	Submit iSMT	OM1-a4		SAC#01b (B12: Short Term DCB)
	Validate iSMT	OM1-a5	SO 002: Regional ATFCM shall validate iSMT in accordance with the applicable ATM constraints	SAC#01a (B12: Short Term DCB) SAC#01b (B12: Short Term DCB)
	Promulgate iRMT	OM1-a10	SO 003: WOC shall submit iRMT in full consistency with the validated trajectory	SAC#01a (B12: Short Term DCB) SAC#01b (B12: Short Term DCB) SAC#05a (B10-B11: Traffic Planning & Synchronization) SAC#05b (B10-B11: Traffic Planning & Synchronization)





Operational Service	EATMA Operating Method - Activity or Flow	Achieved by / Safety Objective [SO xx]	Related SAC# (AIM Barrier or Precursor)
Adjust the Capacity (to the extent where it is available) to fit the predicted Demand	Distribute iSMT OM1-a6 Enrich and publish demand forecast with incoming iSMT data OM1-a8	SO 004: Regional ATFCM shall distribute the iSMT to Sub-regional/local ATFCM and ENR/APP ATS and update demand forecast accordingly	SAC#01a (B12: Short Term DCB) SAC#01b (B12: Short Term DCB)
	Provide Local Impact Assessment OM1-a7 Note: This operational service is not concerned with the iRMT, because too late for the sectors configuration to account for the iRMT	SO 005: Sub-regional/local ATFCM shall receive iSMT and integrate it in the local impact assessment in view of appropriate Capacity adjustment and Demand balancing	SAC#01a (B12: Short Term DCB) SAC#01b (B12: Short Term DCB)
	Reception of the validated iSMT/iRMT OM1-a9 Note: Inside this activity the iSMT reception is considered for Capacity adjustment purposes whilst the iRMT is considered for ATC service purposes (see "ATC services" below)	No specific safety objective, given the mitigation offered by ATFCM measures (e.g. STAM) in case of an inadequate sectors configuration	





Operational Service	EATMA Operating Method - Activity or Flow	Achieved by / Safety Objective [SO xx]	Related SAC# (AIM Barrier or Precursor)
Balance the predicted Demand against the available Capacity	Distribute iSMT OM1-a6	SO 004	SAC#01a (B12: Short Term DCB)
	Enrich and publish demand forecast with incoming iSMT data OM1-a8		SAC#01b (B12: Short Term DCB)
	Provide Local Impact Assessment OM1-a7	SO 005	
	Publish iRMT in the NOP OM1-a11	SO 006: Regional ATFCM shall distribute the iRMT to Sub-regional/local ATFCM in view of appropriate Demand balancing against available Capacity and to ENR/APP ATS in view of the provision of ATC services	
ATC Services	Reception of the validated iSMT/iRMT OM1-a9	SO 007: ENR/APP ATS shall receive timely and accurate iRMT consistent with the allocated ARES (if applicable) in view of the provision of ATC services	SAC#03a (MF7.1 ATC induced tactical conflict) SAC#03b (MF7.1 ATC induced tactical conflict)
	Publish iRMT in the NOP OM1-a11	SO 006	SAC#04a (No AIM available) SAC#04b (No AIM available) SAC#05a (B10-B11: Traffic Planning & Synchronization) SAC#05b (B10-B11: Traffic Planning & Synchronization) SAC#06a (B5-B9: Tactical Conflict Management) SAC#06b (B5-B9: Tactical Conflict Management)





Operational Service	EATMA Operating Method - Activity or Flow	Achieved by / Safety Objective [SO xx]	Related SAC# (AIM Barrier or Precursor)
---------------------	---	--	---

OM2: Mission Trajectory Management in Execution Phase

Flight plan revision (focusing on MT revision in execution phase)	Monitor Mission	OM2-a7	SO 008: WOC shall receive Surveillance Data in view of an enhanced mission monitoring (e.g. to detect possible deviations from the expected trajectory)	SAC#02a (MF6.1 Crew/aircraft induced conflict) SAC#02b (MF6.1 Crew/aircraft induced conflict) SAC#06a (B5-B9: Tactical Conflict Management) SAC#06b (B5-B9: Tactical Conflict Management)
	En-Route/Approach ATS to WOC Data Flow: Surveillance Data	OM2-f1		
Airspace reservation and management	Monitor trajectories and assess traffic situation	OM2-a3	The change affecting these activities does not concern this Operational Service	
ATC Services	Monitor mission	OM2-a7		
	Monitor trajectories and assess traffic situation	OM2-a3	SO 007	SAC#03a (MF7.1 ATC induced tactical conflict) SAC#03b (MF7.1 ATC induced tactical conflict) SAC#04a (No AIM available) SAC#04b (No AIM available) SAC#05a (B10-B11: Traffic Planning & Synchronization) SAC#05b (B10-B11: Traffic Planning & Synchronization) SAC#06a (B5-B9: Tactical Conflict Management) SAC#06b (B5-B9: Tactical Conflict Management)





Operational Service	EATMA Operating Method - Activity or Flow	Achieved by / Safety Objective [SO xx]	Related SAC# (AIM Barrier or Precursor)
---------------------	---	--	---

OM3: WOC triggered iRMT Revision

Flight plan revision (focusing on MT revision in execution phase)	Update iRMT	OM3-a1	No specific safety objective as far as Flight Deck follows the current iOAT FPL	
	Propose iRMT revision	OM3-a2		
	WOC to En-Route/Approach ATS Data Flow: iRMT change request	OM3-f6	SO 009: iRMTs revised as agreed shall be shared whilst keeping consistency among all the following actors: ENR/APP ATS, Regional & Local ATFCM, Adjacent ENR/APP ATS, WOC and Flight Deck	SAC#02a (MF6.1 Crew/aircraft induced conflict)
	Revise iRMT	OM3-a4		SAC#02b (MF6.1 Crew/aircraft induced conflict)
	En-Route/Approach ATS to Adjacent En-Route/Approach ATS, to Regional ATFCM, to Flight Deck and to WOC Data Flow: iRMT (Updated Flight Data)	OM3-f1, OM3-f2, OM3-f3 & OM3-f7		SAC#03a (MF7.1 ATC induced tactical conflict)
WOC to FD Data Flow: mission data	OM3-f4 & OM3-f5	SAC#03b (MF7.1 ATC induced tactical conflict)		
		SAC#04a (No AIM available)		
			SAC#04b (No AIM available)	
			SAC#05a (B10-B11: Traffic Planning & Synchronization)	
			SAC#05b (B10-B11: Traffic Planning & Synchronization)	
			SAC#06a (B5-B9: Tactical Conflict Management)	
			SAC#06b (B5-B9: Tactical Conflict Management)	





Operational Service	EATMA Operating Method - Activity or Flow		Achieved by / Safety Objective [SO xx]	Related SAC# (AIM Barrier or Precursor)
	Monitor Mission	OM3-a7	SO 009	SAC#02a (MF6.1 Crew/aircraft induced conflict) SAC#02b (MF6.1 Crew/aircraft induced conflict) SAC#03a (MF7.1 ATC induced tactical conflict) SAC#03b (MF7.1 ATC induced tactical conflict) SAC#04a (No AIM available) SAC#04b (No AIM available) SAC#05a (B10-B11: Traffic Planning & Synchronization) SAC#05b (B10-B11: Traffic Planning & Synchronization) SAC#06a (B5-B9: Tactical Conflict Management) SAC#06b (B5-B9: Tactical Conflict Management)





Operational Service	EATMA Operating Method - Activity or Flow	Achieved by / Safety Objective [SO xx]	Related SAC# (AIM Barrier or Precursor)
Balance the predicted Demand against the available Capacity	Monitor Actual Mission Trajectory and Update RMT accordingly OM3-a6	SO 010: Regional ATFCM shall update the traffic demand in line with the latest updates of the iRMT	SAC#01a (B12: Short Term DCB) SAC#01b (B12: Short Term DCB)
ATC Services	Monitor trajectories and assess traffic situation OM3-a10	SO 009	SAC#02a (MF6.1 Crew/aircraft induced conflict) SAC#02b (MF6.1 Crew/aircraft induced conflict) SAC#03a (MF7.1 ATC induced tactical conflict) SAC#03b (MF7.1 ATC induced tactical conflict) SAC#04a (No AIM available) SAC#04b (No AIM available) SAC#05a (B10-B11: Traffic Planning & Synchronization) SAC#05b (B10-B11: Traffic Planning & Synchronization) SAC#06a (B5-B9: Tactical Conflict Management) SAC#06b (B5-B9: Tactical Conflict Management)





Operational Service	EATMA Operating Method - Activity or Flow	Achieved by / Safety Objective [SO xx]	Related SAC# (AIM Barrier or Precursor)
---------------------	---	--	---

OM4: ATC triggered iRMT Revision

Flight plan revision (focusing on MT revision in execution phase)	Request iRMT revision	OM4-a1	SO 009	SAC#02a (MF6.1 Crew/aircraft induced conflict) SAC#02b (MF6.1 Crew/aircraft induced conflict) SAC#03a (MF7.1 ATC induced tactical conflict) SAC#03b (MF7.1 ATC induced tactical conflict) SAC#04b (No AIM available) SAC#05a (B10-B11: Traffic Planning & Synchronization) SAC#05b (B10-B11: Traffic Planning & Synchronization) SAC#06a (B5-B9: Tactical Conflict Management) SAC#06b (B5-B9: Tactical Conflict Management)
	Revise iRMT	OM4-a3		
	Monitor Mission	OM4-a6	SO 008	SAC#02a (MF6.1 Crew/aircraft induced conflict) SAC#02b (MF6.1 Crew/aircraft induced conflict) SAC#06a (B5-B9: Tactical Conflict Management) SAC#06b (B5-B9: Tactical Conflict Management)
	En-Route/Approach ATS to WOC Data Flow: Surveillance Data	OM4-f1		





Operational Service	EATMA Operating Method - Activity or Flow	Achieved by / Safety Objective [SO xx]	Related SAC# (AIM Barrier or Precursor)
Balance the predicted Demand against the available Capacity	Monitor Actual Mission Trajectory OM4-a5	SO 010	SAC#01a (B12: Short Term DCB) SAC#01b (B12: Short Term DCB)
ATC Services	Monitor trajectories and assess traffic situation OM4-a7	SO 009	SAC#02a (MF6.1 Crew/aircraft induced conflict) SAC#02b (MF6.1 Crew/aircraft induced conflict) SAC#03a (MF7.1 ATC induced tactical conflict) SAC#03b (MF7.1 ATC induced tactical conflict) SAC#04a (No AIM available) SAC#04b (No AIM available) SAC#05a (B10-B11: Traffic Planning & Synchronization) SAC#05b (B10-B11: Traffic Planning & Synchronization) SAC#06a (B5-B9: Tactical Conflict Management) SAC#06b (B5-B9: Tactical Conflict Management)





Operational Service	EATMA Operating Method - Activity or Flow	Achieved by / Safety Objective [SO xx]	Related SAC# (AIM Barrier or Precursor)
OM5: FD triggered iRMT Revision			
Flight plan revision (focusing on MT revision in execution phase)	Revise iRMT	OM5-a3 SO 009	SAC#02a (MF6.1 Crew/aircraft induced conflict) SAC#02b (MF6.1 Crew/aircraft induced conflict) SAC#03a (MF7.1 ATC induced tactical conflict) SAC#03b (MF7.1 ATC induced tactical conflict) SAC#04a (No AIM available) SAC#04b (No AIM available) SAC#05a (B10-B11: Traffic Planning & Synchronization) SAC#05b (B10-B11: Traffic Planning & Synchronization) SAC#06a (B5-B9: Tactical Conflict Management) SAC#06b (B5-B9: Tactical Conflict Management)
	Monitor Mission En-Route/Approach ATS to WOC Data Flow: Surveillance Data	OM5-a6 OM5-f1 SO 008	SAC#02a (MF6.1 Crew/aircraft induced conflict) SAC#02b (MF6.1 Crew/aircraft induced conflict) SAC#06a (B5-B9: Tactical Conflict Management) SAC#06b (B5-B9: Tactical Conflict Management)





Operational Service	EATMA Operating Method - Activity or Flow	Achieved by / Safety Objective [SO xx]	Related SAC# (AIM Barrier or Precursor)
Balance the predicted Demand against the available Capacity	Monitor Actual Mission Trajectory	OM5-a5	SO 010
ATC Services	Monitor trajectories and assess traffic situation	OM5-a9	SO 009

- SAC#01a (B12: Short Term DCB)
- SAC#01b (B12: Short Term DCB)
- SAC#02a (MF6.1 Crew/aircraft induced conflict)
- SAC#02b (MF6.1 Crew/aircraft induced conflict)
- SAC#03a (MF7.1 ATC induced tactical conflict)
- SAC#03b (MF7.1 ATC induced tactical conflict)
- SAC#04a (No AIM available)
- SAC#04b (No AIM available)
- SAC#05a (B10-B11: Traffic Planning & Synchronization)
- SAC#05b (B10-B11: Traffic Planning & Synchronization)
- SAC#06a (B5-B9: Tactical Conflict Management)
- SAC#06b (B5-B9: Tactical Conflict Management)

Table 15: Solution Operational Services & Safety Objectives (success approach)

Founding Members



Appendix B HAZID Workshop Results

On 5th and 6th of March 2018, a SAF workshop was held at Prague Airport. The workshop was facilitated by SAF experts from EUROCONTROL, AIRBUS D&S, ANS CR (B4) and Deep Blue and had as one of main scopes the identification of possible hazards introduced by the new concept and the derivation of causes and consequences.

The full list of workshop participants is as follows:

- Nicolas FOTA – Safety Expert / EUROCONTROL
- Hugo MANSO TORRES – Safety Expert / EUROCONTROL
- Frank JELINEK – NM Validation Expert / EUROCONTROL
- Igor KUREN - Civil-Military ATM Expert / EUROCONTROL
- Jana HAJDUOVA – Project Manager / ANS CR (B4)
- Milos ZIDEK – ATC Expert / ANS CR (B4)
- Radka HRUBÁ - Safety & quality Expert / ANS CR (B4)
- Martina RAGOSTA – HP Expert / Deep Blue
- Luca SAVE– HP Expert / Deep Blue

The outcome of the HAZID workshop is contained in Table 16.

The hazards were derived using the PJ07-03 OSED [5] Operating Methods modelled via EATMA Process Models.

NOTE:

Some of the activities and information flows in the Operating Methods (i.e. EATMA Process Models) are not in the scope of the Change designed by PJ07-03 because they are already available in the Baseline, i.e. AFUA concept and the related CDM processes are already validated V3 in SESAR 1. These activities and information flows have been included in the Operating Methods to depict the overall picture and thus to facilitate the understanding.

Consequently the design activity (encompassing the safety assessment) will be limited to that scope of the Change.

NOTE 2:

Please take into consideration that the HAZID table shown below was developed in line with the models and SPR/INTEROP-OSED document available at date of the meeting. The safety assessment accounted for the successive updates during the Project evolution, however these updates have not been systematically reflected in the table below.



Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
01: MT Management in Short Term Planning	WOC fails to generate or submit iSMT or fails to re-submit iSMT (following rejection from NM)	<p>WOC system or connection failure</p> <p>WOC operator omission or overloaded</p> <p>*iSMT submitted to NM (centralized validation by IFPS, unlike current ops where OAT FPL submitted to ATC or not submitted at all)</p> <p>*iSMT standardized (XML format, whilst currently is AFTN or via fax/telephone)</p>	<p>If one flight is affected that involves a lost opportunity for NMf to enrich the demand forecast, with no safety impact.</p> <p>If a significant number of flights are affected an undetectable degradation of the imbalance prediction might occur (traffic demand differs from the planned “correct” one by more than 10%). Risk for severe sector overload (use of inadequate ATC sector configuration due to erroneous demand data could lead to significant increase in ATC workload in the affected unit). In extreme cases (lack of ATCO to open new sectors as a last attempt to mitigate hazard) the impact on sector is so high that even the tactical conflict management tasks may be compromised</p>	<p>No safety impact</p> <p>Prevention of imminent collision (STCA & ATCO expedite)</p>	<p>None</p> <p>Hz 01: Undetected incorrect traffic load data provided by Regional ATFCM to users</p> <p>(already existing in baseline operations- see NOSR Hz-04, failure mode FLM-05: Undetectable corruption of traffic load)</p>	<p>MAC-SC3</p> <p>IM=0.4</p>





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
			<p>iRMT (iOAT FPL) should be filed later on (but might be too late for efficient DCB measure).</p> <p>However, note that situation where multiple flights are affected will be detected and mitigated, provided the following safety requirement is considered:</p> <p>SAF REQ: In case of WOC system or connection failure preventing iSMT/iRMT filing, WOC operator shall file or update iSMT/iRMT by alternative means (e.g. phone, fax, mail etc.)</p> <p>In case of connection failure, lack of reception will be detected (will be the same mechanism as for civil FPLs).</p>			





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
	WOC fails to submit iRMT	<p>WOC system failure or connection</p> <p>WOC operator omission or overloaded</p>	<p>If one flight is affected that involves a lost opportunity for NMF to enrich the demand forecast, with no safety impact.</p> <p>The lack of one iRMT should be detected at the first contact with ATC, when they will create an iOAT FPL. That might not be systematically the case for MIL aircraft entering controlled airspace without preliminary notification/coordination (iOAT FPL filing). If undetected, potential for conflict not timely detected by PLN ATCO (note: MTCO is not impacted by the Concept as the iOAT is converted into a SFPL)</p> <p>Note: Missions related to security and Quick Reaction Alerts (i.e. interceptions) are not subject to FPL submission but are coordinated with ATC</p>	Tactical conflict resolution	Hz 02: MIL flight inbound a sector with short notice (from adjacent sector or ARES)	MAC-SC4b





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
			<p>If multiple flights are affected (traffic demand differs from the planned “correct” one by more than 10%), as for the iSMT submission, there will be an impact on NMf performance, with potential for not timely detecting a Hotspot resulting in sector overload. In case of lack of ATCO to open new sectors as a last attempt to mitigate hazard, the impact on sector is so high that even the tactical conflict management tasks may be compromised.</p> <p>However, note that situation where multiple flights are affected will be detected and mitigated, provided the following safety requirement is considered:</p> <p>SAF REQ: In case of WOC system or connection failure preventing iSMT/iRMT filing, WOC operator shall file or</p>	<p>Prevention of imminent collision (STCA & ATCO expedite)</p>	<p>Hz 01: Undetected incorrect traffic load data provided by Regional ATFCM to users</p> <p>(already existing in baseline operations- see NOSR Hz-04, failure mode FLM-05: Undetectable corruption of traffic load)</p>	<p>MAC-SC3 IM=0.4</p>





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
			update iSMT/iRMT by alternative means (e.g. phone, fax, mail etc.)			
	WOC submits late iRMT to NM	WOC system failure or connection WOC operator omission or overloaded	Same effects as above	Same as above	Same as above	Same as above
	NM (IFPS) fails to detect or reject invalid iSMT	System error (part updated to accommodate iSMT/iRMT) *New features (ARES reference, target time TTO, STAY ARES, etc)	iSMT is breaching a network constraint. If multiple flights are affected, it might involve an inaccurate demand forecast with impact on NMF performance & potential for not timely detecting a Hotspot resulting in sector overload. In case of lack of ATCO to open new sectors as a last attempt to mitigate hazard, the impact on sector is so high that even the tactical conflict management tasks may be compromised.	The problem will be detected at iRMT level as ATC system (FDPS) performs exhaustive checking, but that might be too late with regards to DCB activities Planning & tactical tasks under overload	H_z 01: Undetected incorrect traffic load data provided by Regional ATFCM to users (already existing in baseline operations- see NOSR Hz-04, failure mode FLM-05: Undetectable corruption of traffic load)	MAC-SC3 IM=0.4





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
	NM (IFPS) rejects a valid iSMT	System error (part updated to accommodate iSMT/iRMT)	WOC will receive the rejection message and will coordinate with NMOC/IFPS	NMOC revision (human actor in NM)	None	No safety effect
	NM (IFPS) fails to distribute iSMT or	System error (part updated to accommodate	ATC/Supervisor does not receive information regarding	If iSMT reaches the Local ATFCM, the latter will detect the Hotspot (if any) and resolve it	None	No safety effect





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
	ATC fails to receive iSMT	<p>iSMT/iRMT) – e.g. under addressing (missing destinies)</p> <p>*iSMT distributed to both ATC (Local Supervisor) and Local ATFCM:</p> <p>To ATC (Local Supervisor), for preparing sectors configurations</p> <p>To Local ATFCM for flow management</p>	planned MIL flights in view of sectors configuration	<p>If iSMT does not reach the Local ATFCM, then potential for not timely detecting a Hotspot with potential sector overload</p> <p>Planning & tactical tasks under overload</p>	H_z 01: Corrupted traffic load data provided to users due to iOAT FPLs missing or not updated	MAC-SC3 IM=0.4
	NM fails to enrich and publish demand forecast (based on iSMT)	System error	<p>NM does not make use of the new information obtained thanks to the iSMT.</p> <p>If multiple flights are affected, impact on NMF performance,</p>	Planning & tactical tasks under overload	H_z 01: Undetected incorrect traffic load data provided by Regional ATFCM to users (new contributor to	MAC-SC3 IM=0.4





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
		In the scope (Design under development by NM experts)	with potential for not timely detecting a Hotspot that might result in sector overload (in the context where sector capacity buffer will be reduced thanks to this Concept implementation)		already existing Hz-04 and similar to failure mode FLM-05 from Network Operations Safety Report NOSR v1.1 11/2017)	
	Local ATFCM fails to receive iSMT	System error	Local ATFCM cannot make use of iSMT information. If multiple flights are affected, potential for not timely detecting a Hotspot that might result in sector overload (in the context where sector capacity buffer will be reduced thanks to this Concept implementation)	In case the iSMT is not received by Local ATFCM, STAM measures can be at least partially applied after iRMT reception. Planning & tactical tasks under overload	H_z 01: Undetected incorrect traffic load data provided by Regional ATFCM to users (new contributor to already existing Hz-04 and similar to failure mode FLM-05 from Network Operations Safety Report NOSR v1.1 11/2017)	MAC-SC3 IM=0.4



Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
	Local ATFCM fails to assess the local impact of iSMT	System error (potential necessary adaptations to FMP interface/functionalities to host iSMT) Human error	If multiple flights are affected, potential for not timely detecting a Hotspot that might result in sector overload (in the context where sector capacity buffer will be reduced thanks to this Concept implementation)	Planning & tactical tasks under overload	H_z 03: ATFM measures not implemented or implemented partially by Local ATFCM (new contributor to already existing H _z -05 from Network Operations Safety Report NOSR v1.1 11/2017)	MAC-SC4b IM=10
	Local ATFCM receives inaccurate or wrong iSMT	System error (e.g. no update received) *Note: ATM constraints (e.g. Letters of agreement) are out of scope of PJ07.03 (will be considered under PJ09)	If multiple flights are affected, or if the ARES part of the iSMT is incorrect, it might involve an inaccurate demand forecast with impact on NMF performance & potential for not timely detecting a Hotspot	Planning & tactical tasks under overload	H_z 01: Undetected incorrect traffic load data provided by Regional ATFCM to users (new contributor to already existing H _z -04 and similar to failure mode FLM-05 from Network Operations Safety Report NOSR v1.1 11/2017)	MAC-SC3 IM=0.4





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
	NM fails to publish iRMT in the NOP (to be used by Local ATFCM and ATC/Supervisor)	System error	No impact, as far as the iRMT is also distributed to Local ATFCM and ATC/Supervisor		None	No safety impact
	NM (IFPS) fails to distribute iRMT to Local ATFCM	System error	If multiple flights are affected, potential for not timely detecting a Hotspot	Planning & tactical tasks under overload	H_z 01: Undetected incorrect traffic load data provided by Regional ATFCM to users (new contributor to already existing H _z -04 and similar to failure mode FLM-05 from Network Operations Safety Report NOSR v1.1 11/2017)	MAC-SC3 IM=0.4





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
	NM (IFPS) fails to distribute iRMT to ATC (FDPS)	System error (e.g. under addressing, over addressing)	Detected at the first contact with ATC, who will create an iOAT FPL. That might not be systematically the case for MIL aircraft entering controlled airspace without preliminary notification/coordination (iOAT FPL filing). If undetected, potential for conflict not timely detected by PLN ATCO	Tactical conflict resolution	Hz 02: MIL flight inbound a sector with short notice (from adjacent sector or ARES)	MAC-SC4b
	ATC fails to receive iRMT	System error	Same as above	Tactical conflict resolution	Hz 02: MIL flight inbound a sector with short notice (from adjacent sector or ARES)	MAC-SC4b



Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
	ATC receives inaccurate or wrong iRMT	System error (e.g. lack of update)	<p>Potential for conflict not timely detected by PLN ATCO (either MIL aircraft inbound sector from adjacent sector or MIL aircraft leaving ARES), due to:</p> <ol style="list-style-type: none"> Aircraft lateral deviation at a waypoint due to ground-airborne iRMT inconsistency ARES information in iRMT not consistent with the allocated ARES (further used by ATC). <ul style="list-style-type: none"> Wrong activation time (the case where entry time is earlier or later than ARES allocated timeframe will be 	<p>Trajectory conformance monitoring tool (RAM/CLAM)</p> <p>Tactical conflict resolution</p> <p>Note: MAC-SC4a corresponds to a situation where an imminent infringement coming from a crew/aircraft induced conflict was prevented by tactical conflict management</p> <p>In order to detect the inconsistency, and more generally to prevent the lack of coordination, need for:</p> <p>Safety requirement: MIL Flight coordination and transfer of responsibility from one AoR to the other (i.e. ARES to ATC</p>	<p>Hz 04: Conflict-inducing aircraft lateral deviation due to ground-airborne iRMT inconsistency</p> <p>Hz 02: MIL flight inbound a sector with short notice (from adjacent sector or ARES)</p>	<p>MAC-SC4a</p> <p>MAC-SC4b</p>

Founding Members





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
			<p>detected by ATC system, performing check against UUP)</p> <ul style="list-style-type: none"> • Wrong entry point or flight level • Wrong trajectory after exiting <p>3. If undetected, risk for tactical conflict between MIL aircraft exiting ARES and aircraft flying at ARES borders (not predictable based on flight plan info)</p>	<p>sector or ATC to ARES) shall be executed as a system to system exchange in accordance with established standards & regulations</p> <p>Once the inconsistency detected, mitigated through Tactical conflict resolution</p> <p>If the new mitigation proposed above fails, MIL aircraft would exit ARES at a point, level or time unexpected by ATC with risk of separation infringement with aircraft flying close to ARES borders</p> <p>ATC collision prevention (STCA)</p> <p>*Note that FBZ (Flight plan Buffer Zone around ARES) is reduced with ASM concept in order to enhance efficiency. That needs to be considered in the assessment of this risk.</p>	<p>H05: Uncoordinated ARES exit leading to separation infringement</p>	<p>MAC-SC3</p>





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
				Note: MAC-SC3 corresponds to a situation where an imminent collision was prevented by ATC Collision prevention		
02: MT Management in Execution Phase	WOC fails to receive surveillance data or receiving inaccurate data	System error	Lost opportunity to take advantage of the Concept		None	No safety effect
	iRMT information is not timely displayed to PLN ATCO	System error	Risk for tactical conflict (not predictable based on flight plan info)	A iRMT will be created by ATC (Flight Data Operator) Tactical conflict resolution See above "iRMT not received by ATC"	HZ 02: MIL flight inbound a sector with short notice (from adjacent sector or ARES)	MAC-SC4b
	iRMT information displayed to PLN ATCO (strip) is not consistent with the Flight Deck one	System error Human error	Potential for conflict not timely detected by PLN ATCO (either MIL aircraft inbound sector from adjacent sector or MIL aircraft leaving ARES), due to Aircraft lateral deviation at a waypoint	Trajectory conformance monitoring tool (RAM/CLAM) Tactical conflict resolution	HZ 04: Conflict-inducing aircraft lateral deviation due to ground-airborne iRMT inconsistency	MAC-SC4a





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
	NM fails to receive surveillance data	*No change (as per current ops)				
	NM fails to receive ARES status	* No change (as per SESAR 1 RTSA V3)				
	Regional ASM fails to provide ASM support	* No change (as per SESAR 1 RTSA V3)				
	National ASM (AMC) fails to update and share ARES status	* No change (as per SESAR 1 RTSA V3)				





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
03: WOC triggered iRMT Revision	ATC fails to receive or to address or to agree the iRMT revision	System error Human error *Note: no FPL info is sent to NM once the FPL has been activated	The revision is not processed or not agreed by ATC. No safety effect as far as Flight Deck follows the current iOAT FPL (but performance effect on WOC)		None	No safety effect
	ATC (EAP – Extended ATC Planner or PLN ATCO) performs wrong iRMT update impact assessment (encompassing coordination with adjacent sectors/ACCs)	System error Human error *Same impact assessment as for the current one performed for civil flights	No change			





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
	Discrepancy between iRMT agreed via ATC-WOC CDM and the iRMT received by FD from WOC (encompassing the case of a mission abortion)	System errors Human errors CDM process & tool will be addressed within PJ07.03. Proposed Safety Requirement: the CDM process shall be designed such as to avoid iRMT discrepancy	Potential for conflict not timely detected by PLN ATCO (either MIL aircraft inbound sector from adjacent sector or MIL aircraft leaving ARES), due to Aircraft lateral deviation at a waypoint	Trajectory conformance monitoring tool (RAM/CLAM) Tactical conflict resolution	HZ 04: Conflict-inducing aircraft lateral deviation due to ground-airborne iRMT inconsistency	MAC-SC4a
	NM does not receive updated iRMT	System error	If multiple flights are affected, it might involve an inaccurate demand forecast with impact on NMF performance & potential for not timely detecting a Hotspot that might result in sector overload (in the context where sector capacity buffer will be reduced thanks to this Concept implementation)	Planning & tactical tasks under overload	HZ 01: Undetected incorrect traffic load data provided by Regional ATFCM to users (new contributor to already existing HZ-04 and similar to failure mode FLM-05 from Network Operations Safety Report NOSR v1.1 11/2017)	MAC-SC3 IM=0.4



Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
04: ATC triggered iRMT revision	ATC fails to provide or WOC fails to receive iRMT update information	System error Human error	No safety impact, just performance (Lost opportunity for WOC to take advantage of the Concept)		None	No safety effect
	ATC fails to provide or NM fails to receive iRMT update information	System error Human error	If multiple flights are affected, it might involve an inaccurate demand forecast with impact on NMF performance & potential for not timely detecting a Hotspot that might result in sector overload (in the context where sector capacity buffer will be reduced thanks to this Concept implementation)	Planning & tactical tasks under overload	HZ 01: Undetected incorrect traffic load data provided by Regional ATFCM to users (new contributor to already existing Hz-04 and similar to failure mode FLM-05 from Network Operations Safety Report NOSR v1.1 11/2017)	MAC-SC3 IM=0.4
	ATC fails to provide or adjacent ACCs fail to receive iRMT update information	System error Human error	Potential for conflict not timely detected by PLN ATCO (either MIL aircraft inbound sector from adjacent sector or MIL aircraft leaving ARES), due to Aircraft lateral deviation at a waypoint	Trajectory conformance monitoring tool (RAM/CLAM) Tactical conflict resolution	HZ 04: Conflict-inducing aircraft lateral deviation due to ground-airborne iRMT inconsistency	MAC-SC4a





Operating Method	Failure mode	Example of causes & new mitigations to prevent failure mode	Operational effect	Mitigations protecting against propagation of effects	Operational hazard	Severity
05: FD triggered iRMT revision	ATC provides wrong or incomplete impact assessment (encompassing coordination with adjacent sectors/ACCs)	System error Human error No change: Same impact assessment as for the current one performed for civil flights				
	ATC fails to provide or WOC fails to receive iRMT update information	Same as per process model 04				
	ATC fails to provide or NM fails to receive iRMT update information	Same as per process model 04				
	ATC fails to provide or adjacent sectors/ACCs fail to receive iRMT update information	Same as per process model 04				

Table 16 Full HAZID Working table

Founding Members



Appendix C Consolidated List of Safety Requirements

C.1 Safety Requirements (Functionality and Performance)

The safety assessment allowed the identification of two types of functionality & performance safety requirements:

1. Success approach (ensuring that the design enables safe operations in absence of failure within the Solution scope),
2. Failure approach (mitigating safety risk related to failure within the Solution scope).

The following table includes the “success approach” requirements, i.e. those requirements defined during the SPR-INTEROP/OSED development that have been identified in the SAFETY category as per the method explained at §4.2.3. Column 3 indicates the operational hazard(s) that might potentially occur in case the requirement were not satisfied, whilst Column 4 provides traceability to the related success Safety Objective(s).

Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-OP02.0002	Situational awareness to the Downstream En-Route/Approach ATS shall be provided about any updates to iRMT	Hz 02 Hz 04 Hz 05	SO 007 SO 009
REQ-07.03-SPRINTEROP-OP02.0003	The En-Route/Approach ATS shall have a possibility to revise iRMT	Hz 01 Hz 04	SO 006 SO 009
REQ-07.03-SPRINTEROP-OP02.0006	The En-Route/Approach ATS shall receive from Regional ATFCM iSMT/iRMT data based on latest validated iOAT FPL information (including modification messages) in order to allocate and manage the trajectories within respective AoR in execution phase via SWIM technical profile	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-OP02.1001	The ATC shall receive, process and develop requested iMT including demanded ARES configuration	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-OP02.1002	The ATC shall receive, process and develop requested iMT including demanded ARES configuration as ad-hoc ASM scenario with predefined ID	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 007 SO 009



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-OP02.1003	The ATC shall receive, process and develop requested iMT including the ARES flexible parameters in iMT profile description	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-OP02.1004	The ATC shall receive, to process and develop requested iMT profile irrespective of the GAT or OAT segments	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-OP02.1005	The ATC shall provide arrangements for NSF with WOC (AU)	Hz 02 Hz 04	
REQ-07.03-SPRINTEROP-IO02.0007	En-Route / Approach ATS shall be connected to all relevant ATM Nodes for iRMT Revisions distribution information exchange	Hz 02	SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO02.0008	En-Route / Approach ATS shall be connected to all relevant ATM Nodes for iRMT Revisions distribution information exchange. For any possible updates ADEXP/OLDI standards are used	Hz 02	SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO02.0009	En-Route / Approach ATS shall be connected to all relevant ATM Nodes for iRMT Revisions distribution information exchange during execution phase. Possible updates through SWIM technical profile	Hz 02	SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO02.0010	En-Route / Approach ATS shall be connected to receive iOAT FPL Mission Trajectory Data (iSMT/iRMT) and modification messages from Regional ATFCM	Hz 01 Hz 02 Hz 04	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO02.0011	En-Route / Approach ATS shall be connected to receive iOAT FPL Mission Trajectory Data (iSMT/iRMT) and modification messages from Regional ATFCM using improved OAT Flight Plan format	Hz 01 Hz 02 Hz 04	SO 004 SO 006 SO 007 SO 009



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-IO02.0012	En-Route / Approach ATS shall be connected to receive iOAT FPL Mission Trajectory Data (iSMT/iRMT) and modification messages from Regional ATFCM via SWIM technical profile	Hz 01 Hz 02 Hz 04	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO02.0016	The En-Route/Approach ATS shall connect to relevant systems to exchange initial Reference Mission Trajectory data including updates and revisions	Hz 01 Hz 04	SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO02.0017	The En-Route/Approach ATS shall exchange initial Reference Mission Trajectory data including updates and revisions. During transition for any trajectory updates ADEXP/OLDI standards are used	Hz 04	SO 009
REQ-07.03-SPRINTEROP-IE02.0001	iSMT - (Reception of Improved OAT-FPL information) Issuer <ul style="list-style-type: none"> Regional ATFCM (NMOC/IFPS) Intended Addressees <ul style="list-style-type: none"> Relevant civil & military (ATM, ATC) entities Information Element <ul style="list-style-type: none"> ATM Constraints ATM Environment Special Events (iOAT-FPL) Interaction Rules and Policy <ul style="list-style-type: none"> N/A Content Type <ul style="list-style-type: none"> Data Periodicity <ul style="list-style-type: none"> 24/24 On Demand Safety Criticality <ul style="list-style-type: none"> severe Maximum Latency <ul style="list-style-type: none"> Minutes (seconds) 	Hz 01	SO 002 SO 004



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-IE02.0002	iRMT (Update of filed iOAT FPL information)	Hz 02	SO 006
	Issuer <ul style="list-style-type: none"> • Regional ATFCM (NMOC/IFPS) Intended Addressees <ul style="list-style-type: none"> • Relevant civil & military (ATM, ATC) entities Information Element <ul style="list-style-type: none"> • ATM Constraints • ATM Environment • Special Events (iOAT-FPL) Interaction Rules and Policy <ul style="list-style-type: none"> • N/A Content Type <ul style="list-style-type: none"> • Data Periodicity <ul style="list-style-type: none"> • 24/24 • On Demand Safety Criticality <ul style="list-style-type: none"> • severe Maximum Latency <ul style="list-style-type: none"> • Seconds 	Hz 04	SO 007 SO 009
REQ-07.03-SPRINTEROP-IE02.0004	Send iRMT Revision Issuer <ul style="list-style-type: none"> • EN-Route/Approach ATS Intended Addressees <ul style="list-style-type: none"> • Flight Deck and Relevant civil & military (ATM, ATC, WOC, AD/C2) entities Information Element <ul style="list-style-type: none"> • iRMT Interaction Rules and Policy <ul style="list-style-type: none"> • N/A Content Type <ul style="list-style-type: none"> • Voice/Data Periodicity <ul style="list-style-type: none"> • 24/24 Safety Criticality <ul style="list-style-type: none"> • severe Maximum Latency <ul style="list-style-type: none"> • Seconds 	Hz 02 Hz 04	SO 007



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-OP03.1001	The Regional ATFCM shall process iOAT FPL and associated messages	Hz 01	SO 002SO 010
REQ-07.03-SPRINTEROP-OP03.1003	Regional ATFCM shall distribute all accepted iOAT FPLs and associated messages to all relevant civil and military entities in the IFPZ as today implemented for GAT FPLs	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-OP03.1004	Regional ATFCM shall apply ATM Network rules (e.g. RAD checking, AIP) to iOAT FPLs to validate their compliance with them within the IFPZ as today for GAT flights	Hz 01	SO 002
REQ-07.03-SPRINTEROP-OP03.1008	Regional ATFCM shall cross check that ARES data in iOAT FPL comply with ARES allocated via ASM process	Hz 01 Hz 02 Hz 04	SO 002
REQ-07.03-SPRINTEROP-IO03.1001	The Regional ATFCM shall provide interface for the data exchange of iOAT FPL and associated messages	Hz 01 Hz 02 Hz 04	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO03.1002	The Regional ATFCM shall process all standard data formats (ADEXP, XML) applicable to iOAT FPL and associated messages	Hz 01 Hz 02 Hz 04	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO03.1003	The Regional ATFCM shall exchange iOAT FPL and associated messages data via SWIM	Hz 01 Hz 02 Hz 04	SO 004 SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO03.1004	The Regional ATFCM shall provide interface to all AU for the iOAT FPL filing and submission	Hz 01 Hz 02	SO 001 SO 003



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-IO03.1005	The Regional ATFCM shall process all standard data formats (ADEXP, XML) applicable to iOAT FPL	Hz 01 Hz 02 Hz 04	SO 002 SO 004 SO 006 SO 009
REQ-07.03-SPRINTEROP-IO03.1006	Regional ATFCM shall ensure integration of iOAT FPL data for filing and submission via SWIM technical profile	Hz 01 Hz 02	SO 001 SO 003
REQ-07.03-SPRINTEROP-IO03.1007	Regional ATFCM shall provide interface for distribution of iOAT FPL and associated messages data alike for GAT FPL	Hz 01 Hz 02 Hz 04	SO 004 SO 006 SO 009
REQ-07.03-SPRINTEROP-IO03.1008	The Regional ATFCM shall distribute iOAT FPL and associated messages in standard data formats (ADEXP, XML)	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 009
REQ-07.03-SPRINTEROP-IO03.1009	The Regional ATFCM shall distribute iOAT FPL and associated messages in standard data formats (ADEXP, XML) through SWIM technical profile	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 009
REQ-07.03-SPRINTEROP-IO03.1010	Regional ATFCM shall provide interface for iMT data exchange between Regional and Sub-Regional/Local ATFCM	Hz 01 Hz 02	SO 004 SO 005 SO 006
REQ-07.03-SPRINTEROP-IO03.1011	The Regional ATFCM shall exchange iMT data in standard data formats (ADEXP, XML)	Hz 01 Hz 02 Hz 04 Hz 05	SO 004 SO 006 SO 009
REQ-07.03-SPRINTEROP-IO03.1012	The Regional ATFCM shall exchange iMT data with Sub regional/national ATFCM through SWIM technical profile	Hz 01 Hz 02	SO 004 SO 005 SO 006
REQ-07.03-SPRINTEROP-IO03.1013	Regional ATFCM shall provide interface for data exchange between environmental data and flight plan data processing systems	Hz 01	SO 002



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-IO03.1014	The Regional ATFCM shall apply data standards for exchange between environmental data and flight plan data processing systems	Hz 01	SO 002
REQ-07.03-SPRINTEROP-IO03.1015	The Regional ATFCM shall ensure exchange of data between environmental data and flight plan data processing systems via SWIM	Hz 01	SO 002
REQ-07.03-SPRINTEROP-IO03.0004	Regional ATFCM shall be connected to the WOC to receive Mission Trajectory data and answer with validation status	Hz 01 Hz 02	SO 001 SO 002 SO 003 SO 009
REQ-07.03-SPRINTEROP-IO03.0005	The WOC shall exchange Mission Trajectory data with Regional ATFCM using the improved OAT Flight Plan format	Hz 01 Hz 02	SO 001 SO 003
REQ-07.03-SPRINTEROP-IO03.0006	The WOC shall exchange Mission Trajectory data with Regional ATFCM through SWIM technical profile	Hz 01 Hz 02	SO 001 SO 003
REQ-07.03-SPRINTEROP-IE03.0001	<p>Submission of iOATFPL</p> <p>Issuer</p> <ul style="list-style-type: none"> • WOC or ATC in case of FPL revision in execution <p>Intended Addressees</p> <ul style="list-style-type: none"> • Regional ATFCM <p>Information Element</p> <ul style="list-style-type: none"> • iOAT FPL <p>Interaction Rules and Policy</p> <ul style="list-style-type: none"> • N/A <p>Content Type</p> <ul style="list-style-type: none"> • Data <p>Periodicity</p> <ul style="list-style-type: none"> • 24/24 <p>Safety Criticality</p> <ul style="list-style-type: none"> • severe <p>Maximum Latency</p> <ul style="list-style-type: none"> • Seconds 	Hz 01 Hz 02	SO 001 SO 003



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-IE03.0003	Distribution of improved OAT FPL Issuer <ul style="list-style-type: none"> Regional ATFCM Intended Addressees <ul style="list-style-type: none"> En-Route/Approach ATS(civil&military) Information Element <ul style="list-style-type: none"> iOAT FPL Interaction Rules and Policy <ul style="list-style-type: none"> N/A Content Type <ul style="list-style-type: none"> Data Periodicity <ul style="list-style-type: none"> 24/24 Safety Criticality <ul style="list-style-type: none"> severe Maximum Latency <ul style="list-style-type: none"> Seconds 	Hz 01 Hz 02 Hz 04 Hz 05	SO 006 SO 007 SO 009
REQ-07.03-SPRINTEROP-SF03.0003	iOAT FPLs shall be taken into account for Demand forecast prediction	Hz 01	SO 002 SO 004 SO 006 SO 010
REQ-07.03-SPRINTEROP-OP04.0004	The Flight Data Operator in the WOC shall submit the iSMT based on latest available Mission Trajectory data to the Regional ATFCM	Hz 01	SO 001
REQ-07.03-SPRINTEROP-OP04.0005	If changes to the content of a submitted initial Shared Mission Trajectory are needed, the Flight Data Operator shall submit updated initial Shared Mission Trajectory to Regional ATFCM	Hz 01	SO 001
REQ-07.03-SPRINTEROP-OP04.0006	If conditions for transition from initial Shared Mission Trajectory to initial Referenced Mission Trajectory are met, the Flight Data Operator in the WOC shall submit the initial Referenced Mission Trajectory to Regional ATFCM	Hz 01 Hz 02	SO 003



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-OP04.0011	If revision of an initial Referenced Mission Trajectory is needed, the Flight Data Operator in the WOC shall update the Mission Trajectory data	Hz 01 Hz 02	SO 003
REQ-07.03-SPRINTEROP-OP04.0012	The Flight Data Operator in the WOC shall submit the initial Referenced Mission Trajectory Revision Request based on latest available Mission Trajectory data to En-Route/Approach ATS	Hz 04	SO 003
REQ-07.03-SPRINTEROP-OP04.1002	The WOC shall be able to define the ARES configuration as ad hoc ASM scenario with pre-defined ID	Hz 01	SO 001 SO 003
REQ-07.03-SPRINTEROP-OP04.1003	The WOC shall be able to integrate the ARES flexible parameters in iMT profile description	Hz 01	SO 001 SO 003
REQ-07.03-SPRINTEROP-OP04.1004	The WOC shall be able to define the iMT profile irrespective of the GAT or OAT segments and submit it to Regional ATFCM	Hz 01 Hz 02	SO 001 SO 003
REQ-07.03-SPRINTEROP-OP04.1005	The WOC shall pre-validate filed iOAT FPL through the NM validation mechanism before final submission	Hz 01	SO 002
REQ-07.03-SPRINTEROP-IO04.0002	The WOC shall send Mission data update to the Flight Deck with standard phraseology	Hz 04	SO 009
REQ-07.03-SPRINTEROP-IO04.0003	The WOC shall send Mission data update to the Flight Deck via State AU internal communication means	Hz 04	SO 009
REQ-07.03-SPRINTEROP-IO04.0007	The WOC shall be connected to En-Route/Approach ATS to exchange initial Referenced Mission Trajectory data during execution phase	Hz 02	SO 003 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO04.0008	The WOC shall exchange initial Referenced Mission Trajectory data with En-Route/Approach ATS using ADEXP/OLDI format	Hz 02	SO 003 SO 007 SO 009
REQ-07.03-SPRINTEROP-IO04.0009	The WOC shall exchange initial Referenced Mission Trajectory data with En-Route/Approach ATS via AFTN	Hz 02	SO 003 SO 007 SO 009



Safety Requirement ID	Safety Requirement (functionality & performance) description	Related operational hazard(s)	Related success SO(s)
REQ-07.03-SPRINTEROP-IO04.0018	The WOC shall be connected to Regional ATFCM to exchange Mission Trajectory data	Hz 01	SO 001 SO 003
REQ-07.03-SPRINTEROP-IO04.0019	The WOC shall exchange Mission Trajectory data with Regional ATFCM using the iOAT FPL format	Hz 01	SO 001 SO 003
REQ-07.03-SPRINTEROP-IO04.0020	The WOC shall exchange Mission Trajectory data with Regional ATFCM through SWIM technical profile	Hz 01	SO 001 SO 003
REQ-07.03-SPRINTEROP-IE04.0005	<p>Send iRMT</p> <p>Issuer</p> <ul style="list-style-type: none"> • WOC <p>Intended Addressees</p> <ul style="list-style-type: none"> • Regional ATFCM <p>Information Element</p> <ul style="list-style-type: none"> • iRMT <p>Interaction Rules and Policy</p> <ul style="list-style-type: none"> • N/A <p>Content Type</p> <ul style="list-style-type: none"> • Data <p>Periodicity</p> <ul style="list-style-type: none"> • On Demand <p>Safety Criticality</p> <ul style="list-style-type: none"> • Major <p>Maximum Latency</p> <ul style="list-style-type: none"> • Minutes 	Hz 02	SO 003

Table 17 Safety Requirements (functionality and performance) from the “success approach”

The following Table 18 Safety requirements (functionality and performance) from the “failure approach” includes the “failure approach” requirements, i.e. those safety requirements aiming at mitigating the occurrence of the operational hazards (either preventing the occurrence of the cause or preventing the occurred cause to generate the hazard). Within the causal analysis §4.5.1, these safety requirements have been either identified (for the requirements already existing in the SPR-INTEROP/OSED when the safety assessment at the design level was initiated) or derived as new requirements (in which case they are **highlighted in bold**). In the table, the Column 3 shows the mitigated operational hazard.



Safety Requirement ID	Safety Requirement description	Derived from OH
REQ-07.03-SPRINTEROP-OP03.1002	Regional ATFCM shall provide the same options for filing and submission of iOAT FPL as for civil GAT FPL	SO 102
REQ-07.03-SPRINTEROP-SC04.0003	The supporting IT infrastructure SWIM and PENS shall transfer Flight Plan data without error	SO 102
REQ-07.03-SPRINTEROP-SF02.0001	ATCO procedures shall reflect the proper management of the iRMT	SO 101 SO 104
REQ-07.03-SPRINTEROP-SF02.0002	ATCO shall be properly trained in the management of the iRMT	SO 101 SO 104
REQ-07.03-SPRINTEROP-SF02.0003	Mission trajectory coordination and transfer of responsibility from one AoR to the other (i.e. ARES to ATC sector or ATC to ARES) shall be executed as a system to system –supported exchange in accordance with established standards & regulations (SYSCO)	SO 102 SO 104 SO 105
REQ-07.03-SPRINTEROP-SF03.0001	Regional ATFCM operator shall be alerted in case of connection failure with the relevant entities	SO 101
REQ-07.03-SPRINTEROP-SF03.0002	Local ATFCM actor shall be trained in the proper impact assessment of the mission trajectories	SO 103
REQ-07.03-SPRINTEROP-SF04.0001	In case of WOC system or connection failure preventing from iOAT FPL filing/updating, WOC operator shall file or update iOAT FPL by alternative means (e.g. phone, fax, mail etc.)	SO 101 SO 102
REQ-07.03-SPRINTEROP-SF04.0002	WOC shall be alerted via a lack of acknowledgement message in case the submitted iSMT/iRMT has not been received by the Regional ATFCM system	SO 101
REQ-07.03-SPRINTEROP-SF04.0003	Final coordination with regards to iRMT update shall be always between FC and ATCO	SO 104
SR_TS_001	Adequate SW assurance shall be ensured for the IFPS reception, processing & validation of the iSMT/iRMT by NM system”	SO 101 SO 102 SO 104



SR_TS_002	Adequate SW assurance shall be ensured for the distribution of the iSMT/iRMT	SO 101 SO 102 SO 104 SO 105
SR_TS_003	Adequate SW assurance shall be ensured for the demand forecast computation accounting for the iSMT/iRMT	SO 101
SR_TS_004	Adequate SW assurance shall be ensured for the reception, update, processing and distribution of the iSMT/iRMT by the ATC system	SO 101 SO 102 SO 104 SO 105
SR_TS_005	Adequate SW assurance shall be ensured for the processing and distribution of the iSMT/iRMT by the WOC system	SO 104
SR_TS_006	ATC system jointly with ASM system shall be able to identify any inaccurate iRMT distribution within the ATC system including the appropriate activated/deactivated ARES entry and exit points	SO 102
SR_TS_007	Adequate SW assurance shall be ensured for the reception and processing of the iSMT/iRMT by the Local ATFCM system	SO 101 SO 103

Table 18 Safety requirements (functionality and performance) from the “failure approach”

C.2 Safety Requirements (Integrity)

The Safety Requirements (integrity/reliability) for the execution phase will be derived based on more in-depth safety assessment in further lifecycle steps outside the scope of initial V3 (as a refined design needs to be specified in the V3 TS/IRS and the associated NSV-4 EATMA models).

Appendix D Assumptions, Safety Issues & Limitations

D.1 Assumptions log

The following Assumptions were necessarily raised in deriving the above Functional and Performance Safety Requirements:

Ref	Assumption	Validation
A001	As per current operations, WOC is alerted via a lack of acknowledgement message in case the submitted iOAT FPL has not been received by the Regional ATFCM system	Validated by expert judgement during the WebEx meeting 17/06/19
A002		

Table 19: Assumptions log

D.2 Safety Issues log

The following Safety Issues were necessarily raised during the safety assessment:

Ref	Safety issue	Resolution
I001	To clarify system design & procedures such as to ensure that a mission will not fly without iRMT	Open issue
I002		

Table 20: Safety Issues log

D.3 Operational Limitations log

The following Operational Limitations were necessarily raised during the safety assessment:

Ref	Operational Limitations	Resolution
L001		
L002		

Table 21: Operational Limitations log



-END OF DOCUMENT-

