INDUSTRIAL RESEARCH

sesar JOINT UNDERTAKING

SESAR Solution PJ04-W2-28.1 SPR-INTEROP/OSED for V3 - Part II - Safety Assessment Report

Deliverable ID:	**D2.1.050**
Dissemination Level:	**PU**
Project Acronym:	**PJ.04-W2 Solution 28.1**
Grant:	**874472**
Call:	**H2020-SESAR-2019-1**
Topic:	**SESAR-IR-VLD-WAVE2-04-2019**
Consortium Coordinator:	**ADP (SEAC2020)**
Edition Date:	**30 August 2022**
Edition:	**00.00.01**
Template Edition:	**00.00.03**

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Authoring & Approval

Authors of the document

Beneficiary	Date
EUROCONTROL	30/08/2022

Reviewers internal to the project

Beneficiary	Date
Swedavia (SEAC2020)	09/09/2022
LFV	
INDRA	

Reviewers external to the project

Beneficiary	Date
PJ19 partners	

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

Beneficiary	Date
EUROCONTROL	30/08/2022
INDRA	Silent Approval
LFV/COOPANS	Silent Approval
DLR(AT-One)	Silent Approval
NLR(AT-ONE)	Silent Approval
PANSA(B4)	Silent Approval
ENAIRE	Silent Approval
LDO	Silent Approval
SINTEF(NATMIG)	Silent Approval
MUC(SEAC2020)	14/09/2022
ADP(SEAC2020)	Silent Approval
SNBV(SEAC2020)	Silent Approval
ZRH(SEAC2020)	Silent Approval
AVINOR(SEAC2020)	Silent Approval
SWED(SEAC2020)	Silent Approval
THALES AIR SYS	15/09/2022

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Rejected By - Representatives of beneficiaries involved in the project

Beneficiary	Date
None	

Document History

Edition	Date	Status	Beneficiary	Justification
00.00.01	30/08/22			

EUROPEAN PARTNERSHIP

Co-funded by the European Union

PJ.04-W2 Solution 28.1

[CONNECTED REGIONAL AIRPORTS]

This document is part of a project that has received funding from the SESAR Joint Undertaking under grant agreement No 874472 under European Union's Horizon 2020 research and innovation programme.

Abstract

The Connected Regional Airports focus is on the integration of the regional airports into the network through the sending of DPI messages and the implementation of a quasi-automatic milestone surveillance process, reducing the workload of airlines / ground handlers and increasing the predictability.

This document is the solution PJ.04-W2-28.1 SPR-INTEROP/OSED V3 document – Part II – interim edition prior to the final version being submitted as part of the 28.1 Data Pack nearer to the conclusion of Wave 2. Solution 28.1 builds on the (V2) work performed in SESAR1 specifically in relation to SESAR Solution PJ.04-1 "Enhanced Collaborative Airport Performance Planning and Monitoring" developed from the SESAR Solution 21 (Airport Operations Plan and AOP-NOP Seamless Integration).

Table of Contents

List of Tables

EUROPEAN PARTNERSHIP

Co-funded by the European Union

EUROPEAN PARTNERSHIP

Co-funded by the European Union

1 Executive Summary

This document contains the Specimen Safety Assessment for a typical application of the Regional Network Integrated Solution. The Safety Assessment Report (SAR) represents Part II of the SPR-INTEROP/OSED document and presents the assurance that the Safety Requirements for the V1-V3 phases are complete, correct and realistic, thereby providing all material to adequately inform the Regional Network Integrated Solution SPR-INTEROP/OSED and TS/IRS.

Solution 28.1 seeks to integrate the regional airports into the network through a turnaround process monitoring and including specifically the notion of automated milestone generation in an A-CDM context. It could provide sufficient motivation for regional airports to enhance overall network predictability, reducing substantially the workload and obtaining the benefits of the A-CDM (such as greater predictability and network integration inputs).

The milestone process of A-CDM has been simplified, reducing the milestones, decreasing the complexity of the definition and the operation under this new concept. The inputs by the Ground Handlers / Aircraft Operators have been reduced as a result of automatic determination of the Target Off block time (TOBT) based on the aircraft event-based milestones to ease the process and adapt it to the operations volume of the regional airports. A DMAN (Pre-Departure Sequence) is not mandatory; therefore, the milestones associated are not required either.

The applicability to regional airports is reliant on the high degree of predictability of airport parameters including taxi-times, turnaround times and passenger boarding times. These parameters will be de fined by the regional airports based in their own experience and the historical data, taking into account those variables they consider appropriate to assure the high predictability of the values. Nevertheless, a recommendation is made in this document.

This Safety Assessment Report (SAR) is contributing to the Operational Service and Environment Definition (OSED)/Safety and Performance Requirements (SPR)/Interoperability (INTEROP). As such it is not a self-contained document. It requires to have at hand the referenced documents.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

2 Introduction

2.1 Background

Previous work performed on the new operating method as described within this document was done under the auspices of SESAR1 PJ.04-1. Details on the concept description can be found in:

- SESAR Solution PJ.04-01 SPR-INTEROP/OSED for Part I [7]
- SESAR Solution 04.01 SPR-INTEROP/OSED - Part V - Performance Assessment Report (PAR) [8]

Under SESAR1 PJ.04-1 there was no work in the development of OSED Part II SAR, therefore this approach is new and not based in any previous work.

This document contains the Specimen Safety Assessment for a typical application of the PJ.04-W2-28.1 Solution and is the part II of the SPR-INTEROP/OSED deliverable. The report presents the assurance that the Safety Requirements for the V3 phases are complete, correct and realistic.

Solution PJ.04-W2-28.1 addresses the following OI:

- AO-0824: Regional network-integrated airports (RNI)

2.2 General Approach to Safety Assessment

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

- A success approach which is concerned with the safety of the Solution service provision in the absence of failure within the end-to-end Solution Functional System, encompassing both Normal operation and Abnormal conditions,
- A conventional failure approach which is concerned with the safety of the Solution service provision in the event of failures within the end-to-end Solution Functional System.

These two approaches are applied to the derivation of safety properties at each of the successive lifecycle stages V2 and V3 of the Solution development (Safety Requirements at service level and at design level).

This Safety Assessment Plan is based on the results of the Safety & HP Scoping & Change Assessment process described in Guidance C of the Guidance to apply SESAR Safety Reference Material [3] complemented by the more recent relevant guidance available in the STELLAR Slideboard Safety part. This preparatory process clarifies the scope of the Change (Solution versus Reference), identifies the main safety issues associated with the specific Solution, identifies the design safety drivers for the Solution and helps in deciding the safety assessment activities required for that type of change.

2.3 Scope of the Safety Assessment

The following parts of the safety assessment lifecycle are covered by the current issue of the Safety Plan and consequently of the safety assessment work to be undertaken and finally documented in the Safety Assessment Report (SAR) for V3:

Co-funded by the European Union

- Initial identification of safety implications of the Change
- Identification and establishment of a set of **Safety Requirements at ATS Service level (SRS)** (Developed in this Document)
- Derivation of **Safety Requirements at design level** (**SRDs at SPR and TS level**) to satisfy the SRSs (based on combined safety analysis of the design, and safety-related measurements, observations and debriefing of the validation exercises). 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 SPR-INTEROP/OSED and TS/IRS documents for the design of the Functional system for the Solution (encompassing people, procedures & airspace and equipment). **Only for the technical elements** of the Functional system design, the safety requirements will be derived at two levels: initial design level (high level technical elements in the SPR) and refined design level (Functional Blocks in the TS out of which the high level technical elements are built), whilst ensuring requirements traceability of the latter towards the initial design level requirement(s). The V3 safety assessment outcomes will be documented in successive versions of the Safety Assessment Report (SAR).

2.4 Layout of the Document

The layout of this Safety Assessment report is as follows:

- **Section 1** presents the executive summary of the document.
- **Section 2** provides background information regarding the definition, design and validation addressed in the PJ.04-W2-28.1 Concepts, the principles for safety assessment in SESAR Programme and the scope of this safety assessment
- **Section 3** provides the main information collected within the SAF&HP Scoping and Change assessment and Safety Assessment Plan development process in order to set the scene for the safety assessment documented in the SAR.
- **Section 4** presents the Safety Requirements at Service level for the corresponding “Other than ATS” operational Solution.
- **Section 5** documents the Safety Requirements at Design level (SRDs) for the corresponding “Other than ATS” operational Solution.
- **Section 6** shows the extent to which the achievability of the SRS has been demonstrated through the satisfaction of the success criteria of the safety validation objectives defined in relation to the Solution planned validation exercises or other specific validation means (e.g. data analysis, Safety and/or HP workshops).
- **Appendix A** presents the definition of the SRS (functionality and performance) in order to set the Service Safety Specification under normal (i.e. those conditions that are expected to occur on a day-to-day basis) and abnormal conditions of operation.
- **Appendix B** presents the results of the risk assessment done at the service specification level, including service hazards identification and assessment in view of deriving additional SRS.
- **Appendix C** shows how the Safety Requirements at Service level (SRS) for normal and abnormal conditions of operation derived in sections 4.2 and 4.3 map onto the related elements of the Design Model (functional system components or interactions/data flows) and

derive Safety Requirements at Design level (SRD) (functionality and performance) for normal and abnormal conditions of operation.

- **Appendix D** presents the detailed risk evaluation and mitigation of the Service Hazards from section 4.4 performed at the level of the design of the solution functional system.
- **Appendix E** includes all the assumptions that were necessarily raised in deriving the above Safety Requirements, safety issues that were necessarily raised during the safety assessment and the operational limitations that were raised in the safety assessment.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

3 Setting the Scene of the safety assessment

3.1 Operational concept overview and scope of the change

Regional Network Integrated Airports (RNI Airports) solution is a cost-efficient way of achieving the connection with the NM reducing the effort of the Stakeholders compared to the one of a full A-CDM operation. As such, the only pre-requisite for a targeted regional airport is the availability of an Airport Operational Database (AODB).

This Solution is aiming at improving the connectivity between regional airports and the NMOC thanks to the provision of DPI messages based on target times and a reduced set of turnaround milestones compared to the full A-CDM implementation. The applicability to regional airports is reliant on the high degree of predictability of airport parameters including taxi-times, turnaround times and passenger boarding times. Ground handler workload is reduced as a result of automatic determination of the aircraft-ready time (TOBT) based on the aircraft event-based milestones and the status of the passenger boarding provided by the local airport system.

For more detail on the operational concept go to SESAR Solution PJ04-W2-28.1 SPR-INTEROP/OSED for V3 - Part I.

3.2 Solution Operational Environment and Key Properties

The airports considered in this OSED are part of the category defined as “Medium Airports” which Parent Operating Environment is the “Airport Category“, as defined in the EATMA.

A Medium Airport Operating Environment corresponds to the aerodrome movement area and the volume of controlled airspace around an airport with a number of annual movements greater or equal to 40.000 and less than 150.000, where a movement is either an IFR departure or an IFR arrival.

3.3 Stakeholders’ expected benefits with potential Safety impact

Benefits can be expected for each of the principal airport stakeholders as a result of implementation of the RNI concept, but there is one key benefit regrading safety, the reduction in the workload of ATC with a predefined pre-departure sequence that will reduce the congestion in the airside improving the safety during the operation.

3.4 Intended Operational use of the Service Concept

3.4.1 Intended use identified from SESAR Operational Solutions

This sections does not apply, this solution so far is a standalone solution.

3.4.2 Other intended use outside-SESAR

This sections does not apply, this solution so far is a standalone solution.

3.5 Relevant applicable standards

Co-funded by the European Union

Several existing standards ensure the interoperability of the technical systems that will be developed by the industrial partners to implement the concept and the functionality of the solution. Further, by having the standard in place, a set of data elements with defined quality are considered to be available. Below a (non-exhaustive) overview of the applicable standards and regulations is provided.

3.5.1.1 A-CDM

There is currently no implementing rule for A-CDM (yet) but there is a European Standard (ETSI EN 303 212) "Airport Collaborative Decision Making (A-CDM); Community Specification for application under the Single European Sky Interoperability Regulation EC 552/2004" [10]

In addition, several EUROCAE (European Organisation for Civil Aviation Equipment) documents (European Standards) of relevance are:

- ED-141 System Requirements Document [11]
- ED-145 Interface Definition Document [12]
- ED-146 Test and Validation Document [13]

These are considered to ensure interoperability between technical system enablers, when adhered to.

3.5.1.2 Single European Sky

PJ.04-W2-28.1 will need to take account of the Single European Sky Interoperability Regulation (EC 552/2004) [10] and amended (SES2) by regulation EC 1070/2009 [15]. Specifically the pillars relating to managing capacity on the ground as well as EC Implementing Rule IR390/2013 [16] laying down a performance scheme for air navigation services and network functions with respect to the airport-related KPIs ([16] - Annex 1).

3.5.1.3 Environmental

Several EU Regulations and Directives already constrain aviation and airports current operations and future development, and at least impose airports to monitor their impact notably on noise and ambient air quality:

- The Regulation No 598/2014 of 16 April 2014 on the establishment of rules and procedures with regard to the introduction of noise-related operating restrictions at Union airports within a balanced approach and repealing Directive 2002/30/EC [14]
- The Directive No 2002/49/EC of 25th June 2002 relating to the assessment and management of environmental noise [17]
- The Directive No 2008/50/EC of 21st May 2008 on ambient air quality and cleaner air for Europe [18]
- The Directive No 2016/2284 of 14 December 2016 on the reduction of national emissions of certain atmospheric pollutants, amending Directive 2003/35/EC and repealing Directive 2001/81/EC, the National Emission Ceilings Directive (NEC Directive) from the date of its transposition (30 June 2018) ensuring that the emission ceilings for 2010 set in that Directive shall apply until 2020 [19]

Co-funded by the European Union

Additional national or local regulations might also impose other constraints and obligations on airports. For example, the French Law No2015-992 [20] (and particularly Article 45) obliges larger French airports to take immediate action to reduce their emissions (by -10% in 2020, and -20% by 2025 compared to 2010).

3.5.1.4 Common Project One

Commission Implementing Regulation (EU) 2021/116 of 1 February 2021 on the establishment of the Common Project One supporting the implementation of the European Air Traffic Management Master Plan provided for in Regulation (EC) No 550/2004 of the European Parliament and of the Council. Amends Commission Implementing Regulation (EU) No 409/2013 and repeals Commission Implementing Regulation (EU) No 716/2014 (Text with EEA relevance)

Co-funded by the European Union

4 Safety specification at Service level

4.1 Overview of activities performed

This section addresses the following activities:

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

4.2 Service Safety specification – Normal conditions of operation

The SRS (functionality&performance) for normal conditions of operation are derived taking into account:

- All relevant Use Cases
- EATMA Models at operational specification level (NOV-5 diagrams).
- Impact on neighbouring ATM Systems.

The design characteristics/items of the Solution functional system should not be considered at this level but at the design level (in section 5.2), when the derived SRSs will enable the derivation of the Safety Requirements at Design level (SRD). For more detail on the SRS please go to Appendix A.

SRS ID	SRS for Normal conditions of operation
SRS 001	AUs/GHs shall submit (and resubmit if any update is needed) the FPL in time for enabling reliable traffic prediction
SRS 002	AUs/GHs shall assure the integrity of the data that will undergo through a system check to assure it
SRS 003	Airport Operator shall assure the integrity of the data contained in an E-DPI that will be used by the NM
SRS 004	Airport Operator shall assure the integrity of the data contained in a T-DPI-t that will be used by the NM
SRS 005	NM shall assure the integrity of the data contained in a FUM that will be used by the Airport Operator for the whole A-CDM process computation
SRS 006	AUs/GHs shall assure the integrity of the TOBT declared, which will feed the PDS and will be used for Resource allocation
SRS 007	Stakeholders shall assure the integrity of any milestone an aircraft goes through (e.g. ACGT) provided to the RNI platform with the correct procedures

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SRS ID	SRS for Normal conditions of operation
SRS 008	ATC shall assure the integrity of the TSAT declared in case a Departure Manager is available
SRS 009	Airport Operator shall assure the integrity of the data contained in a T-DPI-s that will be used by the NM
SRS 010:	Airport Operator shall assure the integrity of the data contained in a C-DPI that will be used by the NM

Table 1: List of SRS (functionality and performance) for normal conditions of operation

4.3 Service Safety specification - Abnormal conditions of operation

The SRS (functionality&performance) for abnormal conditions of operation are derived taking into account:

- All relevant Use Cases
- EATMA Models at operational specification level (NOV-5 diagrams).
- Impact on neighbouring ATM Systems.

The design characteristics/items of the Solution functional system should not be considered at this level but at the design level (in section 5.2), when the derived SRSs will enable the derivation of the Safety Requirements at Design level (SRD). For more detail on the SRS please go to Appendix A.

SRS ID	SRS for abnormal conditions of operation
SRS 011	Whenever RNI platform Servers are down, a degraded mode shall be provided in which the information shall be migrated to another server with limited capabilities that will allow the operation to continue but with restricted mechanics
SRS 012	Whenever the AU/GH data is not received partially, Stakeholders shall assure that there is the possibility to introduce this data manually to assure the consistency and integrity of the RNI model. In case ATC could not provide their data, there is the possibility to be introduced, but, if the workload is considered too high, it shall be avoided and ATC data will be incomplete reducing the benefits gained in the RNI model. It shall be assured that the DPIs emission to the NMOC is not compromised, if it is, then we are talking about a failure condition in the “Provision of departure planning information to the NM” service

Table 2: List of additional SRS for Abnormal conditions of operation

4.4 Mitigation of the System-generated Risks (failure conditions)

4.4.1 Service Hazards identification and analysis

Present in this section the consolidated results from the hazard identification, analysis and HAZID workshop (detailed working table, results and HAZID workshop participation are included in Appendix B).

Co-funded by the European Union

ID	Service Hazard Description	Operational Effects	Mitigation of effects propagation	Severity *(most probable effect)*
SH 01	RNI platform failure	Impossibility to provide the service "Provision of departure planning information to the NM" and local RNI procedures out	A DPI real-time monitoring tool will allow, when DPI are lost or not adequate, detect a potential anomaly and revert NM operation to using FPL data for trajectory prediction.	Planned Tactical conflict (MF5.1); MAC-SC4b
SH 02	RNI platform AOP-NOP Connection failure	Impossibility to provide the service "Provision of departure planning information to the NM "	A DPI real-time monitoring tool will allow, when DPI are lost or not adequate, detect a potential anomaly and revert NM operation to using FPL data for trajectory prediction.	Planned Tactical conflict (MF5.1); MAC-SC4b
SH 03	RNI platform data integration failure	Impossibility to provide the service "Provision of departure planning information to the NM" and local RNI procedures out	A DPI real-time monitoring tool will allow, when DPI are lost or not adequate, detect a potential anomaly and revert NM operation to using FPL data for trajectory prediction.	Planned Tactical conflict (MF5.1); MAC-SC4b

Table 3: Service Hazards and Analysis

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

SRS ID	Additional Safety Requirements at Service level *(functionality & performance)*	Mitigated Service Hazard
SRS 013	Provision of a DPI real-time monitoring tool that in case of degraded DPI information provision, when DPI are lost or not adequate, it detects a potential anomaly and stops the reception of DPIs, reverting the NM procedures back to using FPL data for trajectory prediction (similarly to the case of A-CDM airports) – performance degraded, but safety ensured.	SH 01; SH02 and SH 03

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Table 4: Additional SRS (functionality and performance) to mitigate Service hazards effects

4.5 Process assurance of the Safety Specification at service level

For more detail on this section content access the Appendix A and B of the Document.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

5 Safe Design of the Solution functional system

The purpose of this section is to document the Safety Requirements at Design level (SRDs) for the corresponding “Other than ATS” operational Solution.

The SRDs are design characteristics/items of the Solution functional system to ensure that the system operates as specified and is able to achieve the SRS (because based on the verification/demonstration of these characteristics/items, it could be concluded that the SRS are met, i.e. the Design safety drivers are satisfied).

Safety requirements at design level (SRD) are to be placed on the elements of the Solution functional System that are changed or affected by the change (through change in behaviour or through new interactions introduced).

The derived SRDs are to be consistent with the set of requirements produced by the Solution team in charge of SPR-INTEROP/OSED Part I (Section 4) and completeness and correctness of the full set of SRDs with regards to the satisfaction of the SRSs is to be shown.

5.1 Overview of activities performed

This section addresses the following activities:

- Introduction of the design model (initial or refined) of the Solution functional system – section 5.2
- Derivation of Safety Requirements (functionality & performance) at Design level (SRD) in normal and abnormal conditions of operation from the SRS (functionality and performance) of sections 4.2 and 4.3, and supported by the analysis of the initial or refined design model - section 5.3
- Assessment of the adequacy of the design (initial or refined) in the case of internal failures and mitigation of the Solution service hazards (identified at section 4.4.1) through derivation from SRS (integrity & reliability) of Safety Requirements (functionality & performance) and Safety Requirements (integrity&reliability) at Design level (SRD)- section 5.4
- Realism of the refined safe design (i.e. achievability and “testability” of the SRD) - section 5.5
- Safety process assurance at the initial or refined design level – section 5.6”.

5.2 Design model of the Solution Functional System

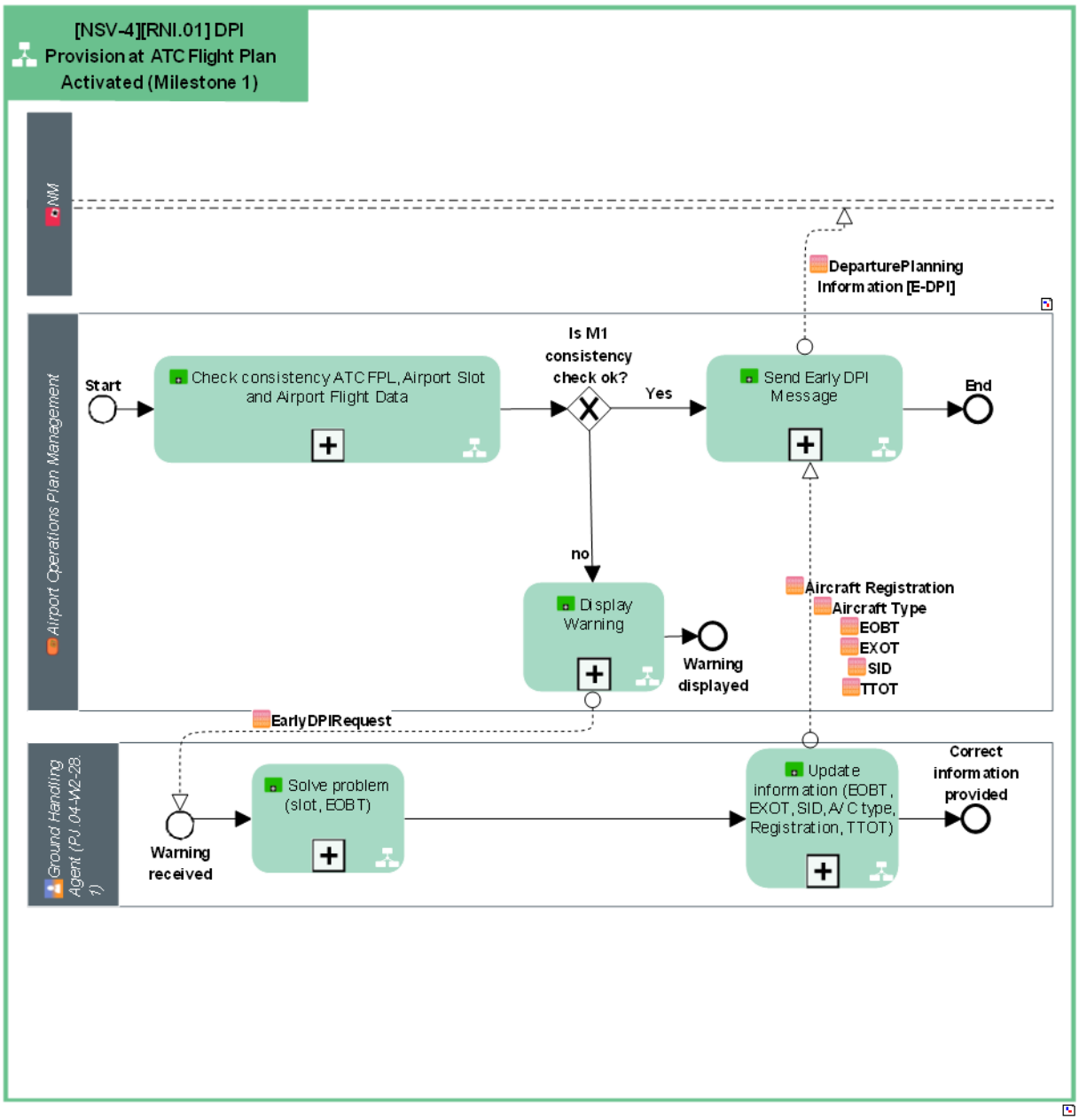
This sections contains the Design Model of the Solution functional system, which is a high-level architectural representation of the Solution system design.

5.2.1 Description of the Design Model

5.2.1.1 [NOV-5][RNI.01] DPI Provision at ATC Flight Plan Activated (Milestone 1)

The RNI airport shall send automatically an E-DPI (Early) Message to NMOC at EOBT-3h with EOBT, EXOT, SID, Aircraft Type, Registration, TTOT (=EOBT+EXOT).

The transmission of an E-DPI Message confirms to NMOC that an airport slot and flight plan for a particular flight has been correlated in accordance with local rules at the airport.



5.2.1.2 [NOV-5][RNI.02] DPI Provision at Take Off from Outstation (Milestone 3)

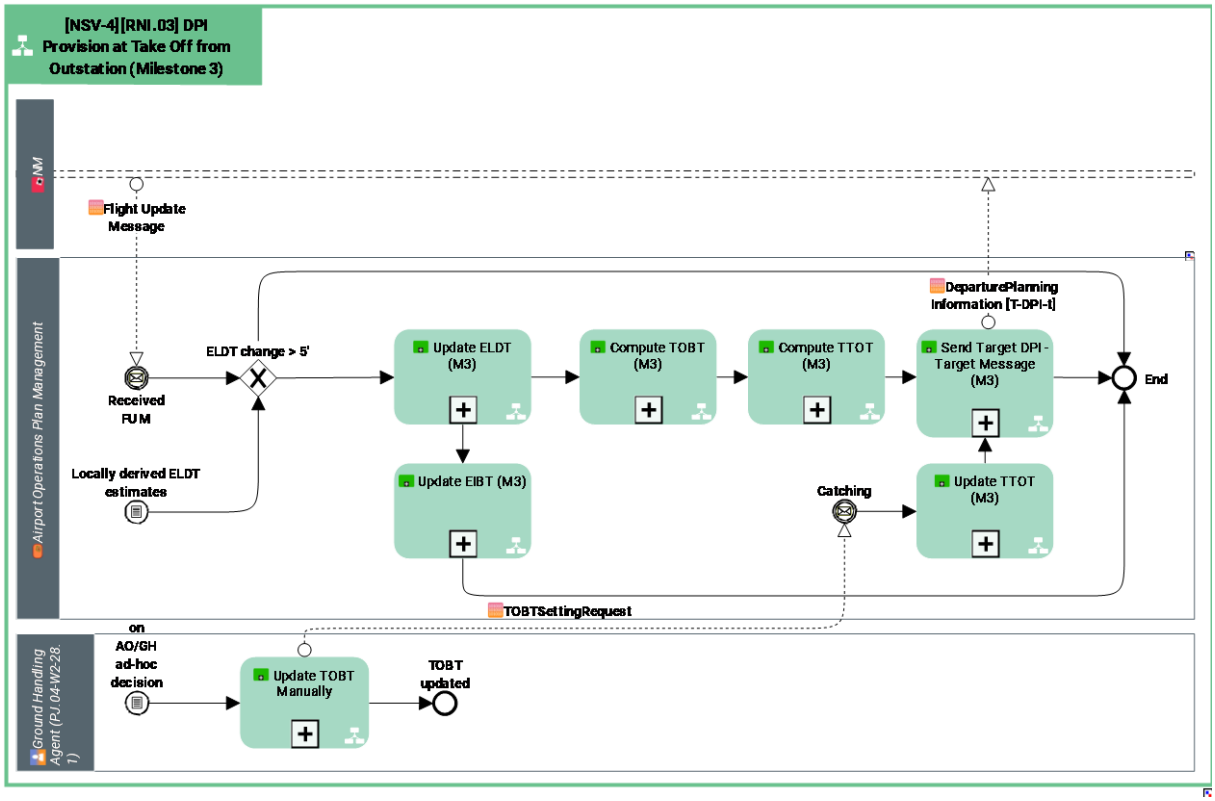
When a flight inbound to the RNI airport takes off from the outstation (status = 'airborne'), an initial TOBT and TTOT shall be calculated based on the latest time between EOBT and ELDT+EXIT+XTTA. And TTOT = TOBT+EXOT.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

If the departure airport is more than 3hrs flying time from the destination airport the ATOT is received from either the Network Operations FUM or via the Aircraft Operator or Ground Handling Agent. Using the ATOT an ELDT can be calculated by using the Estimated Elapsed Time on the FPL.

If the flight is within 3hrs flying time of the destination airport, NMOC monitors progress of the flight and send FUM Messages to provide updated ELDT.



5.2.1.3 [NOV-5][RNI.03a] DPI Provision at Ground Handling Started without PDM (Milestone 6 to 9)

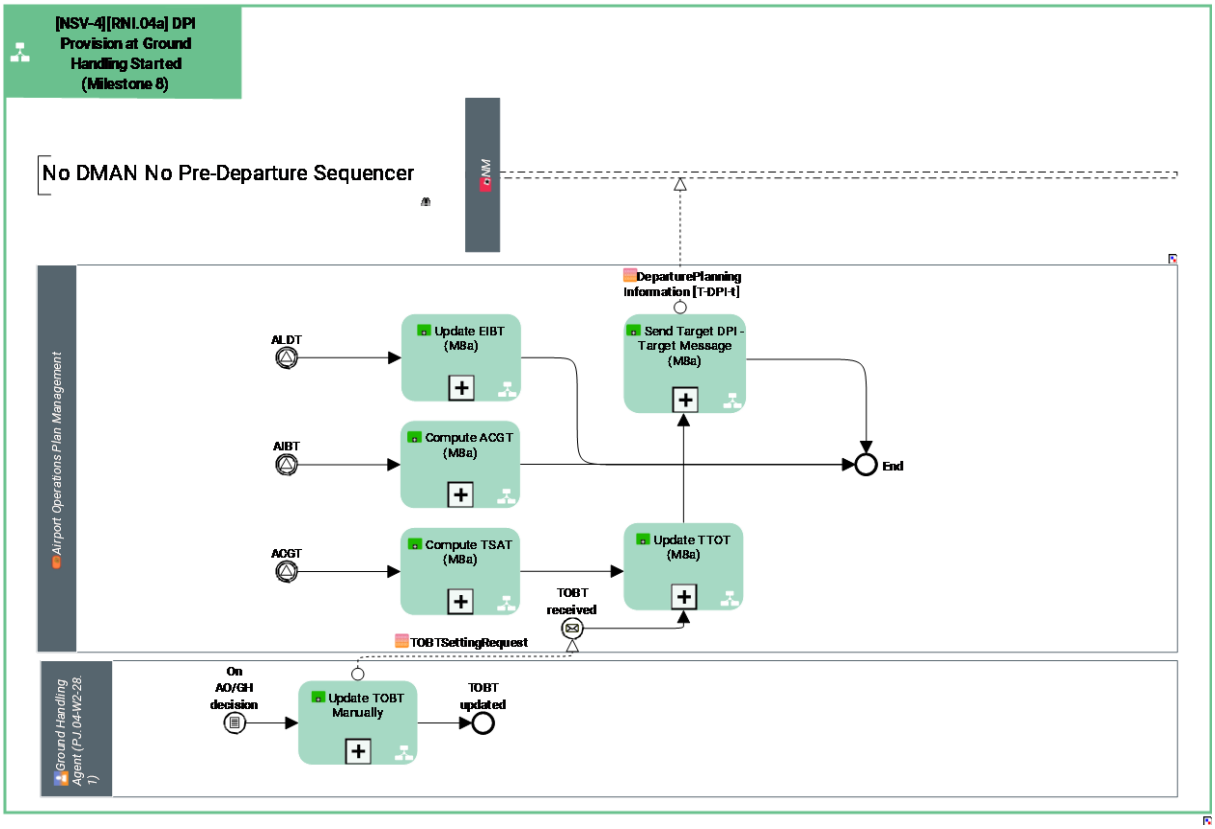
This UC covers the case where no DMAN exists at the airport, but it may exist or not a PDS.

For flights that are on a normal turn-round (SOBT-AIBT) < 2h, Actual Commencement of Ground Handling Time (ACGT) = AIBT.

Use of SOBT and EOBT caters for the case of aircraft on a 'long' turnaround such as a night stop. ACGT = MAX(SOBT,EOBT) - XTTA.

SOBT is the scheduled off-block time, EOBT the latest estimated off-block time and XTTA is derived from the RNI database for the flight in question.

EUROPEAN PARTNERSHIP
Co-funded by the European Union



5.2.1.4 [NOV-5][RNI.03b] DPI Provision at Ground Handling Started with PDM (Milestone 6 to 9)

This UC covers the case where a DMAN is in operations at the airport.

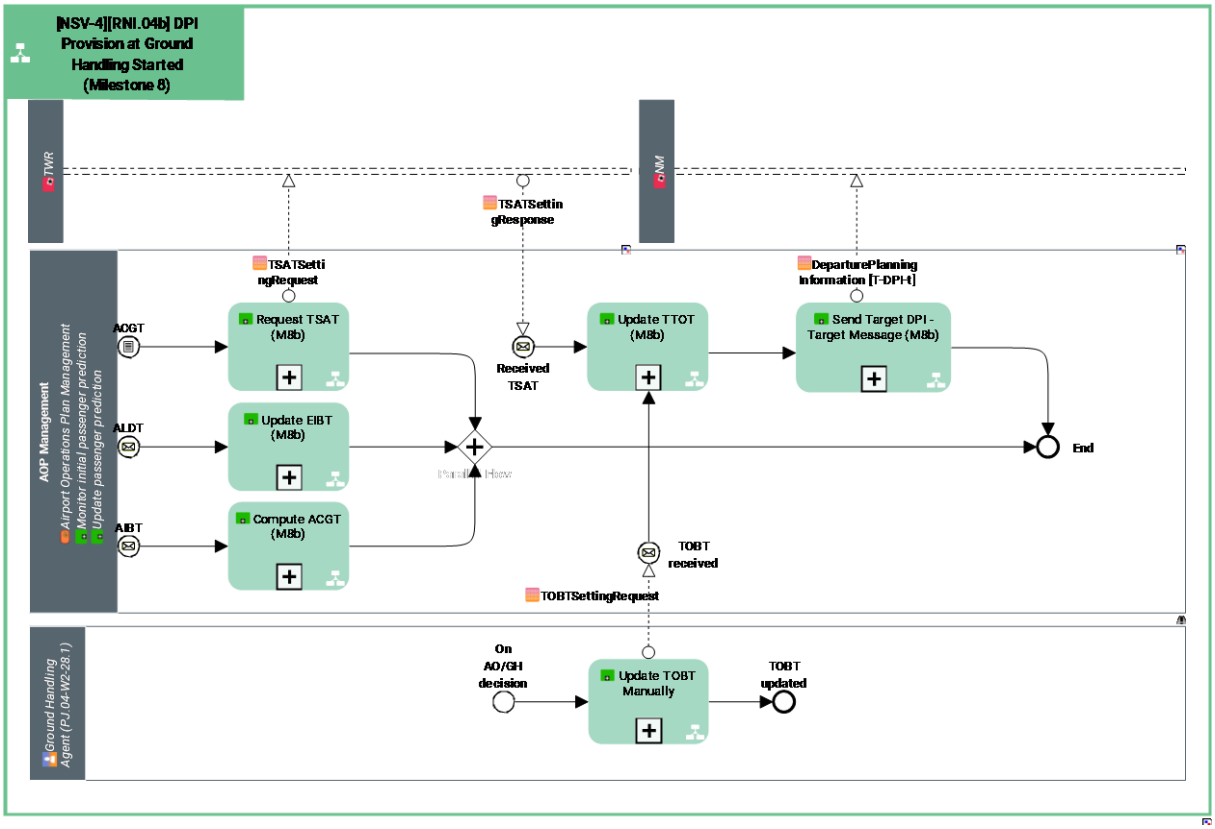
For flights that are on a normal turn-round (SOBT-AIBT) < 2h, Actual Commencement of Ground Handling Time (ACGT) = AIBT.

Use of SOBT and EOBT caters for the case of aircraft on a 'long' turnaround such as a night stop. ACGT = MAX(SOBT,EOBT) - XTTA.

SOBT is the scheduled off-block time, EOBT the latest estimated off-block time and XTTA is derived from the RNI database for the flight in question.

EUROPEAN PARTNERSHIP

Co-funded by the European Union



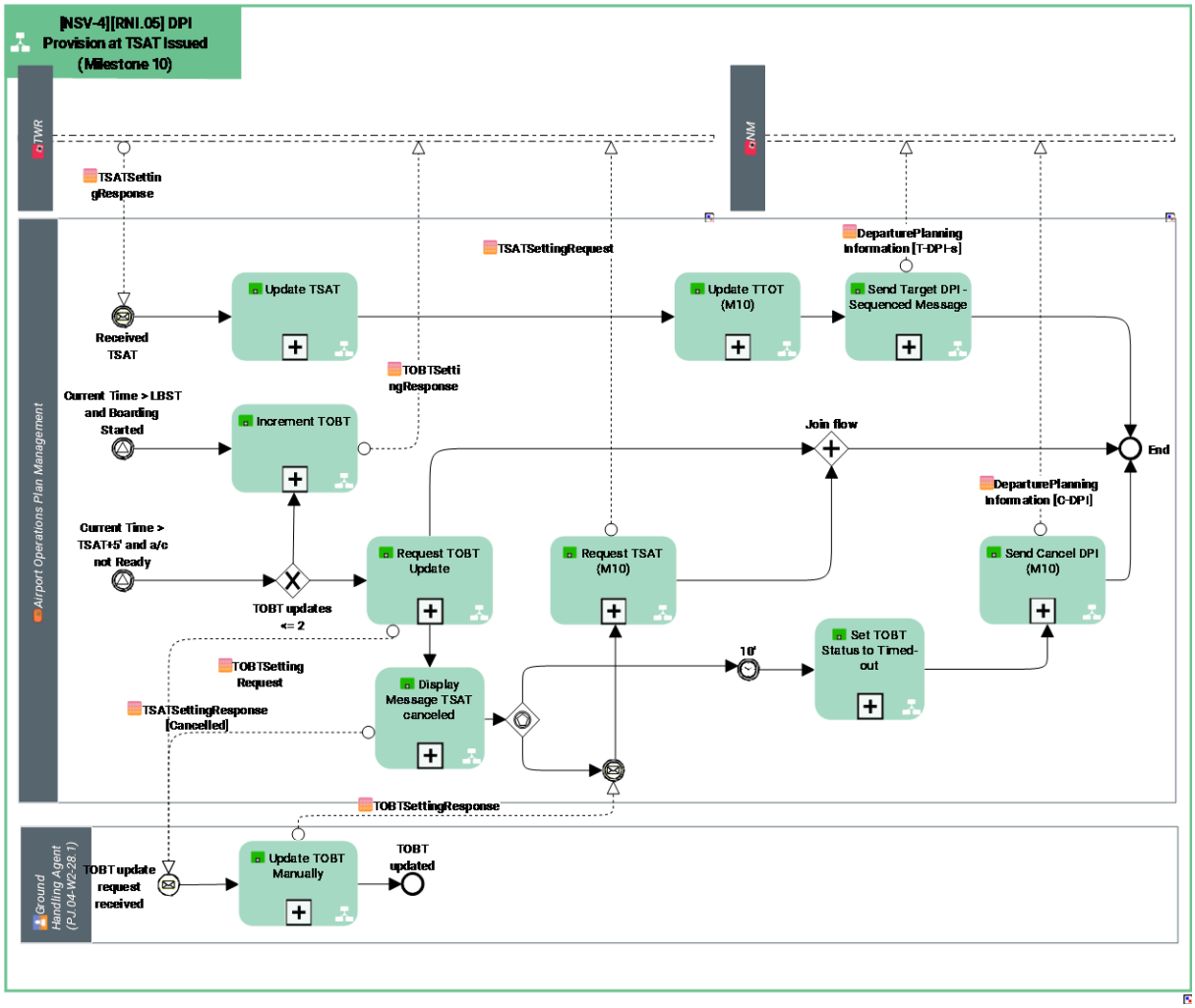
5.2.1.5 [NOV-5][RNI.04] DPI Provision at TSAT Issued (Milestone 10 and 11)

The RNI airport sends automatically a T-DPI-s (Sequenced) Message to NMOC at local implementation definition (A-CDM manual recommends between TOBT-40' and TOBT-30') with TTOT calculated with TSAT (output from the pre-departure sequence) and EXOT.

The inputs for the Pre-departure Sequence are the TOBT+Taxi-Time (EXOT) (for non-regulated flights), the CTOT (for regulated flights) and any Airport constraints. The output of the Pre-Departure Sequence is the TSAT.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

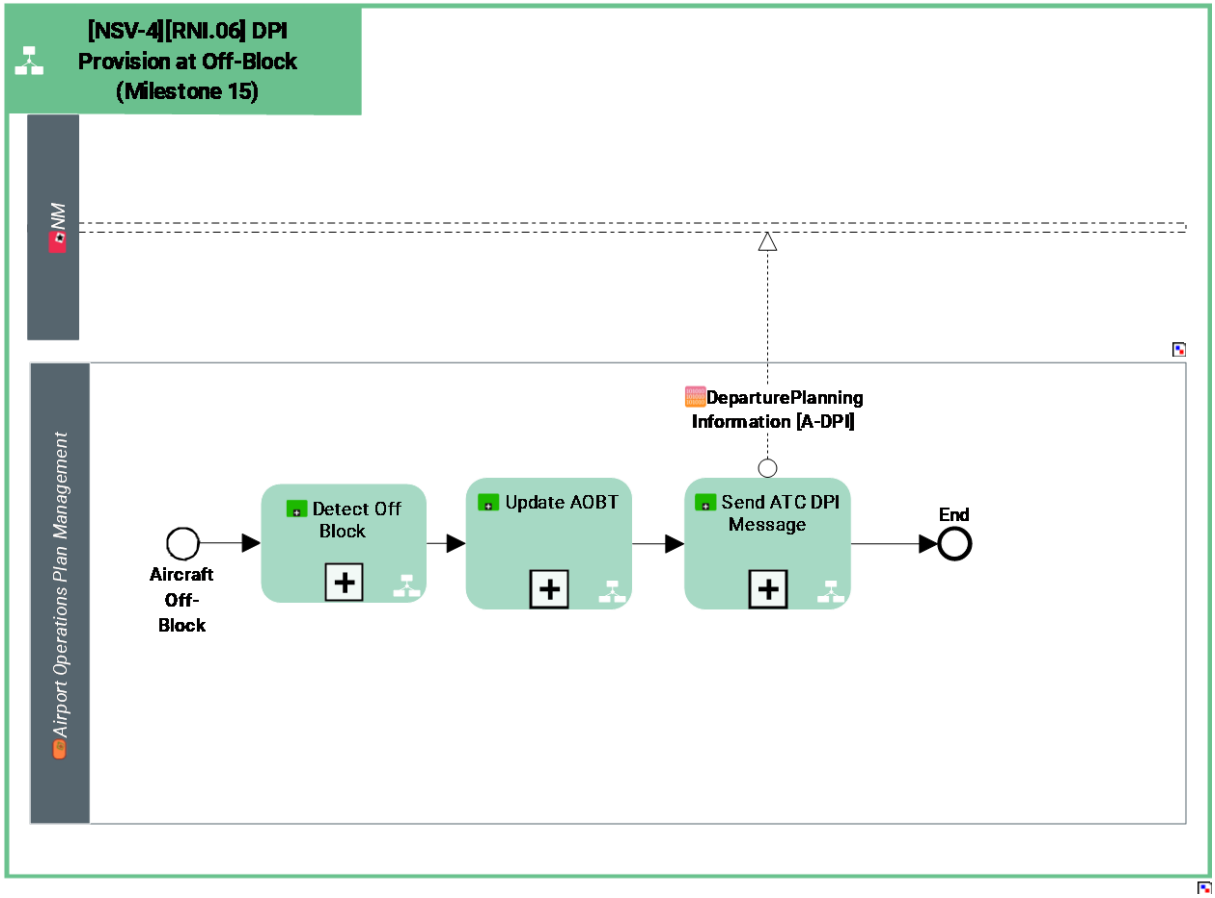


5.2.1.6 [NOV-5][RNI.05] DPI Provision at Off-Block (Milestone 15)

The time (AOBT) the aircraft pushes back/vacates the parking position, an ATC DPI message is sent to NMOC, which is also informed if TTOT changes by more than the agreed tolerance.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

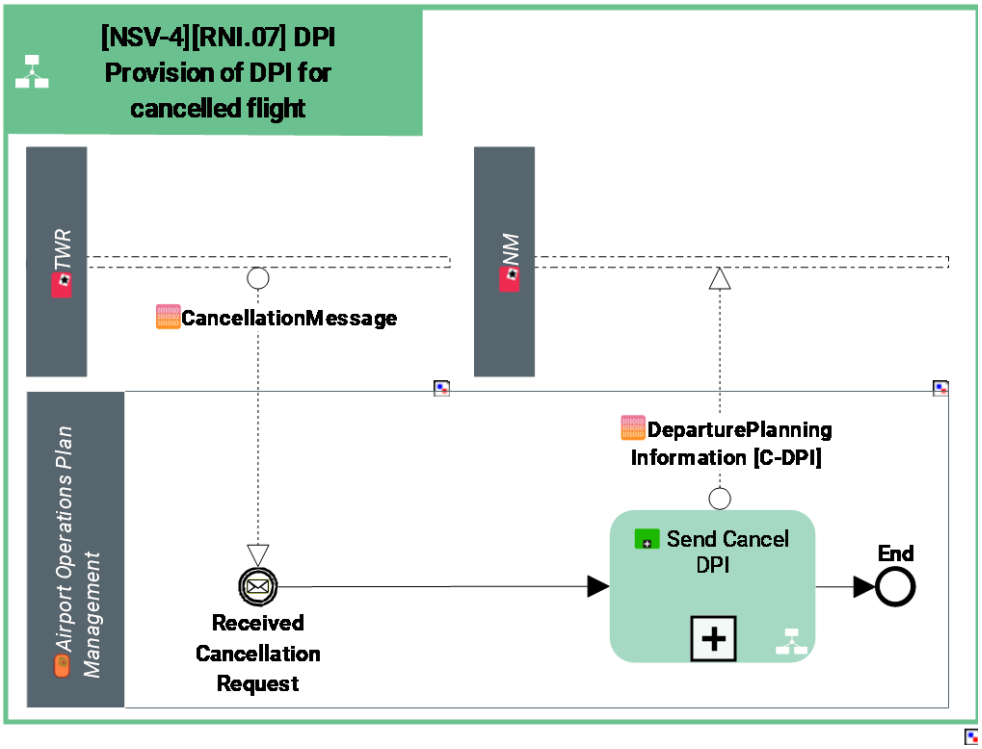


5.2.1.7 [NOV-5][RNI.06] DPI Provision of DPI for cancelled flight

The airport will send a C-DPI (CNL) Message to NMOC at the time when a previously sent TTOT is no longer valid and a new TTOT is not yet known.

EUROPEAN PARTNERSHIP

Co-funded by the European Union



5.2.2 Task Analysis

Non required, the solution seeks an automated model where Human Resources tasks are not required (besides TOBT confirmation by the GH/AUs).

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

The purpose of this section is to present the Safety Requirements at Design level (SRD) derived for Normal and Abnormal conditions of operation following related SAF-GUI in STELLAR.

The derivation of Safety requirements at design level - SRD for Normal and Abnormal conditions of operation is mainly driven by the SRS (functionality and performance) for Normal and Abnormal conditions of operation from sections 4.2 and 4.3.

Meanwhile additional SRD might be identified (and need to be documented here) from the static view and dynamic view analysis of the system behaviour in normal and abnormal operational conditions that needs to be conducted in order to show completeness/correctness of the Safety Requirements (Functionality and Performance) .

5.3.1 Safety Requirements at Design level (SRD) – Normal and Abnormal conditions

In this section it is provided the consolidated list of Safety Requirements at Design level (SRDs) (functionality and performance) for Normal and Abnormal conditions of operations derived by mapping the Safety Requirements at Service level (SRSs) for Normal and Abnormal conditions of operation documented in section 4.2 and 4.3 onto the related elements of the Design Model.

Co-funded by the European Union

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

Safety Requirement ID [Design Model Element]	Safety Requirement (functionality & performance)	Derived from SRS (ID)
SRD 001	RNI platform shall validate the FPL in accordance with the available information and assure the correct information is available	SRS 001
SRD 002	The RNI platform shall assure the correct computation, visualization and distribution to all the involved Stakeholders of the Target and Estimated Times	SRS 002; 003; 004; 005; 006; 007; 008; 009; 010 & 012
SRD 003	The RNI platform shall have the possibility to seamlessly migrate to a server with reduced capabilities until the main servers recovers from the failure.	SRS 011

Table 5. Safety Requirements at design level (functionality and performance) satisfying SRS for Normal and Abnormal conditions

5.3.2 Additional SRD from Static analysis of the functional system behaviour

Non Applicable (Appendix C.2.)

5.3.3 Additional SRD from Dynamic analysis of the functional system behaviour

Non Applicable (Appendix C.3.)

5.3.4 Effects on Safety Nets

Non Applicable (Appendix C.3.)

5.4 Safety Requirements at design level addressing Internal Functional System Failures

The purpose of this section is to present the Safety Requirements at Design level (SRD) addressing internal system failures derived following the SAM-PSSA [2] and related SAF-GUI in STELLAR.

Safety requirements at design level - SRD are derived from the SRS associated to failure conditions which have been identified in section 4.4.

The following Safety Requirements at Design Level (SRD) are to be included (derived from a top-down causal analysis of the Service Hazards identified in section 4.4.1, from a bottom-up failure modes and effects analysis encompassing the analysis of common causes and , if applicable, from the SRS (functionality & Performance) derived during the Service Hazard assessment section 4.4.1):

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

Co-funded by the European Union

- If applicable, SRD (functionality and performance) derived to provide mitigation against service hazard effects (protective mitigation, from the SRS (functionality&performance) derived during the Service Hazard assessment.

5.4.1 Design analysis addressing internal functional system failures

As identified before, the rop dow analysis realised has undergo the following process:

1. Identification of a complete list of Solution functional system failures that could cause each service hazard. The only service identified is the "Provision of departure planning information to the NM", therefore the only functional system failure that could cause a service hazard is the collapse of this service. For more detail please access Section 4.4 and Appendix B.
2. Identification of the required Mitigation means preventing causes to occur or preventing their effect to propagate up to the service hazard. The means identified are returning to old operating method processing the DCB process through the flight plans data rather without the DPI information.
3. Demonstration of the feasibility and effectiveness of the contingency procedures associated to the degraded modes of operation in which the functional system might enter as a result of certain failure modes. This is under demonstration under the OBJ-04-W2-28.1-V3-VALP-2811.0005 validation objective.
4. Determine potential common cause failures and ensure their mitigation through dedicated SRD or design choice as it is included in Appendix D.

5.4.2 Safety Requirements at design level addressing internal system failures

Table 6. Additional SRD (functionality & performance) to mitigate the service hazards Provide in contains consolidated list of Safety Requirements at Design level (functionality and performance) addressing internal system failures with the SRD (functionality and performance) derived from the SRS documented in section 4.4 to provide adequate mitigations to reduce the likelihood that specific failures would propagate up to the service hazard, with due consideration for mitigating the common cause failures.

No SRD (integrity/reliability) were required taking into account the Additional SRD (functionality & performance elaborated to cover the whole SRS documented in section 4.4.

To access more detail go to Appendix D.

Safety Requirement ID	Safety Requirement at Design level (SRD) (functionality & performance)	Derived from SRS (ID) or Common Cause failure
SRD 004	Implementation of a capability that allows to detect when, either the information of the DPIs is not transmitted, or when this information is compromised and does not have the precision and integrity required. At that moment, NM performs the DCB process again with the flight plans data instead of the data contained in the DPIs, reducing the	**SRS 013 :**

	capacity of the sectors due to the lower precision of the information, but increasing security (old operating method)	

Table 6. Additional SRD (functionality & performance) to mitigate the service hazards

5.5 Realism of the safe design

Safety Requirement ID	Safety Requirement at Design level (SRD) (functionality & performance)	Derived from SRS (ID) or Common Cause failure
SRD 001	RNI platform shall validate the FPL in accordance with the available information and assure the correct information is available	SRS 001
SRD 002	The RNI platform shall assure the correct computation, visualization and distribution to all the involved Stakeholders of the Target and Estimated Times	SRS 002; 003; 004; 005; 006; 007; 008; 009; 010 & 012
SRD 003	The RNI platform shall have the possibility to seamlessly migrate to a server with reduced capabilities until the main servers recovers from the failure.	SRS 011
SRD 004	Implementation of a capability that allows to detect when, either the information of the DPIs is not transmitted, or when this information is compromised and does not have the precision and integrity required. At that moment, NM performs the DCB process again with the flight plans data instead of the data contained in the DPIs, reducing the capacity of the sectors due to the lower precision of the information, but increasing security (old operating method)	**SRS 013 :**

The system is nothing new, A-CDM was previously successfully implemented. RNI solutions is an automated and less complex operative model than A-CDM, that will operate the same way it does A-CDM. Therefore, the DPI emission has been largely studied and tested, and all the possible safety measures implemented.

Because of this precedent, it is considered that the SRDs are highly achievable and will not require additional development and will not be expensive.

5.6 Process assurance for a Safe Design

Assurance is achieved as explained in the previous section.

Co-funded by the European Union

6 Demonstration of Service specification achievability

Within the HAZID and Safety & HP Scoping and change assessment session held the 29/11/2021 and further re-visited the 03/12/2021, a preliminary safety impact assessment was conducted, involving operational experts which were relevant for the use of service(s) provided by the solution. That allowed to understand the potential safety implication of the solution as per the paragraphs below.

The Safety driver will be the conformance to the NM data quality requirements for DPIs. The safety demonstration strategy will be:

1. Prove conformance to the NM data quality requirements for DPIs → to include a safety validation objective in VALP Part I in view of demonstrating the conformance to these data quality requirements within the VAL EXE.

Identifier	OBJ-04-W2-28.1-V3-VALP-2811.0005
Objective	To validate that the platform provides sufficient quality in the DPI messages being sent to the Network Manager.
Title	A-CDM in a regional airport DPI message quality
Category	<Safety>
Key environment conditions	Traffic as per the airport traffic at the moment of the exercise (shadow mode), Regional Airport
V Phase	V3

2. Argue that in case of degraded DPI information received, a mitigation will be implemented (safety requirement) in terms of a DPI real-time monitoring tool as part of the validation platform. When DPI are lost or not adequate, the system will detect a potential anomaly and NM would revert to using FPL data for trajectory prediction (similarly to the case of A-CDM airports) – performance degraded, but safety ensured.

3. Perform a Safety assessment workshop with operational experts when OSED starts to mature but not too late for allowing potential safety requirements to be checked in the VAL EXE (if feasible) and included in the final OSED. Given the synergy with 28.3, either experts from that solution might be invited or a joint safety workshop might be organized.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

7 Acronyms and Terminology

Acronym	Definition
ACGT	Actual Commence of Ground Handling
RNI platform	A-CDM Information Sharing Platform
ADP	Aeroports de PAris
AIBT	Actual In Block Time
ANS	Air Navigation Service
AO	Aircraft Operator
AOBT	Actual Off Block Time
AODB	Airport Operational Database
AOP	Airport Operations Plan
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATM	Air Traffic Management
ATOT	Actual Take Off Time
ATS	Air Traffic Serviced
AU	Airspace User
CDM	Collaborative Decision Making
CNL	Cancel
CTOT	Calculated Take Off Time
DCB	Demand Capacity Balancing
DMAN	Departure Manager
DPI	Departure Planning Information
EATMA	European ATM Architecture
EC	European Comission
ED	Edition

Co-funded by the European Union

EEA	European Economic Area
ELDT	Estimated Landing Time
EN	Enabler
EOBT	Estimated Off Block Time
ER	En Route
ETSI	European Telecommunications Standards Institute
EU	European Union
EUROCAE	European Organisation for Civil Aviation Equipment
EXE	Exercise
EXIT	Estimated Taxi In Time
EXOT	Estimated Taxi Out Time
FMEA	Failure Modes and Effects Analysis
FPL	Flight Plan
FUM	Flight Update Message
GH	Ground Handler
GUI	Guidance
HAZID	Hazard Identification
HP	Human Performance
ID	Identification
IFPS	Integrated initial flight plan processing system
IFR	Instrumental Flight Rules
MAC	MAC
NM	Network Manager
NMOC	Network Manager Operations Centre
NOP	Network Operation Plan
OBJ	Object
OI	Operational Improvement

Co-funded by the European Union

OSED	Operational Service and Environment Definition
PAR	Performance Assessment Report
PDM	Pre-Departure Management
PDS	Pre-Departure Sequence
PJ	Project
PSSA	Preliminary System Safety Assessment
RNI	Regional Network Integrated
SAF	Safety
SAM	Safety Assessment Methodology
SAR	Safety Assessment Report
SEAC	SESAR European Airports Consortium
SESAR	Single European Sky ATM Research
SH	Service Hazard
SID	Standard Instrumental Departure
SOBT	Schedule Off Block Time
SRD	Safety Requirements at Design level
SRM	Safety Reference Material
SRS	Safety Requirements at Service Level
TMA	Terminal Manoeuvring Area
TOBT	Target Off Block Times
TS	Technical Specifications
TSAT	Target Start Up Approval Time
TTOT	Target Take Off Time
UC	Use Case
VAL	Validation
VALP	Validation Plan
VLD	Validation

Co-funded by the European Union

XTTA	Expected Turnaround Time

Table 7: Acronyms

Term	Definition	Source of the definition
Solution Functional System	Designates the Solution Functional ATM/ANS System as defined in Regulation EU 2017/373 [1] (i.e. encompassing procedures, human resources and equipment).	SPR-INTEROP/OSED for V3 - Part II - Safety Assessment Report
Advanced ATC Tower Airport (AAT)	Airports that have no plans to implement the A-CDM process but still wish to integrate into the ATM network may do so as an Advanced ATC TWR Airport. Such an Airport may provide a reduced set of DPI messages with a reduced set of advantages (compared to CDM Airports). An Advanced ATC TWR Airport provides Target Take-Off-Time (TTOT) estimations as well as Variable Taxi-Times (VTTs) and SIDs to the NMOC. These are provided from the moment that the aircraft leaves the blocks.	Advanced ATC TWR Implementation Guide Edition Nº 1.6
Airport Operations Plan (AOP)	The AOP (Airport Operations Plan) is the single, common and collaboratively agreed rolling plan used by all involved stakeholders whose purpose is to provide common situational awareness. It requires individual stakeholders to make changes within their own sphere of operations. The AOP interacts with a number of services, systems and external stakeholders (e.g. Network).	ATM Lexicon
ATFCM	A service complementary to Air Traffic Control (ATC), the objective of which is to ensure an optimum flow of air traffic to or through areas within which traffic demand at times exceeds the available capacity of the ATC system.	EUROCONTROL, CFMU (2002), Air Traffic Flow Management Operations: ATFM Users Manual, Edition 8.0, 18.3.2002
Demand Capacity	Integrated Local DCB (Demand and Capacity Balancing) Processes see the seamless integration of local network management with extended ATC	SOL PJ09.02

Co-funded by the European Union

Balancing (DCB)	planning and arrival management activities in short-term and execution phases. It represents the core functionality for the Integrated Network ATM Planning (INAP) process through an enhanced Local DCB tool set. The solution will improve the efficiency of ATM resource management, as well as the effectiveness of complexity resolutions by closing the gap between local network management and extended ATC planning.	
DPI	The purpose of the Departure Planning Information (DPI) message is to supply the NMOC with flight data related updates that are made available by DCB tools, sequencing tools (e.g. DMAN), ANI-, CDM-, RNI- or ADV ATC TWR Airport systems. The main data elements to be received via the DPI message are: - An accurate estimation of the take-off time - The taxi-time (EXOT) - The SID - TOBT & TSAT At CDM airports where the Aircraft Type and Registration are verified, the DPI message can also contain updates of: - The aircraft type - The aircraft registration These DPI messages are described in more detail in Reference [9]	DPI Implementation Guide Edition Nº 2.3
Information Service	An information service is a service delivering information or data to actors and/or systems without transformation of the underlying data. Information services can include filtering and/or combining of information. They are the only responsible for system data	OFA 5.1.1, Section 1.6

Co-funded by the European Union

	exchange, they can be considered as interfaces among systems.	
Network Operations Plan (NOP)	A set of information and actions derived and reached collaboratively both relevant to, and serving as a reference for, the management of the Pan-European network in different timeframes for all ATM stakeholders, which includes, but is not limited to, targets, objectives, how to achieve them, anticipated impact.	ATM Lexicon
Operational Service	An operational service is a product of a sequence of operational processes on request of an actor to another actor who will execute the service with clear identification of an output. A service is offered by an operational entity, (i.e. an organizational actor (e.g. ANSP (Air navigation Services Provider)) or a human actor (e.g. ATCO (Air Traffic Controller)). There are several levels of operational service, depending on the level of granularity required. At lower level an operational service can be supported by: Information service(s) to carry out information needed by the operational service without transforming the information, and/or Application service(s) to use this information in order to provide an output via automation / computation, i.e. with transformation of the information	OFA 5.1.1, Section 1.6
Regional Network Integrated Airport	Currently the integration of airports into the ATM Network is achieved through either the A-CDM concept or the Advanced Tower concept. A third category of airport (regional airports) is proposed where a reduced set of CDM milestones is implemented and calculated in a quasi-automatic fashion -	Operational Improvement AO-0824

	reducing the need for Airline / Ground Handler inputs. Such an approach relies on the stability and predictability of taxi-times which is considered as feasible in such airports. This will be a way to simplify the work needed to manually update CDM milestones, and also to enable the connection of regional airport to NMOC.	

Table 8: Glossary of terms

EUROPEAN PARTNERSHIP

Co-funded by the European Union

8 References

Safety

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

[2] SAM EUROCONTROL Safety Assessment Methodology V2.1 (https://www.eurocontrol.int/tool/safety-assessment-methodology)

[3] Guidance to Apply SESAR Safety Reference Material (E.d 00.03.01)

[4] D2.1.010 - PJ.04-W2-28.1 VALP - Part II – SAP (ED. 00.00.02)

Operational and Technical

[5] SESAR Solution PJ04-W2-28.1 SPR-INTEROP/OSED for V3 - Part I (Ed. 00.00.05)

[6] SESAR 2020 Solution PJ04-W2-28.1 TS/IRS for V3 - Part I (MEGA/HOPEX 08/08/2022)

[7] SESAR Solution PJ.04-01 SPR-INTEROP/OSED for Part I (Ed. 01.02.00)

[8] SESAR Solution 04.01 SPR-INTEROP/OSED - Part V - Performance Assessment Report (Ed. 01.00.01)

[9] DPI Implementation Guide; Edition 1.800; 19 Mar 2015

Standards

[10]ETSI EN 303 212 V1.1.1 Airport Collaborative Decision Making (A-CDM); Community Specification for application under the Single European Sky Interoperability Regulation EC 552/2004

[11] ED-141 System Requirements Document

[12] ED-145 Interface Definition Document

[13] ED-146 Test and Validation Document

[14]Regulation (EU) No 598/2014 of the European Parliament and of the Council of 16 April 2014 on the establishment of rules and procedures with regard to the introduction of noise-related operating restrictions at Union airports within a Balanced Approach and repealing Directive 2002/30/EC

[15]Regulation (EC) No 1070/2009 of the European Parliament

[16]Commission Implementing Regulation (EU) No 390/2013

[17]Directive 2002/49/EC of the European Parliament and of the Council of 25 June 2002 relating to the assessment and management of environmental noise

[18]Directive 2008/50/EC of the European Parliament and of the Council of 21 May 2008 on ambient air quality and cleaner air for Europe

[19]Directive No 2016/2284 of 14 December 2016 on the reduction of national emissions of certain atmospheric pollutants, amending Directive 2003/35/EC and repealing Directive 2001/81/EC, the National Emission Ceilings Directive (NEC Directive)

[20]Law no. 2015-992 on Energy Transition for Green Growth (Energy Transition Law)

Appendix A Defining the Service Safety Specification for Normal and Abnormal conditions of operation

This appendix presents the definition of the SRS (functionality and performance) in order to set the Service Safety Specification under normal (i.e. those conditions that are expected to occur on a day-to-day basis) and abnormal conditions of operation.

The set of SRS has to be complete for the scope of the change brought in by the Solution. The consolidated list is provided in Sections 4.2 (normal conditions of operation) and 4.3 (abnormal conditions of operation).

A.1 SRS obtained from other operational solutions or standards

The solutions developed within the SESAR environment in Wave 1 that could contribute SRS did not develop this content, so there are no Docs. precedents to iterate over.

Additionally, the existing regulations do not cover the Service Safety Specification for Normal and Abnormal conditions of operation, but the Safe Design of the Solution functional system, contained within Section number 5 “Safe Design of the Solution functional system”.

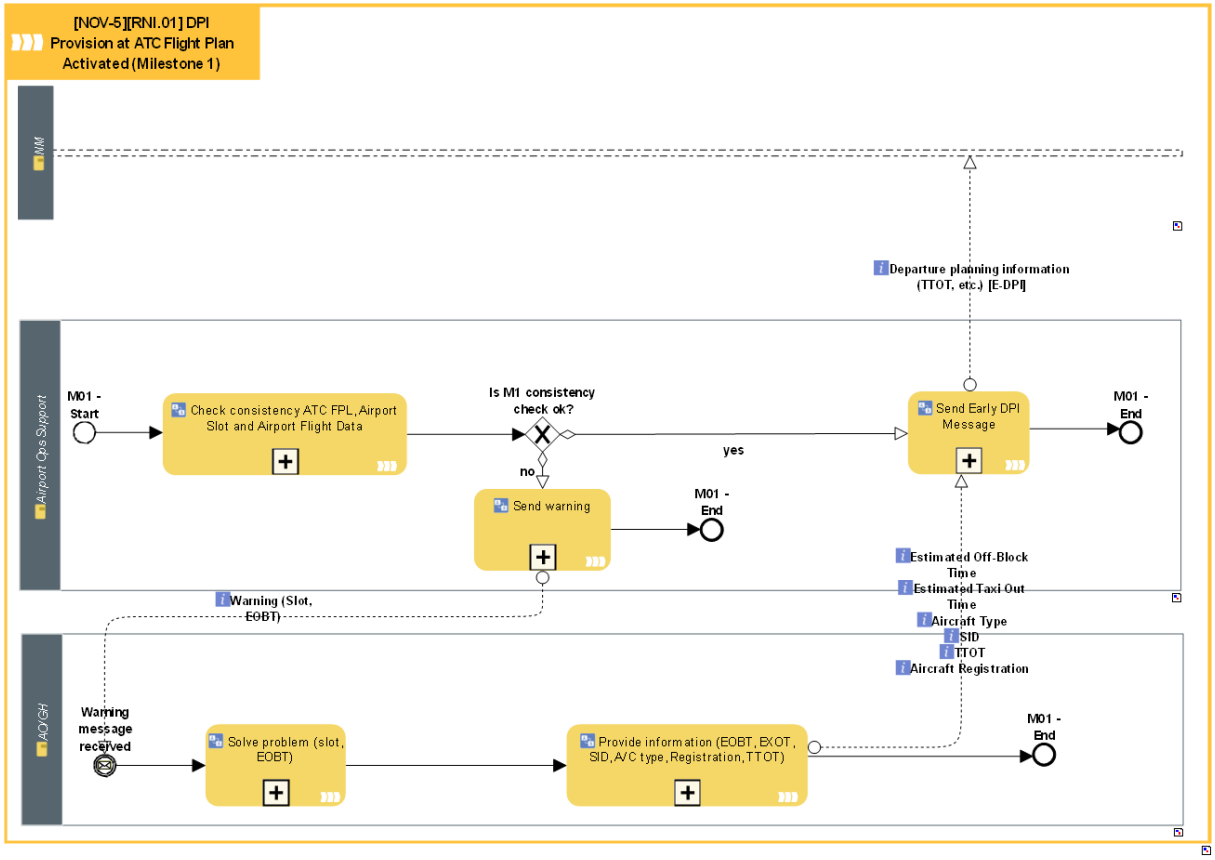
A.2 EATMA Process models or alternative description

A.2.1 [NOV-5][RNI.01] DPI Provision at ATC Flight Plan Activated (Milestone 1)

The RNI airport shall send automatically an E-DPI (Early) Message to NMOC at EOBT-3h with EOBT, EXOT, SID, Aircraft Type, Registration, TTOT (=EOBT+EXOT).

The transmission of an E-DPI Message confirms to NMOC that an airport slot and flight plan for a particular flight has been correlated in accordance with local rules at the airport.

Co-funded by the European Union



A.2.2 [NOV-5][RNI.02] DPI Provision at Take Off from Outstation (Milestone 3)

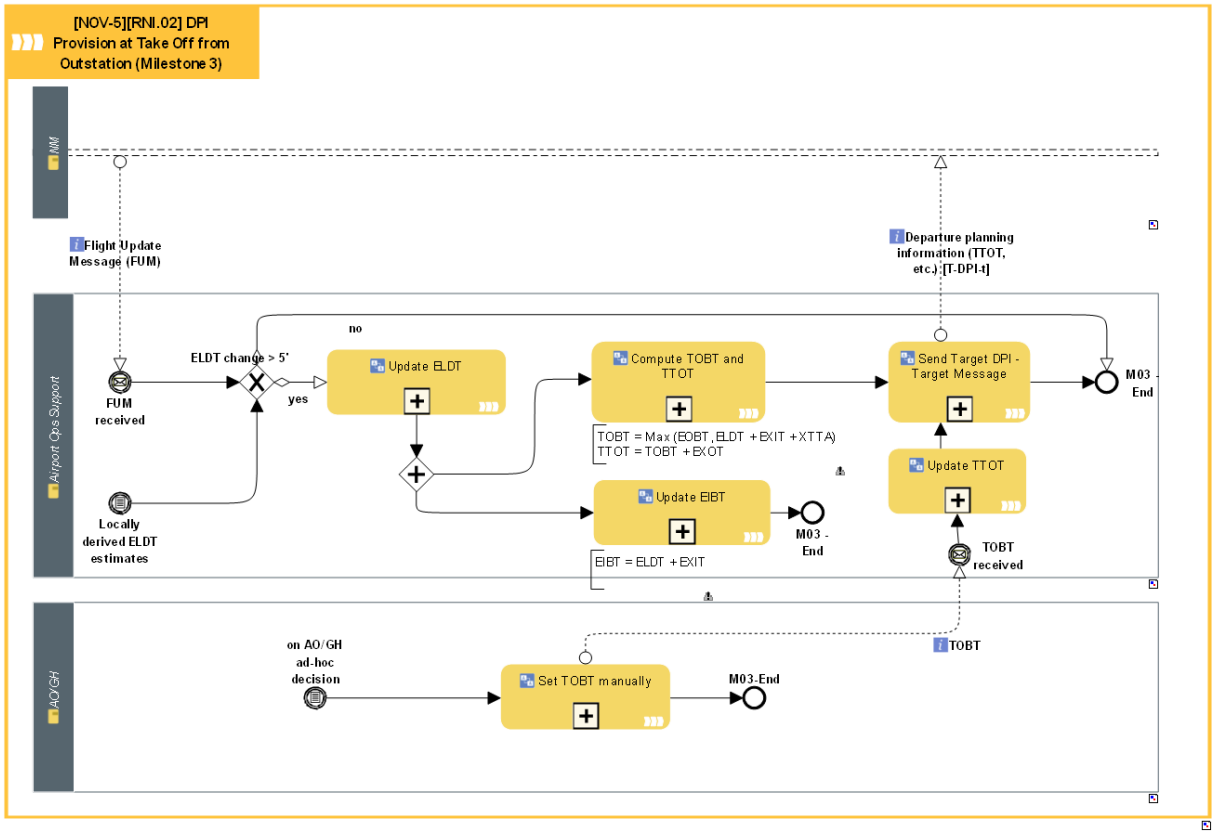
When a flight inbound to the RNI airport takes off from the outstation (status = 'airborne'), an initial TOBT and TTOT shall be calculated based on the latest time between EOBT and ELDT+EXIT+XTTA. And TTOT = TOBT+EXOT.

If the departure airport is more than 3hrs flying time from the destination airport the ATOT is received from either the Network Operations FUM or via the Aircraft Operator or Ground Handling Agent. Using the ATOT an ELDT can be calculated by using the Estimated Elapsed Time on the FPL.

If the flight is within 3hrs flying time of the destination airport, NMOC monitors progress of the flight and send FUM Messages to provide updated ELDT.

EUROPEAN PARTNERSHIP

Co-funded by the European Union



A.2.3 [NOV-5][RNI.03a] DPI Provision at Ground Handling Started without PDM (Milestone 6 to 9)

This UC covers the case where no DMAN exists at the airport, but it may exist or not a PDS.

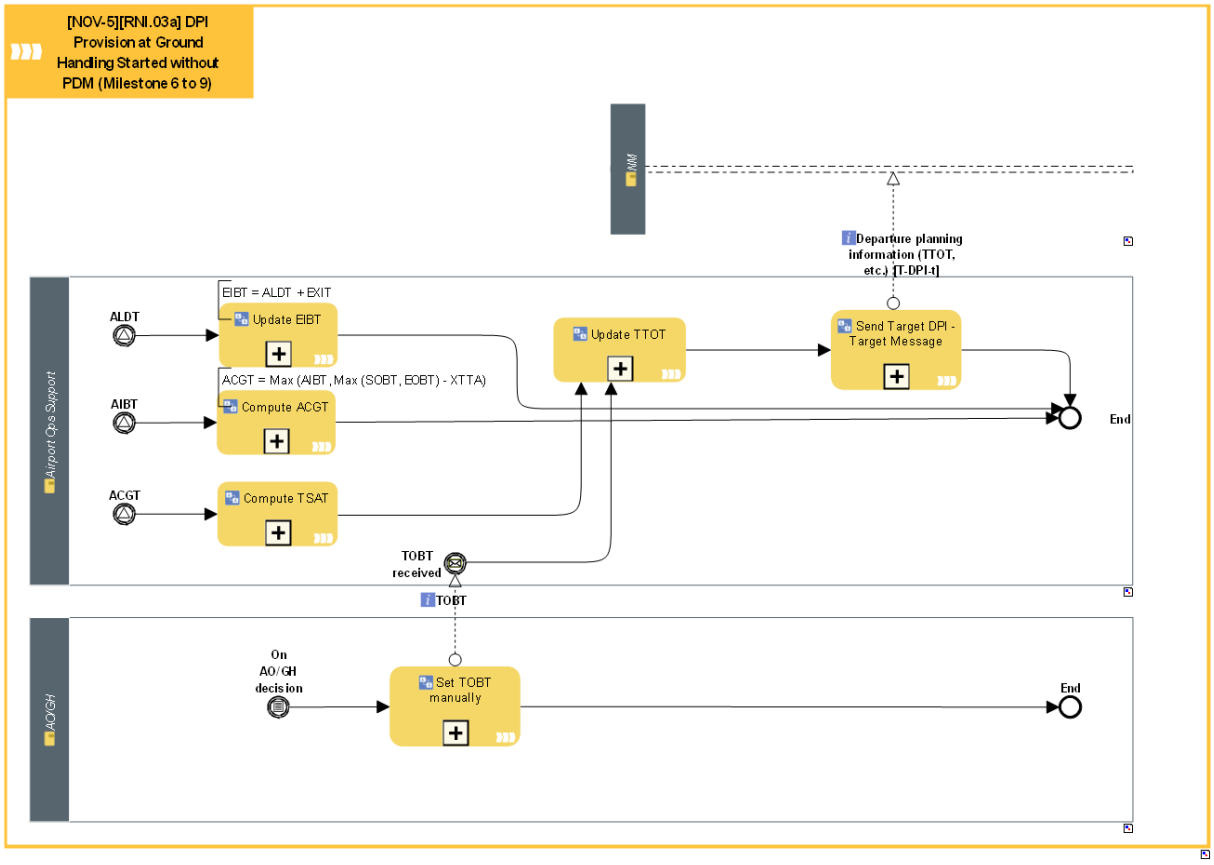
For flights that are on a normal turn-round (SOBT-AIBT) < 2h, Actual Commencement of Ground Handling Time (ACGT) = AIBT.

Use of SOBT and EOBT caters for the case of aircraft on a 'long' turnaround such as a night stop. ACGT = MAX(SOBT,EOBT) - XTTA.

SOBT is the scheduled off-block time, EOBT the latest estimated off-block time and XTTA is derived from the RNI database for the flight in question.

EUROPEAN PARTNERSHIP

Co-funded by the European Union



A.2.4 [NOV-5][RNI.03b] DPI Provision at Ground Handling Started with PDM (Milestone 6 to 9)

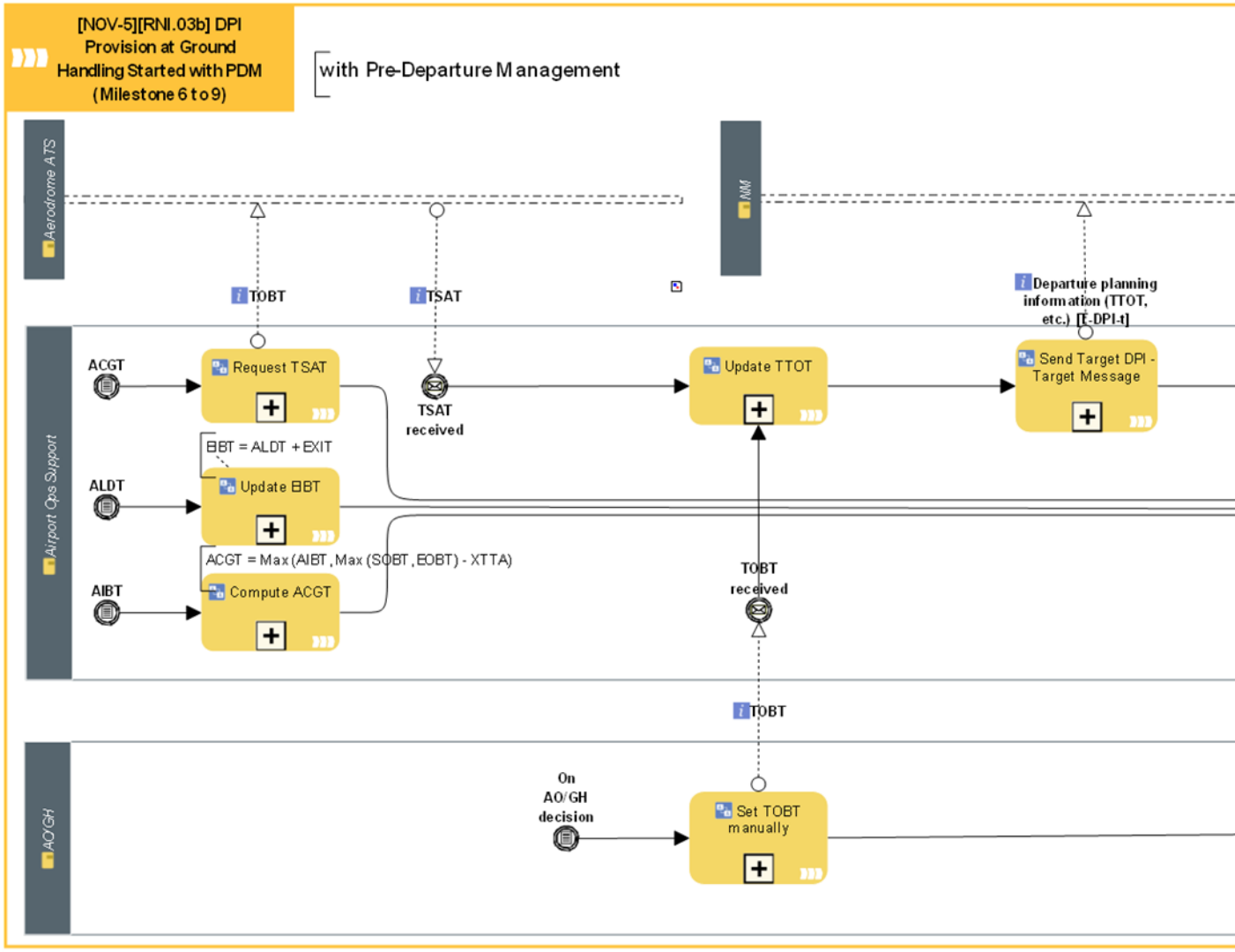
This UC covers the case where a DMAN is in operations at the airport.

For flights that are on a normal turn-round (SOBT-AIBT) < 2h, Actual Commencement of Ground Handling Time (ACGT) = AIBT.

Use of SOBT and EOBT caters for the case of aircraft on a 'long' turnaround such as a night stop. ACGT = MAX(SOBT,EOBT) - XTTA.

SOBT is the scheduled off-block time, EOBT the latest estimated off-block time and XTTA is derived from the RNI database for the flight in question.

Co-funded by the European Union



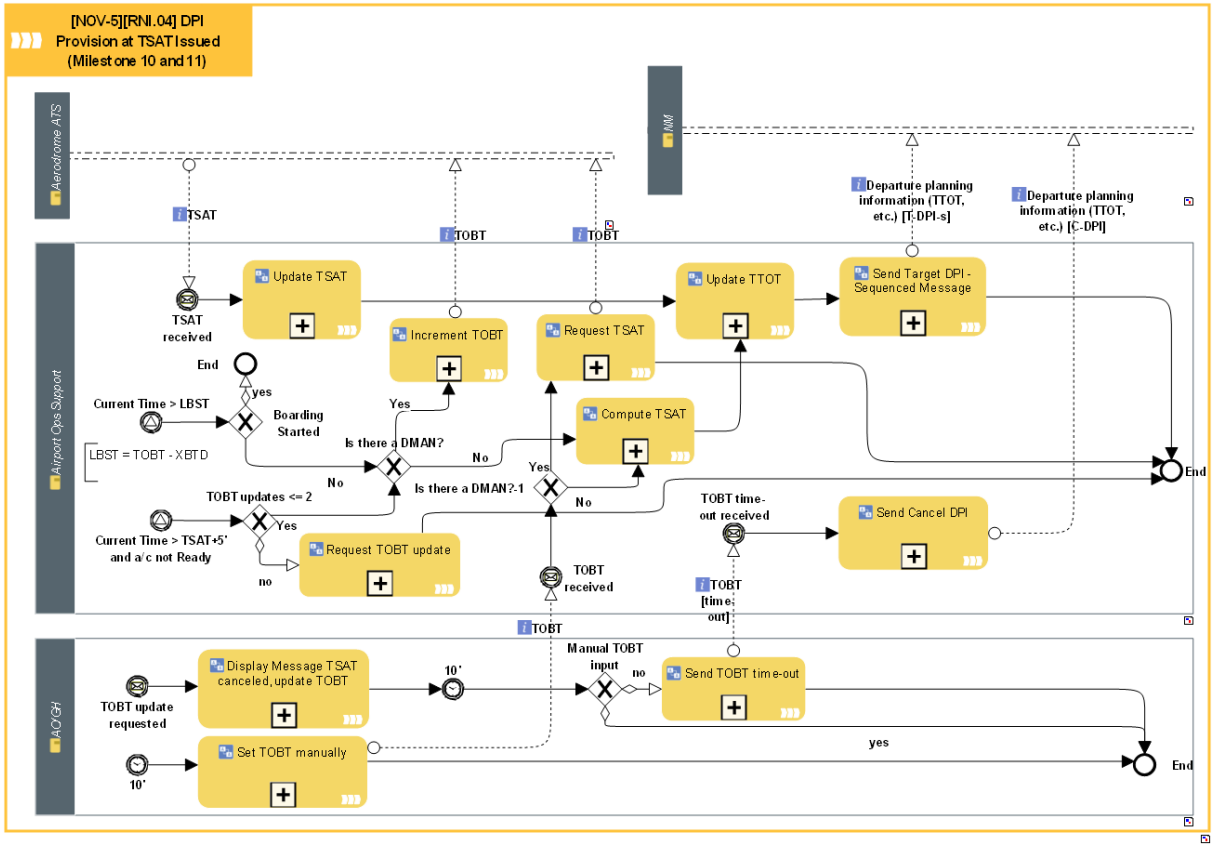
A.2.5 [NOV-5][RNI.04] DPI Provision at TSAT Issued (Milestone 10 and 11)

The RNI airport sends automatically a T-DPI-s (Sequenced) Message to NMOC at local implementation definition (A-CDM manual recommends between TOBT-40' and TOBT-30') with TTOT calculated with TSAT (output from the pre-departure sequence) and EXOT.

The inputs for the Pre-departure Sequence are the TOBT+Taxi-Time (EXOT) (for non-regulated flights), the CTOT (for regulated flights) and any Airport constraints. The output of the Pre-Departure Sequence is the TSAT.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

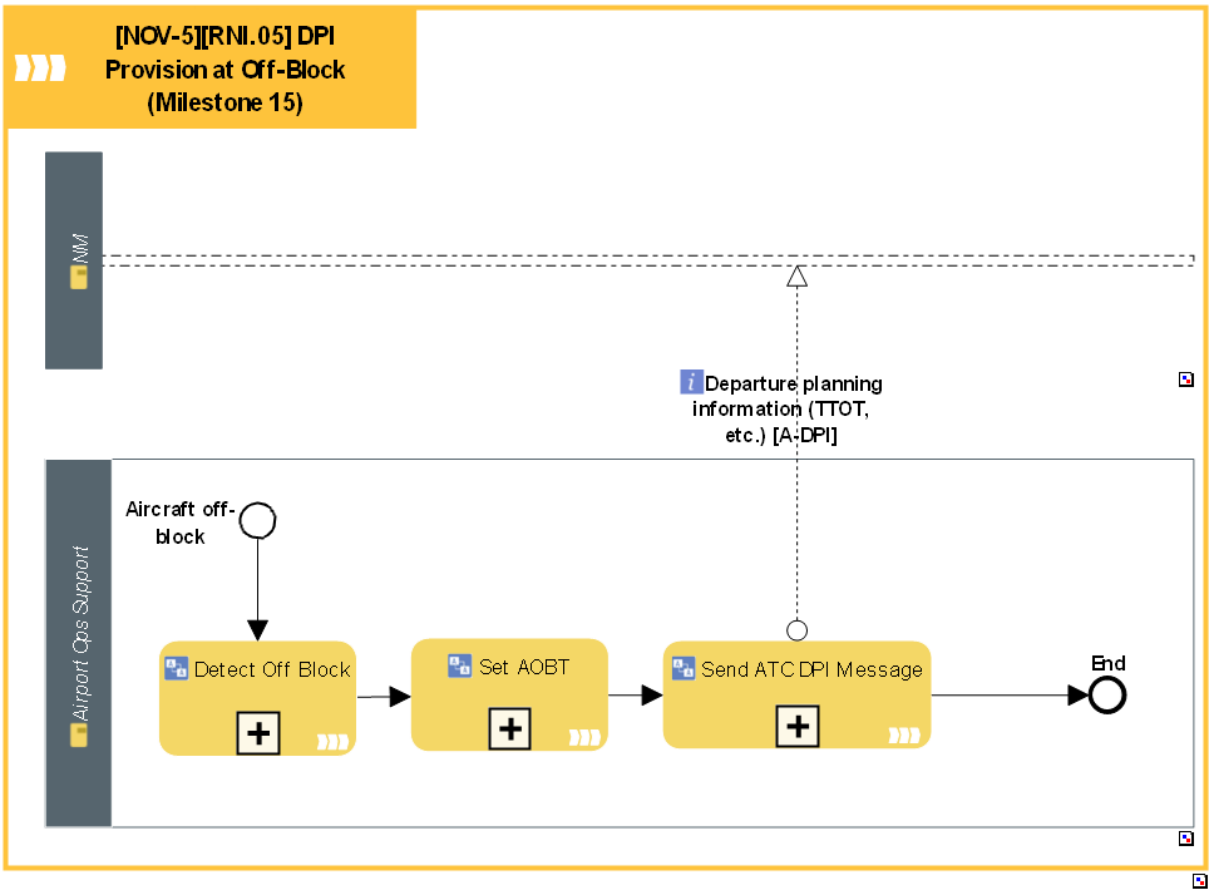


A.2.6 [NOV-5][RNI.05] DPI Provision at Off-Block (Milestone 15)

The time (AOBT) the aircraft pushes back/vacates the parking position, an ATC DPI message is sent to NMOC, which is also informed if TTOT changes by more than the agreed tolerance.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

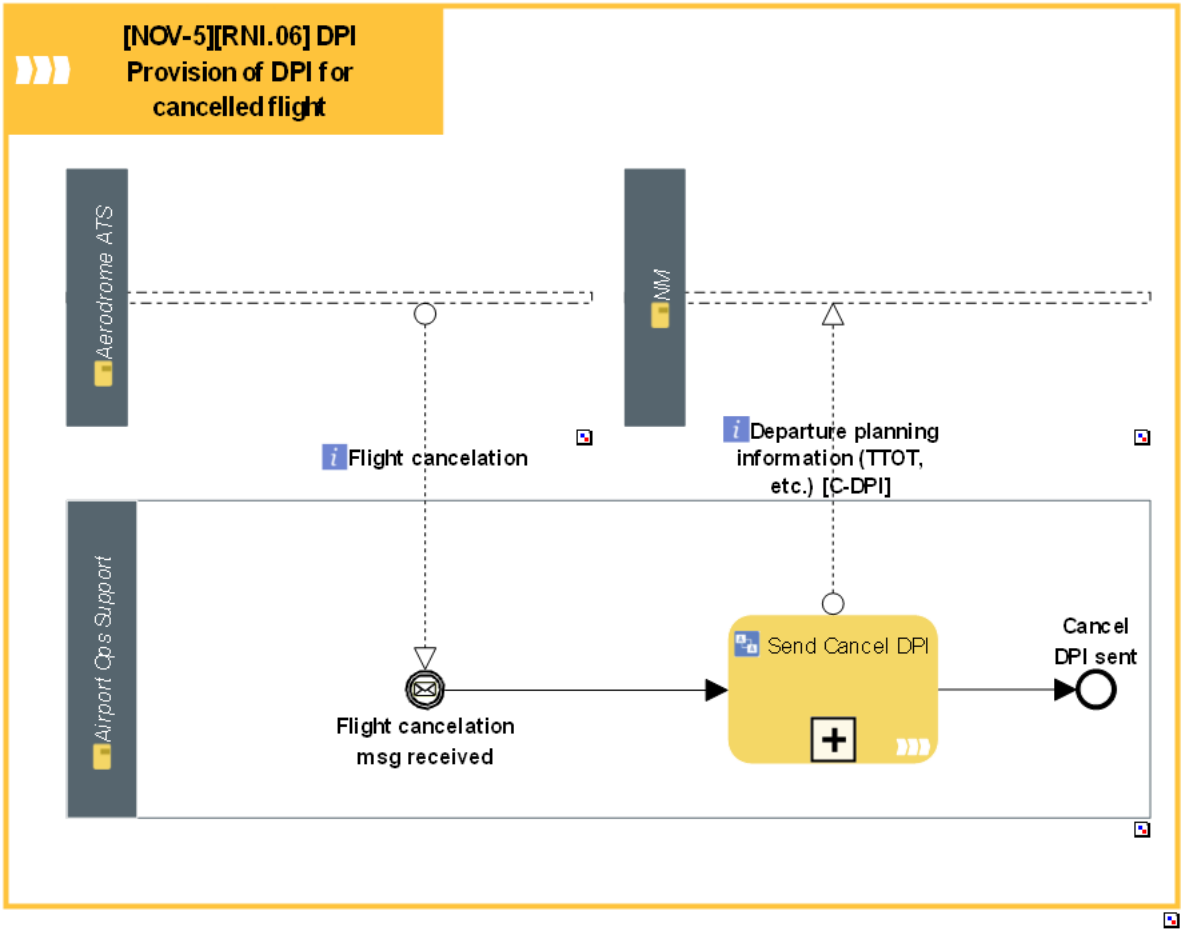


A.2.7 [NOV-5][RNI.06] DPI Provision of DPI for cancelled flight

The airport will send a C-DPI (CNL) Message to NMOC at the time when a previously sent TTOT is no longer valid and a new TTOT is not yet known.

EUROPEAN PARTNERSHIP

Co-funded by the European Union



A.3 Derivation of SRS for Normal conditions of operation

SRS for Normal Operations were obtained as a derivation driven by EATMA Process Models presented previously.

Service	EATMA Use Case- Activity or Flow	Derived SRS
[NOV-5][RNI.01] DPI Provision at ATC Flight Plan Activated (Milestone 1)		
Early data management	Create/update FPL	**SRS 001**: AUs/GHs shall submit (and resubmit if any update is needed) the FPL in time for enabling reliable traffic prediction
	Data integrity	**SRS 002:** AUs/GHs shall assure the integrity of the data that will undergo through a system check to assure it
	E-DPI integrity	**SRS 003:** Airport Operator shall assure the integrity of the data contained in an E-DPI that will be used by the NM
[NOV-5][RNI.02] DPI Provision at Take Off from Outstation (Milestone 3)		
Actual, Target and Estimate Times integrity	T-DPI-t integrity	**SRS 004:** Airport Operator shall assure the integrity of the data contained in a T-DPI-t that will be used by the NM

Co-funded by the European Union

Service	EATMA Use Case- Activity or Flow	Derived SRS
	FUM integrity	**SRS 005:** NM shall assure the integrity of the data contained in a FUM that will be used by the Airport Operator for the whole A-CDM process computation
	TOBT integrity	**SRS 006:** AUs/GHs shall assure the integrity of the TOBT declared, which will feed the PDS and will be used for Resource allocation
[NOV-5][RNI.03a] DPI Provision at Ground Handling Started without PDM (Milestone 6 to 9)		
Actual, Target and Estimate Times integrity	T-DPI-t integrity	**SRS 004:** Airport Operator shall assure the integrity of the data contained in a T-DPI-t that will be used by the NM
	TOBT integrity	**SRS 006:** AUs/GHs shall assure the integrity of the TOBT declared, which will feed the PDS and will be used for Resource allocation
	Milestones integrity	**SRS 007:** Stakeholders shall assure the integrity of any milestone an aircraft goes through (e.g. ACGT) provided to the RNI platform with the correct procedures
[NOV-5][RNI.03b] DPI Provision at Ground Handling Started with PDM (Milestone 6 to 9)		
Actual, Target and Estimate Times integrity	T-DPI-t integrity	**SRS 004:** Airport Operator shall assure the integrity of the data contained in a T-DPI-t that will be used by the NM
	TOBT integrity	**SRS 006:** AUs/GHs shall assure the integrity of the TOBT declared, which will feed the PDS and will be used for Resource allocation
	Milestones integrity	**SRS 007:** Stakeholders shall assure the integrity of any milestone an aircraft goes through (e.g. ACGT) provided to the RNI platform with the correct procedures
	TSAT integrity	**SRS 008:** ATC shall assure the integrity of the TSAT declared in case a Departure Manager is available
[NOV-5][RNI.04] DPI Provision at TSAT Issued (Milestone 10 and 11)		
Actual, Target and Estimate Times integrity	T-DPI-s integrity	**SRS 009:** Airport Operator shall assure the integrity of the data contained in a T-DPI-s that will be used by the NM
	TOBT integrity	**SRS 006:** AUs/GHs shall assure the integrity of the TOBT declared, which will feed the PDS and will be used for Resource allocation
	Milestones integrity	**SRS 007:** Stakeholders shall assure the integrity of any milestone an aircraft goes through (e.g. ACGT) provided to the RNI platform with the correct procedures
	TSAT integrity	**SRS 008:** ATC shall assure the integrity of the TSAT declared in case a Departure Manager is available

Co-funded by the European Union

Service	EATMA Use Case- Activity or Flow	Derived SRS
Cancelation data	Cancel DPI integrity	**SRS 010:** Airport Operator shall assure the integrity of the data contained in a C-DPI that will be used by the NM
[NOV-5][RNI.05] DPI Provision at Off-Block (Milestone 15)		
Actual, Target and Estimate Times integrity	T-DPI-s integrity	**SRS 009:** Airport Operator shall assure the integrity of the data contained in a A-DPI that will be used by the NM
	Milestones integrity	**SRS 007:** Stakeholders shall assure the integrity of any milestone an aircraft goes through (e.g. ACGT) provided to the RNI platform with the correct procedures
[NOV-5][RNI.06] DPI Provision of DPI for cancelled flight		
Cancelation data	Cancel DPI integrity	**SRS 010:** Airport Operator shall assure the integrity of the data contained in a C-DPI that will be used by the NM

Table 9: Derivation of SRS for Normal Operations driven by EATMA Process models

A.4 Derivation of SRS for Abnormal conditions of operation

A.4.1 Identification of Abnormal Conditions

Abnormal conditions in this solution will include a system crash or the impossibility of carrying out the procedures according to the OSED for various reasons.

Under an abnormal condition of the RNI platform, the RNI platform shall be allowed to enter a degraded state provided that it can easily be recovered when the abnormal condition passes.

Today's operations do not have the tools provided by this solution, and therefore, in the event of abnormal conditions that not allows the RNI platform to operate in degraded mode, operations will be resumed as was done prior to the implementation of this solution, reducing capacity or applying measures to be defined locally if required.

A.4.2 Risk analysis of Abnormal Conditions and derivation of SRS (Functionality&Performance)

Present in Table 10 for each abnormal condition of operation identified and listed in the previous section, the results of the risk analysis assessing the immediate operational effect and the possible mitigations of the safety consequences of the abnormal condition with a reference to new derived SRS consolidated in section 4.3 “Service Safety specification - Abnormal conditions of operation”.

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SRS XXX]
ABN1	RNI platform servers are down	RNI platform flight information will not be updated	**SRS 011** (More detail in Section 4.3)

Co-funded by the European Union

ABN4	Data partially not received	Integrations are fallen and data from Stakeholders could not be introduced (e.g. ACGT)	**SRS 012** (More detail in Section 4.3)

Table 10: Risk analysis for Abnormal conditions of operation

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix B Risk assessment of the change at service level

B.1 HAZID workshop

The HAZID workshop was held together with the Safety & HP Scoping and change assessment session the 29/11/2021 and further re-visited the 03/12/2021, where a hazard identification has been conducted, involving operational experts which were relevant for the use of service(s) provided by the solution. That allowed to understand the potential safety implication of the solution as per the paragraphs below.

The Other than ATS Service is: Provision of departure planning information to the NM. But nevertheless, local RNI platform malfunctioning has to be taken into account, not as a service, but a precursor to the malfunction of the service through a lack of accuracy in the "Provision of departure planning information to the NM".

The Solution provides data to NM (predicted take-off times via DPI messages) which contributes to enhancing the traffic prediction in support of DCB. As part of the standard A-CDM deployment process there is a need for the airport to meet certain data quality requirements laid down by NM (e.g. average difference between ATOT and TTOT at different time horizons).

- The introduction of an inefficient and unnecessary regulation (with no safety impact)
- The failure to introduce a necessary regulation resulting in possible sector overloads through negatively impacting the DCB process, including the efficiency of the last barrier within DCB which is the Hotspot monitoring in view of late detection and resolution. That involves a potential safety impact.

It is however worth noting that this situation already exists today, but that situation might be exacerbated in an environment where Regional airports would implement the solution and based on the increasing confidence in the accuracy of the traffic prediction (enabled also by other solutions to be implemented in that time horizon) might reduce the safety margins with regards to the hotspot management. As a conclusion there is a need for safety assessment, where the Safety driver will be the conformance to the NM data quality requirements for DPIs.

The safety demonstration strategy will be:

1. Prove conformance to the NM data quality requirements for DPIs including a safety validation objective in VALP Part I in view of demonstrating the conformance to these data quality requirements within the VAL EXE.
2. Argue that in case of degraded DPI information received, a mitigation will be implemented (safety requirement) in terms of a DPI real-time monitoring tool as part of the validation platform. When DPI are lost or not adequate, the system will detect a potential anomaly and NM would revert to using FPL data for trajectory prediction (similarly to the case of A-CDM airports) – performance degraded, but safety ensured.
3. Perform a Safety assessment workshop with operational experts when OSED starts to mature but not too late for allowing potential safety requirements to be checked in the VAL EXE (if feasible) and included in the final OSED. Given the synergy with 28.3, either experts from that solution might be invited or a joint safety workshop might be organized.
4. Provide the Safety Assessment Report (Part II of OSED) in line with the final validation report.

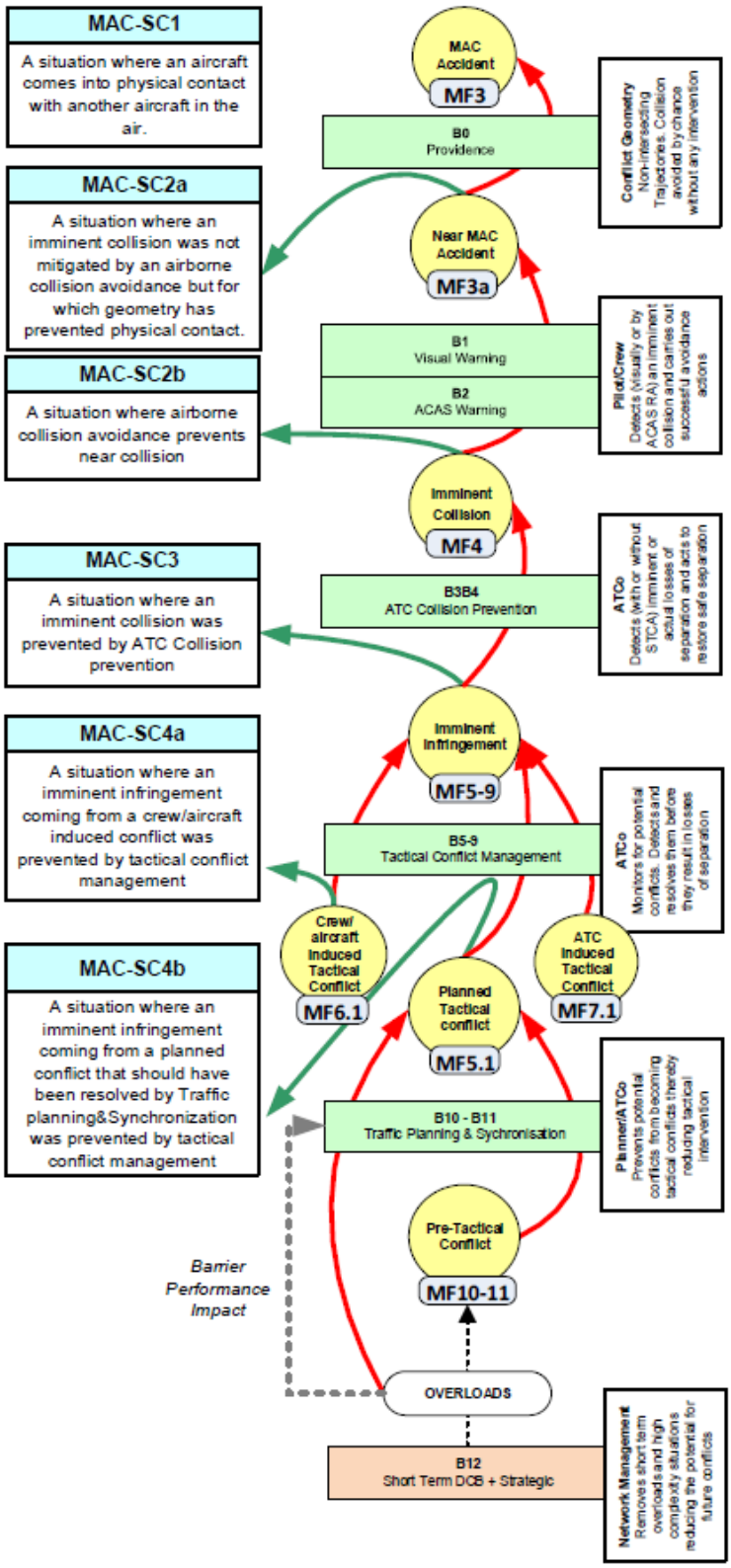
EUROPEAN PARTNERSHIP

Co-funded by the European Union

For the Service Hazard severity, the Severity Classifications for the MAC model (ER and TMA) has been used, taking into account the service affected is the airspace DCB process. To do this, the model presented in Guidance to Apply SESAR Safety Reference Material has been used, section G.3.

A DPI real-time monitoring tool as part of the validation platform, will allow, when DPI are lost or not adequate, detect a potential anomaly and revert NM operation to using FPL data for trajectory prediction (similarly to the case of A-CDM airports) – performance degraded, but safety ensured.

This could be detected when DPIs are issued in real time, through B5-B9 Tactical Conflict Management barrier ("ATCO Monitors for potential conflicts. Detects and resolves them before they result in losses of separation"), resulting in a MAC-SC4b hazard ("A situation where an imminent infringement coming from a planned conflict that should have been resolved by Traffic planning & Synchronization was prevented by tactical conflict management") archived as a MF5.1 ("Planned Tactical conflict").



EUROPEAN PARTNERSHIP

Co-funded by the European Union

Use Case / Service failure mode	Example of causes & preventive mitigations	Operational Effect (through service provision to ATS or aircraft)	Mitigations protecting against propagation of effects	Service hazard & Severity
Provision of departure planning information to the NM	RNI platform failure	Possible sector overloads through negatively impacting the DCB process, including the efficiency of the last barrier within DCB which is the Hotspot monitoring in view of late detection and resolution	A DPI real-time monitoring tool as part of the validation platform, will allow, when DPI are lost or not adequate, detect a potential anomaly and revert NM operation to using FPL data for trajectory prediction (similarly to the case of A-CDM airports) – performance degraded, but safety ensured.	Planned Tactical conflict (MF5.1); MAC-SC4b
	RNI platform AOP-NOP Connection failure	Possible sector overloads through negatively impacting the DCB process, including the efficiency of the last barrier within DCB which is the Hotspot monitoring in view of late detection and resolution	A DPI real-time monitoring tool as part of the validation platform, will allow, when DPI are lost or not adequate, detect a potential anomaly and revert NM operation to using FPL data for trajectory prediction (similarly to the case of A-CDM airports) – performance degraded, but safety ensured.	Planned Tactical conflict (MF5.1); MAC-SC4b
	RNI platform data integration failure	Possible sector overloads through negatively impacting the DCB process, including the efficiency of the last barrier within DCB which is the Hotspot monitoring in view of late detection and resolution	A DPI real-time monitoring tool as part of the validation platform, will allow, when DPI are lost or not adequate, detect a potential anomaly and revert NM operation to using FPL data for trajectory prediction (similarly to the case of A-CDM airports) – performance degraded, but safety ensured.	Planned Tactical conflict (MF5.1); MAC-SC4b

Table 11. Full HAZID working table

B.2 HAZID participation list

Several long meetings were held to assess the safety implications (official and internal ones). This meetings included Alan Marsden as Solution 28.1 Leader and Octavian Fota in the role of PJ19 Safety Representative).

Appendix C Designing the Solution functional system for Normal and Abnormal conditions of operation

C.1 Deriving SRD from the SRS

SRS for Normal and Abnormal Operation (ID & content)	Safety Requirement at Design level[1] (SRD) or Assumption	Maps onto
SRS 001: AUs/GHs shall submit (and resubmit if any update is needed) the FPL in time for enabling reliable traffic prediction	**SRD 001:** RNI platform shall validate the FPL in accordance with the available information and assure the correct information is available	Integration with IFPS (Integrated initial flight plan processing system)
SRS 002: AUs/GHs shall assure the integrity of the data that will undergo through a system check to assure it	**SRD 002:** The RNI platform shall assure the correct computation, visualization and distribution to all the involved Stakeholders of the Target and Estimated Times	Integration with external systems or manual AUs/GHs inputs
SRS 003: Airport Operator shall assure the integrity of the data contained in an E-DPI that will be used by the NM	**SRD 002:** The RNI platform shall assure the correct computation, visualization and distribution to all the involved Stakeholders of the Target and Estimated Times	DPI emission service to NMOC
SRS 004: Airport Operator shall assure the integrity of the data contained in a T-DPI-t that will be used by the NM	**SRD 002:** The RNI platform shall assure the correct computation, visualization and distribution to all the involved Stakeholders of the Target and Estimated Times	DPI emission service to NMOC
SRS 005: NM shall assure the integrity of the data contained in a FUM that will be used by the Airport Operator for the whole A-CDM process computation	**SRD 002:** The RNI platform shall assure the correct computation, visualization and distribution to all the involved Stakeholders of the Target and Estimated Times	FUM reception service from NMOC

Co-funded by the European Union

SRS 006: AUs/GHs shall assure the integrity of the TOBT declared, which will feed the PDS and will be used for Resource allocation	**SRD 002:** The RNI platform shall assure the correct computation, visualization and distribution to all the involved Stakeholders of the Target and Estimated Times	Integration with external systems or manual AUs/GHs inputs
SRS 007: Stakeholders shall assure the integrity of any milestone an aircraft goes through (e.g. ACGT) provided to the RNI platform with the correct procedures	**SRD 002:** The RNI platform shall assure the correct computation, visualization and distribution to all the involved Stakeholders of the Target and Estimated Times	Integration with external systems or manual AUs/GHs inputs
SRS 008: ATC shall assure the integrity of the TSAT declared in case a Departure Manager is available	**SRD 002:** The RNI platform shall assure the correct computation, visualization and distribution to all the involved Stakeholders of the Target and Estimated Times	Integration with external systems or manual ATC inputs
SRS 009: Airport Operator shall assure the integrity of the data contained in a T-DPI-s that will be used by the NM	**SRD 002:** The RNI platform shall assure the correct computation, visualization and distribution to all the involved Stakeholders of the Target and Estimated Times	DPI emission service to NMOC
SRS 010: Airport Operator shall assure the integrity of the data contained in a C-DPI that will be used by the NM	**SRD 002:** The RNI platform shall assure the correct computation, visualization and distribution to all the involved Stakeholders of the Target and Estimated Times	DPI emission service to NMOC
SRS 011: Whenever RNI platform Servers are down, a degraded mode shall be provided in which the information shall be migrated to another server with limited capabilities that will allow the operation to continue but with restricted mechanics	**SRD 003:** The RNI platform shall have the possibility to seamlessly migrate to a server with reduced capabilities until the main servers recovers from the failure.	Integration with external systems or manual AUs/GHs inputs
SRS 012: Whenever the AU/GH data is not received partially, Stakeholders shall assure that there is the possibility to introduce this data manually to assure the consistency and integrity of the RNI model. In case ATC	**SRD 002:** The RNI platform shall assure the correct computation, visualization and distribution to all the involved Stakeholders of the Target and Estimated Times	Integration with external systems or manual AUs/GHs inputs

Co-funded by the European Union

could not provide their data, there is the possibility to be introduced, but, if the workload is considered too high, it shall be avoided and ATC data will be incomplete reducing the benefits gained in the RNI model. It shall be assured that the DPIs emission to the NMOC is not compromised, if it is, then we are talking about a failure condition in the "Provision of departure planning information to the NM" service		

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

C.2 Static analysis of the solution functional system behaviour

Non applicable.

C.3 Dynamic analysis of the Solution functional system behaviour

Non Applicable.

Co-funded by the European Union

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

This appendix presents the detailed risk evaluation and mitigation of the Service Hazards from section 4.4 performed at the level of the design of the solution functional system.

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

The purpose is to derive from the SRS (integrity/reliability) that have been derived in section 4.4.2 (SRS 013):

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

D.1.1 Top-down analysis of the design

Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
C01	RNI platform failure	RNI platform is down and could not provide the service defined	Return DCB process method through the flight plans data rather without the DPI information.
C02	RNI platform AOP-NOP Connection failure	The receptor or the emissary is not able to stablish the communication process and the data could not be transmitted	Return DCB process method through the flight plans data rather without the DPI information.
C03	RNI platform data integration failure	The data is not reliable due to the failure in the integration with other systems or non-reliable sources	Return DCB process method through the flight plans data rather without the DPI information.

Table 13. Example of table detailing one service hazard causes and associated preventive mitigations (SRD)

D.1.2 Bottom-up analysis of the design

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Functional system element	Failure mode	Effects	Mitigation/Safety Requirement	Service hazard
RNI platform	RNI platform NM connection fails	RNI platform – NM exchange of information is either impossible or the data integrity could not be assured	OBJ-04-W2-28.1-V3-VALP-2811.0005	Service Provision of departure planning information to the NM compromised

Table 14. Example of FMEA (Failure Modes and Effects Analysis) table

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

SRS (functionality& performance) for protective mitigation (ID & content)	Safety Requirement at Design level[2] (SRD) or Assumption	Maps onto
SRS 013: Provision of a DPI real-time monitoring tool that in case of degraded DPI information provision, when DPI are lost or not adequate, it detects a potential anomaly and stops the reception of DPIs, reverting the NM procedures back to using FPL data for trajectory prediction (similarly to the case of A-CDM airports) – performance degraded, but safety ensured.	**SRD 004:** Implementation of a capability that allows to detect when, either the information of the DPIs is not transmitted, or when this information is compromised and does not have the precision and integrity required. At that moment, NM performs the DCB process again with the flight plans data instead of the data contained in the DPIs, reducing the capacity of the sectors due to the lower precision of the information, but increasing security (old operating method)	DPI emission service to NMOC

Table 15: SRD derived by mapping SRS (functionality&performance) for degraded conditions on to Design Model Elements

Co-funded by the European Union

Appendix E Assumptions, Safety Issues & Limitations

E.1 Assumptions log

No Assumptions were required therefore documented

E.2 Safety Issues log

No additional safety issues were risen during the meetings (besides the ones contained in the hazard identification in Appendix B), therefore there is no safety issues log.

E.3 Operational Limitations log

No operations limitations were raised during the meetings, therefore there is no operations limitations log.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

-END OF DOCUMENT-

EUROPEAN PARTNERSHIP

Co-funded by the European Union