Deliverable Step 1 - Fully Validated SPR

Document information	
Project Title	Ground and Airborne Capabilities to Implement Sequence
Project Number	05.06.01
Project Manager	NORACON
Deliverable Name	Deliverable Step 1 - Fully Validated SPR
Deliverable ID	D84
Edition	00.05.00
Template Version	03.00.00
Task contributors	
AIRBUS, ALENIA, DFS, ENAV, Eurocontrol, NATS and NORACON	

Abstract

The document includes the initial set of the safety and performance requirements (SPR) for the implementation of the Ground & Airborne Capabilities to Implement Sequence based on the Controlled Time of Arrival (CTA) concept supporting SESAR Solution#6. It also describes the safety assessments and performance assessment performed in order to justify the identification of the described requirements.

Authoring & Approval

Prepared By – *Authors of the document.*		
Name & Company	Position & Title	Date
[redacted] ENAV	[redacted]	15/07/2016

Reviewed By – *Reviewers internal to the project.*		
Name & Company	Position & Title	Date
[redacted] NORACON	[redacted]	13/07/2016
[redacted] Airbus		13/07/2016
[redacted] /Airbus		13/07/2016
[redacted] Airbus		13/07/2016
[redacted] NORACON		13/07/2016
[redacted] DFS		13/07/2016
[redacted] Alenia-Leonardo		17/06/2016
[redacted] Eurocontrol		13/07/2016
[redacted] Eurocontrol		13/07/2016
[redacted] NATS		13/07/2016
[redacted] NORACON		13/07/2016

Reviewed By – *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date
[redacted] ENAV	[redacted]	04/08/2016
[redacted] /Airbus		13/07/2016
[redacted] Eurocontrol		06/10/2016

Approved for submission to the SJU By – *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
[redacted] /Airbus	[redacted]	21/07/2016
[redacted] DFS		28/07/2016
[redacted] Alenia-Leonardo		04/08/2016
[redacted] Eurocontrol		28/07/2016
[redacted] NATS		27/07/2016
[redacted] NORACON		04/08/2016

Rejected By – *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
None		

Rational for rejection
None.

Document History

Edition	Date	Status	Author	Justification
00.00.01	30/05/2016	Draft version	[redacted]	Version updated OFA 4.1.5 SAR
00.00.02	06/06/2016	Released for internal review		Version updated with Final OSED
00.00.03	04/07/2016	Released for external review		Final version for external review
00.01.00	22/07/2016	Final version		Released for Approval
00.02.00	04/08/2016	Final version		Updated for submission to the SJU
00.03.00	05/10/2016	Final version		Updated after SJU review 1th round
00.04.00	27/10/2016	Final version		Updated after SJU review 2nd round
00.05.00	30/11/2016	Final version		Rescope and formal update

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

List of figures

Executive summary

The document is related to the T05.06.01-103 task – Step 1 Fully Validated SPR – of the 05.06.01 SESAR project: Ground & Airborne Capabilities to Implement Sequence. The results of the project is supporting SESAR Solution #6

Development of *"Update of SPR with all results* [Task T103]" has to be considered as the *Step 1 Fully Validated SPR* deliverable of Step 1 SPR group of documents. It follows the "*Step 1 SPR Iteration 3* [Task T088]".

The main objective of P05.06.01 is to enable the more widespread use of on-board aircraft time and trajectory-management abilities supported by appropriate ground-based systems to improve arrival management and sequence building. The CTA function, on which is based the P05.06.01, is important to support Traffic Synchronization activities improving arrival management and sequence building especially for high to medium density operations. Note that for this version of document, as it follows Step 1 activities, the CTA concept is investigated for low to medium density operations.

The document collects safety and performance requirements for the implementation of the Ground & Airborne Capabilities to Implement Sequence related to the use of Controlled Time of Arrival (CTA) time constraints and trajectory exchange explored within an Initial 4D (i4D) environment. Note that i4D enhances CTA operations but it is not a prerequisite for CTA itself. In other words, CTA operations are possible also for non-i4D equipped aircraft.
The SPR requirements are identified starting from the analysis of the existing material of the related Step 1 OSED - Final document [11], the P16.6.1 OFA 4.1.5 SAR Iteration3 [24] and P16.6.2 OFA 4.1.5 SRA [43]. In particular, the P05.6.01 people contributed to the P16.06.01 and P16.06.02 work in order to develop their documentation and these collaboration permitted to obtain both safety and performance requirements.
The requirements collected in this context are properly justified by Operational Safety Assessment (OSA), Operational Performance Assessment (OPA) and Security Risk Assessment (SRA) presented in dedicated appendix sections below.

Giving an overview of the work performed, the OSA aims at defining:

- Safety objectives to mitigate the effects of operational hazards. They define the maximum frequency of occurrence at which a hazard can be tolerated to occur.
- Safety requirements to meet the above defined safety objectives. They could be seen as risk mitigation means required to reduce the risk(s) to an acceptable level.

The OSA has been carried out following the guidelines provided by P16.06.01 SESAR Safety Reference Material (SRM) [8].

From performance perspective, the OPA aims at defining the performance requirements associated to CTA operations. This evaluation has been done by:

- Listing the identified operational potential issues which may impact negatively on Key Performance Areas (KPAs);
- Listing the mitigations or preventions for these issues and then
- Deriving the associated Operational Performance Requirements.

Moreover, OFA Security Risk Assessment of P16.6.2, aiming to produce controls that mitigated the risk of identified primary assets, has been taken into account to produce SPR security requirements.

Note that for each kind of requirements collected into SPR, Appendix A shows the correspondent assessments and justifications.

Introduction

1.1 Purpose of the document

This Safety and Performance Requirements (SPR) document provides the safety and performance requirements for Services related to the Operational Processes defined in the paragraph 2.3 .

The Safety and Performance Requirements, collected into this document, coming from the Safety and Performance Assessment related to the implementation of CTA aspects in Step 1 phase. In particular, Safety Requirements have been updated and refined in accordance with the safety activities done in the context of the related OFA while, Performance Requirements have been introduced as results of analysis of Key Performance Areas potential operational impact on CTA operations.

1.2 Scope

The P05.06.01 Step 1 Fully Validated SPR supports the operational services [2.2] and concept elements [2.1] identified in the chapter 2.

The scope of the document is to provide the basis to ensure and demonstrate that the implemented system, considering its inherent design and technologies, can meet the relevant operational, safety and performance requirements for the services described [2.2]. Following the approach described in Figure 1 below, the Steps are driven by the OI Steps addressed by the project in the Integrated Roadmap document [22]. In detail, the safety and performance requirements defined in the document are related to the services expected to be provided by the use of CTA operations.

This SPR document contributes to the Operational Focus Area 04.01.02 even though the major part of documentations used refer to the old OFA 04.01.05 "i4D + CTA". Therefore this deliverable has been developed taking into account the OFA i4D + CTA Safety Assessment Report [24] driven by P16.06.01, with the support of P4.3, P05.06.01 and WG78 technical and operational experts and OFA 04.01.05 Security Risk assessment of P16.06.02 [43]. Regarding the performance assessment, the work performed aims to obtain particular mitigations and/or preventions necessary to overcome the possible negative impact that the new CTA operations may have on some Key Performance Areas with the objective to achieve the desired level of performance expectations.

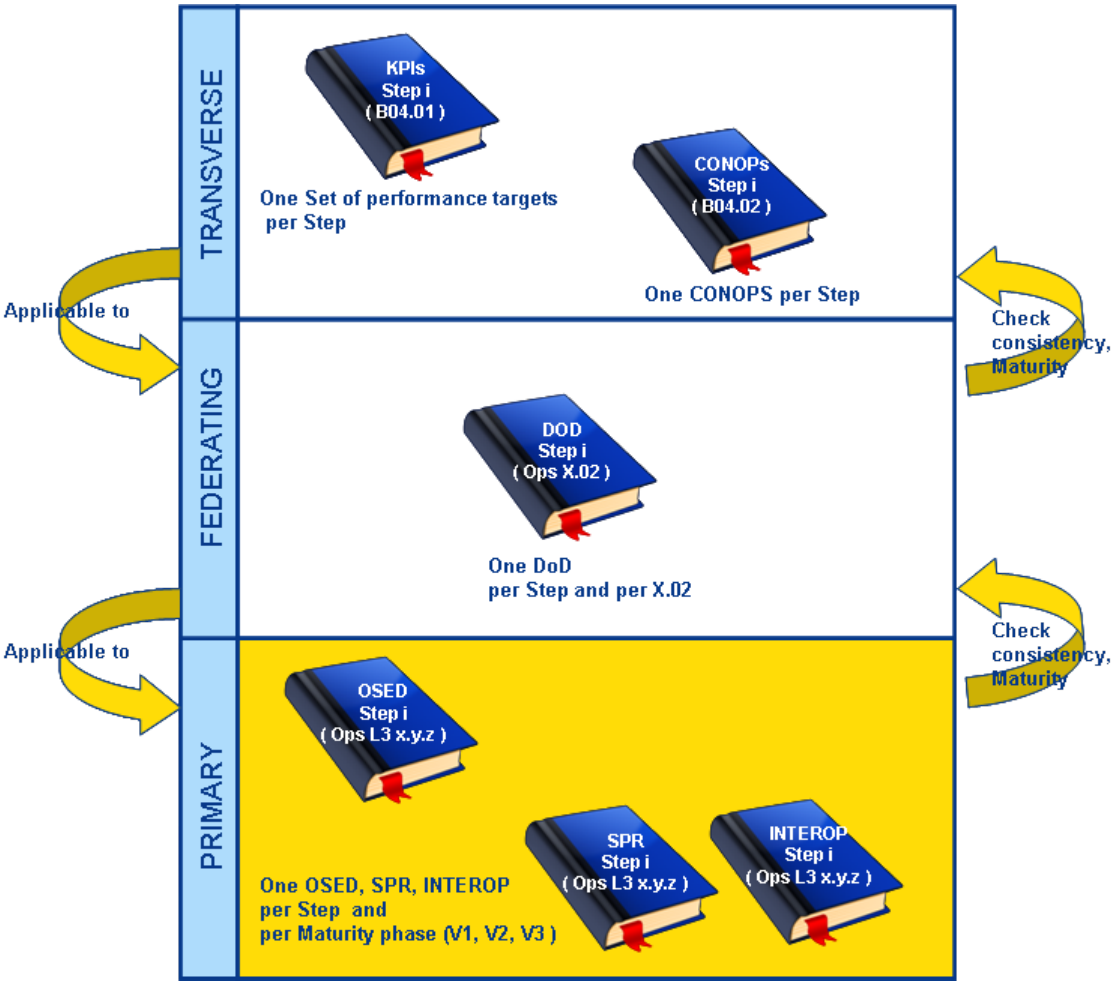

Figure 1: SPR document with regards to other SESAR deliverables

1.3 Intended readership

Following Primary Projects could get benefit from this SPR:

- (in WP 04) P4.3, P4.5
- (in WP 05) P5.5.1, P5.6.7
- (in WP 09) P9.1
- (in WP 10) P10.2.1, P10.7.1, P10.9.4

At a higher project level OPS, the following Federating Projects could take advantage of this document for the architecture and performance modelling activities:

- P4.2, P5.2, P5.3

The transversal areas could also benefit from this SPR:

- SWP16.06.01
- SWP 16.06.02
- SWP 16.06.05
- Project B.05

1.4 Structure of the document

The structure of this SPR is as follows:

- **Chapter 1** provides general information about the document.
- **Chapter 2** provides a summary of the operational concept described within P05.06.01 Step 1 OSED – Final [11].
- **Chapter 3** is dedicated to the collection of the safety and performance requirements coming from safety and performance assessments.
- **Chapter 4** lists the applicable and reference documents.
- **Appendix A** describes the whole assessment and justification performed in order to derive the related safety, security and other performance requirements.
- **Appendix B** shows the Accident Incident Model for Mid-Air Collision in En-Route and TMA.
- **Appendix C** shows Functional Blocking breakdown from Technical Architecture Description in Cycle 2015.
- **Appendix D** the Appendix D shows additional considerations that could represent useful inputs for future projects related to scopes similar to the P05.06.01 scope.

1.5 Background

A continuous coordination with OFA 04.01.05 Safety Plan working group, that involves P16.6.1, P4.3, P5.6.1 and WG 78 technical and operational experts, aiming to the production of the WP16.06.01 OFA i4D+CTA SAR, has been useful to perform a deep screening of the project driving and identifying the potential safety impact on CTA operations. The project safety activity has been deployed starting from the development of the concepts and, overall, from the OFA Safety Assessment Report [24]. The continuous exchange with the 16.06.01 Front Office reference (by AIRBUS) has contributed in the development of the full OFA 04.01.05 Safety works and, at the same time, on the identification of TMA scenario Hazards. The expertise involved in the OFA SAR joint activities were identified between the contributors of the 05.06.01 SPR (ENAV, ECTL, and AIRBUS via the 16.06.01 Front Office reference for the P05.06.01 AIRBUS itself). The approach followed is the one proposed by SESAR Safety Reference Material (SRM)[8] which promotes a safety assessment dealing with both pre-existing hazards, in absence of failure of the system (i.e. success approach), and possible hazards generates in case of failure of the system (i.e. failure approach). Once the hazards have been identified and the associated safety objectives have been set, it has been required to analyse the proposed architecture in order to identify the potential causes which could lead to a hazard and so derive the safety requirements.

Regarding the performance and security risk assessment it is important to highlight that for the first one a useful methodology has been set while for the second one was coordinated with P16.6.2.

Please note also that the operational environment and services described in the P05.06.01 OSED [11] have been considered as a starting point because, for both safety and performance assessment, it is important to have a clear picture of the services, which will be provided by the CTA function, and of the environment in which it will operate.

1.6 Glossary of terms

Term	Definition
Abnormal conditions	'Abnormal conditions' are those external changes in the operational environment that the ATM/ANS functional system may exceptionally encounter (e.g. severe WX, airport closure, etc.) under which the system may be allowed to enter a degraded state provided that it can easily be recovered when the abnormal condition passes and the risk during the period of the degraded state is shown to be acceptable.[8]
Asset	Elements in the system that have value for the achievement of business objectives [31]
Availability	The property of being accessible and usable upon demand by an authorized entity[31]
Basic CTA Aircraft	A term, frequently used especially within P5.6.1 discussions and documents, normally to distinguish between the CTA-related capability of currently equipped aircraft (i.e. those aircraft that are equipped with today's RTA functionality), and the capability of i4D aircraft (i.e. those aircraft that are equipped with the enhanced RTA capability/functionality being considered/developed within i4D). The term 'Non-i4D' is also used to describe Basic CTA/RTA aircraft. Note: The term could - and probably should in most cases - be read as "Basic RTA", since the CTA is simply the ground-derived time delivered to the flight and it is the airborne RTA function that controls the aircraft to the time.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [31]
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature [31]
CTA	Controlled Time of Arrival – An ATM imposed time constraint on a defined merging[1] point associated to an arrival runway [SESAR lexicon]. CTA may be the original ETA of the aircraft converted to a CTA, or it may be the aircraft's original ETA with a time-adjustment, used, in either case, to 'control' the required time/position for the aircraft in the arrival sequence. **Note**: This term is sometimes used interchangeably with CTO. **Note**: The term 'CTA Operations' are sometimes used as a generic term to describe the application of the CTA concept.
CTO	Controlled Time Over – An ATM imposed time constraint over a point [SESAR Lexicon] CTO is an ATM constraint for an aircraft to pass a designated point at a designated time. It may be the original ETO of the aircraft converted to a CTO or it may be the aircraft's original ETO with a time-adjustment, used, in either case, to 'control' the required time for the aircraft to pass a designated point. ***Note:** This term is sometimes used interchangeably with CTA.*

[1] The CTA definition provided is extracted from the SESAR Lexicon. For practical purposes the CTA is more likely to be used on 'a defined point' associated to an arrival runway, rather than specifically being 'a defined merging point.

Term	Definition
Degraded mode	'Degraded mode of operation' is a pre-defined reduced level of operational service invoked by equipment outage or malfunction, staff shortage or procedures.[8]
EPP	ADS-C EPP (Extended Projected Profile) report is the ADS-C report containing the sequence of 1 to 128 waypoints or pseudo waypoints with associated constraints or estimates (altitude, time, speed, etc…), Gross Mass and estimate at Top Of Descent, speed schedule, etc.[8]
ETA	Estimated Time of Arrival - The time computed by the FMS for the flight arriving at a point related to the destination airport [SESAR lexicon].
ETA Min/Max interval	The ETA min/max interval[2] defines the range of arrival times at a specified lateral fix which are achievable using RTA, with a level of confidence of 95% assuming meteorological uncertainty. The computation of ETA min/max does not depend of current guidance mode and it takes into account all applicable flight plan constraints. Note: WG85 [23] releases a white paper detailing the ETA Min/Max computation.
E-TMA	Extended Terminal Manoeuvring Area – A TMA extending to the aircraft top of descent. The E-TMA usually includes the TMA and nearby feeder sectors.
ETO	Estimated Time Over - The time computed by the FMS for the flight to pass a point on its intended trajectory [P5.6.1 use].
Hazard	Hazard shall mean any condition, event, or circumstance which could induce an accident. This covers both pre-existing aviation hazards (not caused by ATM/ANS functional systems) and new hazards introduced by the failure of the ATM/ANS functional systems.[8]
I4D Aircraft	Aircraft equipped with CPDLC, ADS-C for communication of RTA reliable interval and EPP downlink and enhanced FMS RTA functionality, as developed by Airbus within P09.01, with enhanced accuracy and predictability (Assurance of 95% fulfilment of CTA with +/- 10 seconds accuracy).
I4D Operations	I4D Operations is a generic term used to describe the use of i4D services to enhance CTA operations.
I4D Services	I4D service is a generic term used to encompass the use of information that is available from i4D equipped aircraft only, such as ADS-C information, ETA Min/Max information and EPP downlink.
Non-CTA Aircraft	Aircraft unable to participate in CTA operations (neither Basic CTA nor i4D capability).
Likelihood	Evaluation of the chance of a threat scenario successfully occurring [31]

[2] In this statement is used the ETA Min/Max "interval", already known as ETA Min/Max "window" to be coherent with WP9.1 definition.

Term	Definition
Normal conditions	'Normal conditions' are those conditions of the operational environment the ATM/ANS functional system is expected to encounter in day-to-day operations and for which the system must always deliver full functionality and performance.[8]
Pre-existing hazard	Pre-existing hazard by definition exists in the operational environment before any form of 'deconfliction' has taken place. It is, therefore, not caused by the system – rather, the main purpose of introducing the system is to eliminate this pre-existing hazard or at least maintain the associated risks at an acceptably low level.[8]
Primary Asset	Intangible function, service, process or information that are part of the ATM system within the scope of the project and has value to the system [31]
Risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby have an impact on the OFA [31]
Risk assessment	The overall process of risk identification and risk evaluation [31]
Risk evaluation	The process of assigning values to the likelihood and impacts of a risk [31]
Risk identification	The process of finding, listing and characterizing elements of risk [31]
Risk treatment	The process of selecting and implementing measures to modify risk [31]
Safety requirements	Safety requirement shall mean the necessary risk reduction measures identified in the risk assessment to achieve a particular safety objective. They describe the functional, performance and integrity safety properties at the system-design level as well as organisational, operational, procedural, and interoperability requirements or environmental characteristics – from Article 2(12) of Regulation (EC) No 1035/2011. Currently, in Regulation (EC) No 1035/2011, the following definition applies: "'safety requirement' means a risk-mitigation means, defined from the risk-mitigation strategy that achieves a particular safety objective, including organisational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics".[8]
Success approach	It is the first step required to perform a complete Operational Safety Assessment in which we assess how effective the new concepts and technologies would be when they are working as intended – i.e. how much the pre-existing risks that are already in aviation will be reduced by the ATM changes. This is concerned with the positive contribution to aviation safety that the ATM changes make in the absence of failure.[8]

Term	Definition
Supporting Asset	Supporting assets are entities which enable the primary assets. Supporting assets possess the vulnerabilities that are exploitable by threats aiming to impair primary assets. [31]
Threat	The potential cause of an unwanted incident which may result in an impact on the OFA [31]
Threat Scenario	A threat scenario is a combination of a threat over a supporting asset within the considered environment [31]
Vulnerability	A security weakness of an asset that can be exploited by an attacker via a threat [31]

1.7 Acronyms and Terminology

Term	Definition
4DTRAD	Four Dimension Trajectory Data Link Service
AC or A/C	Aircraft (including Aircraft Systems)
ACC	Area Control Centre
ACL	ATC Clearance
ACT	Activation Message (OLDI)
ADAS	Advanced Data-link and Airborne Surveillance Applications
ADD	Aircraft Derived Data
ADS-C	Automatic Dependant Surveillance – Contract
AGDC	Air-Ground Datalink Communication [Functional Block]
AGDS	Air-Ground Datalink Services [Functional Block]
AIM	Accident Incident Model
AMA	Arrival Management Message (OLDI)
AMAN	Arrival Manager
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider

Term	Definition
AoR	Area of Responsibility
ASAS	Airborne Self Separation
ASOR	Allocation of Safety Objectives and Requirements
ASPA	ASAS Spacing
ATC	Air Traffic Control
ATM	Air Traffic Management
ATN	Aeronautical Telecommunications Network
ATS	Air Traffic Services
ATSU	Air Traffic Service Unit
ATSU_CONTROL	Air Traffic Service Unit of aircraft under control
ATSU_DEST	Air Traffic Service Unit of aircraft destination
ATCO	Air Traffic Controller
ATCO_EXE	Executive Controller
ATCO_PLN	Planner Controller
BC	Basic Causes
BPMN	Business Process Modelling Notation
CDA	Continuous Descent Approach
CDA	Current Data Authority (for Datalink)
CPDLC	Controller Pilot Datalink Communication
COP	Co-ordination Point
CTA	Controlled Time of Arrival
CTO	Controlled Time Over
DCB	Demand-Capacity Balancing
DUG	Datalink User Group
E-AMAN	Extended AMAN

Term	Definition
EC	Environmental Condition
EFF	Efficiency
EMM	External Mitigation Means
ENAV	Italian Company for Air Navigation Services (Ente Nazionale per l'Assistenza al Volo)
ENR	En-Route
ENV	Environment
EPP	Extended Projected Profile
ETA	Estimated Time of Arrival
ETFMS	Enhanced Tactical Flow Management System
E-TMA	Extended Terminal Manoeuvring Area
EUROCAE	European Organization for Civil Aviation Equipment
FAF	Final Approach Fix
FC	Flight Crew
FDPS	Flight Data Processing System
FH	Flight Hour
FLE	Flight Efficiency
FMC	Flight Management Computer
FMS	Flight Management System
FPL	Flight Plan
F&P	Functionality & Performance
F&P- SO	Functionality & Performance- Safety Objective
GD	Ground System
G/G	Ground to Ground
HMI	Human Machine Interface
I4D	initial Four Dimensions

Term	Definition
IAF	Initial Approach Fix
ICAO	International Civil Aviation Organisation
IER	Information Exchange Requirements
IFR	Instrument Flight Rules
IMM	Internal Mitigation Means
IOC	Initial Operational Capability
IT	Iteration
KPA	Key Performance Area
KPI	Key Performance Indicator
LoA	Letters of Agreement
LREH	Long Range Eligibility Horizon
MAC	Mid Air Collision
MET	Meteorology
MF	Metering Fix
MP	Metering Point
MTCD	Medium Term Conflict Detection
OE	Operational Effect
OFA	Operational Focus Area
OH	Operational Hazard
OHA	Operational Hazard Assessment
OI	Operational Improvement (Step)
OLDI	Online Data Interchange
OPA	Operational Performance Assessment
OSD	Operational Service Description
OSED	Operational Service and Environment Description

Term	Definition
OSP	Operational Sub-Package
PP	Primary Projects
PRE	Predictability
P-RNAV	Precision Area Navigation
PT	Predicted Trajectory
RBT	Reference Business Trajectory
RCS	Risk Classification Scheme
RMT	Reference Mission Trajectory
RNP	Required Navigation Performance
R/T	Receiver/Transmitter
RTA	Required Time of Arrival
SAF	Safety
SHO	Sector Operating per Hour
SO	Safety Objectives
SPR	Safety and Performance Requirements
SR	Safety Requirements
SRM	Safety Reference Material
STAR	Standard Terminal Arrival Route
STCA	Short Term Conflict Alert
TCAS	Traffic Collision Avoidance Systems
TCM	Traffic Complexity Manager
ToD	Top of Descent
TMA	Terminal Manoeuvring Area
TMF	Trajectory Management Framework
TMS	Traffic Management System

Term	Definition
TP	Trajectory Prediction
TRA	Temporary Reserved Airspace
TTG	Time To Gain
TTL	Time To Lose
VDL	VHF Datalink
VHF	Very High Frequency
WCE	Worst Credible Effect
WILCO	Will comply

2 Summary of Operational Concept (from OSED)

Since the following paragraphs are derived from P05.06.01 OSED [11], please refer to it for a complete and detailed description of the concept.

2.1 Description of the Concept Element

SESAR Storyboard Step 1 "Time Based Operations" describes the operational improvements and capabilities to be progressively available from 2013 onwards and is focused on KPAs for Flight Efficiency, Predictability, Capacity and Environment.

Project 05.06.01 is concerned with how CTA will be used to support Traffic Synchronisation activities, therefore whilst the exchange of trajectory data via datalink (i4D) represents the nominal scenario within the ATM target concept, it is important to note that i4D enhances CTA operations and it is not a pre-requisite for CTA operations, i.e. CTA may be used to support Traffic Synchronisation also in environments where i4D is not available.

With regards to i4D equipped aircraft:
'Initial 4D operations are limited to the sharing of on-board 4D trajectory data and the provision of a single time constraint at a specific point during the descent/approach phase including monitoring of trajectory and conformance to the assigned constraint'[57]

More in detail, i4D can be said to be comprised of two core elements:

1) A trajectory exchange between air and ground which may be used for multiple purposes including synchronised trajectory data (air and ground having a common view of the trajectory) and for use in ground based tools such as an Arrival Manager (AMAN), and;
2) The use of CTA/RTA within the context of Queue Management activities.

With regards to the first element, that of the trajectory exchange, there are fundamental conceptual questions surrounding both the purpose of the trajectory exchange (why are we doing it?), and the means to achieve the trajectory exchange (how do we do it?). In the first regard the synchronisation of trajectory information is vital, for safety reasons, to ensure that both air and ground have a common view of the trajectory. It is not possible for either actor to negotiate on, for example, changes to the trajectory if air (e.g. FMS) and ground (e.g. FDPS) have different views of the information. In the second regard, it is envisaged that required trajectory data will be exchanged through enhanced datalink systems and associated services. SESAR P4.5 and P5.5.1[57] have produced the Trajectory Management Framework (TMF) for Step 1 within which the Processes and Services relating to CTA& i4D are described and the reader is encouraged to consult [14] for a detailed view of trajectory related processes.

Within the Step 1 timeframe it is envisaged that the use of time constraints, associated to an arrival runway, will serve as the primary means to meter and sequence traffic in the Terminal Manoeuvring Area (TMA).
It is expected that Controlled Time of Arrival (CTA) constraints will be issued to aircrafts operating within congested nodes of the air traffic network as a means of transferring arrival delay from low level holding to the en-route phase of flight by means of linear holding. Existing airborne navigation and auto-flight capabilities, such as Required Time of Arrival (RTA) as provided by modern Flight Management Systems (FMS) and further RTA related development, will enable aircraft to self-manage to meet imposed time constraints and thus promote more flight efficient airborne managed delay profiles.

In the context of the operational concept description, the scope of Step 1 operations can be summarised as follows:

- The establishment of synchronised air and ground routes (i4D capability only);
- The proposal/use of Controlled Time of Arrival (CTA) with all interested actors, ground and airborne, involved for the purpose of synchronising arrival traffic at a specific waypoint.
- The additional capability to obtain from certain aircraft (i4D capability only) a Reliable RTA Interval (ETA Min/Max) at a waypoint on the aircraft's current route of flight, which may be used in CTA calculation.

In detail, the concept can be explicated into a series of steps (see Figure 2) described deeper into reference OSED [11]. Note that the blue boxes and arrows refer to i4D equipped aircrafts while red to basic CTA.

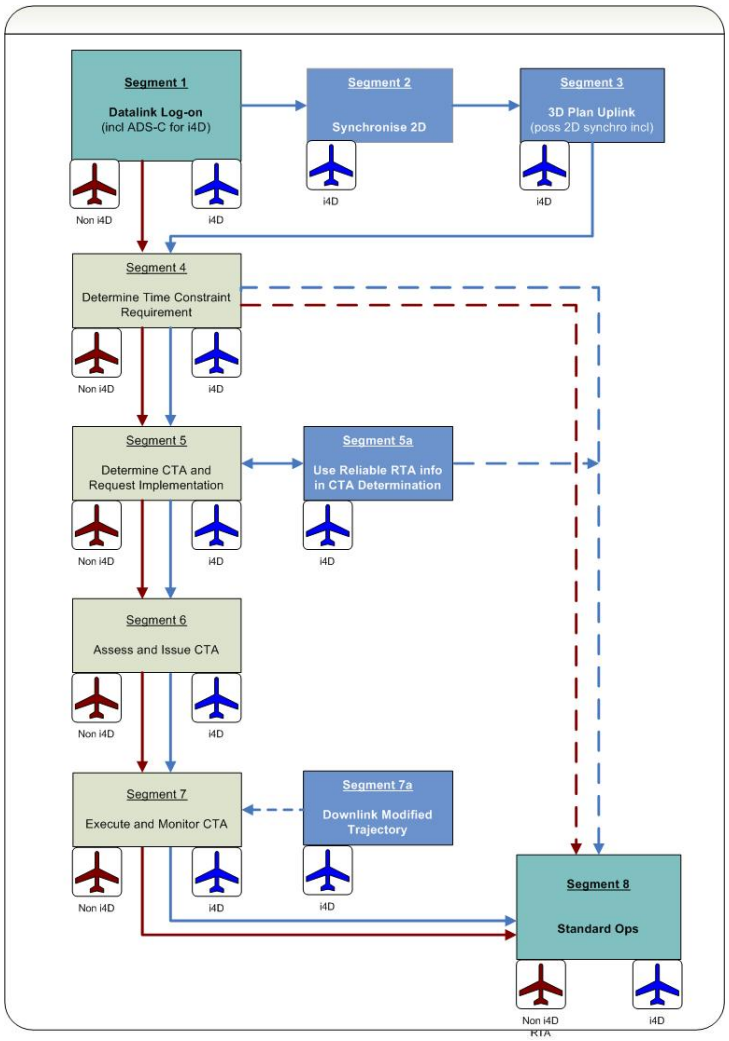

Figure 2: Arrival Management with CTA

2.2 Description of Operational Services

The following model is consistent with the model developed in the Interoperability document [25] of the P4.3 and adapts the symbology to the SRM guidance [8]. The following figure shows the OFA i4D+CTA functional model coming from OFA SAR document [24] so, for a detailed description, please refer to it.

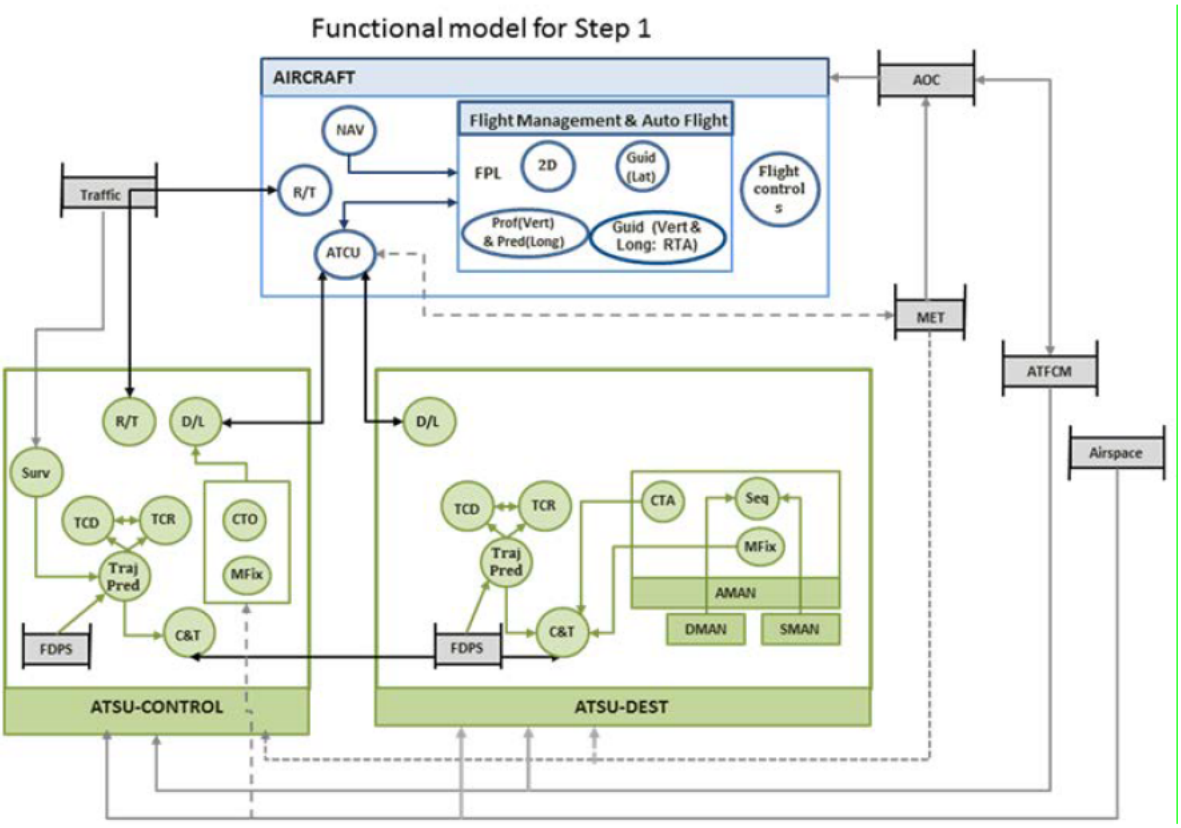

Figure 3: i4D+CTA OFA Functional Model

The model had been progressively elaborated to identify the functions supported by the services and impacted by the old i4D&CTA OFA. The functional model was useful to identify the functions supported by the services and impacted by the i4D + CTA OFA. The actual processes are described with the latest development in the next chapters.

2.3 OFA04.01.02 Enhanced Arrival & Departure Management Process

As reported in the OSED [11], the following high level process, covering the application Operational Focus Area (04.02.01) has been defined in the P5.2 Step 1 DOD latest update [12].

This process covers the OFA within which P5.6.1 has performed its work. A series of lower level processes, and the associated activity descriptions, relating to the CTA concept have been defined by P5.2 based on the work of P5.6.1 and are included in this section. Full details of the methodology used can be found in the reference document[12].

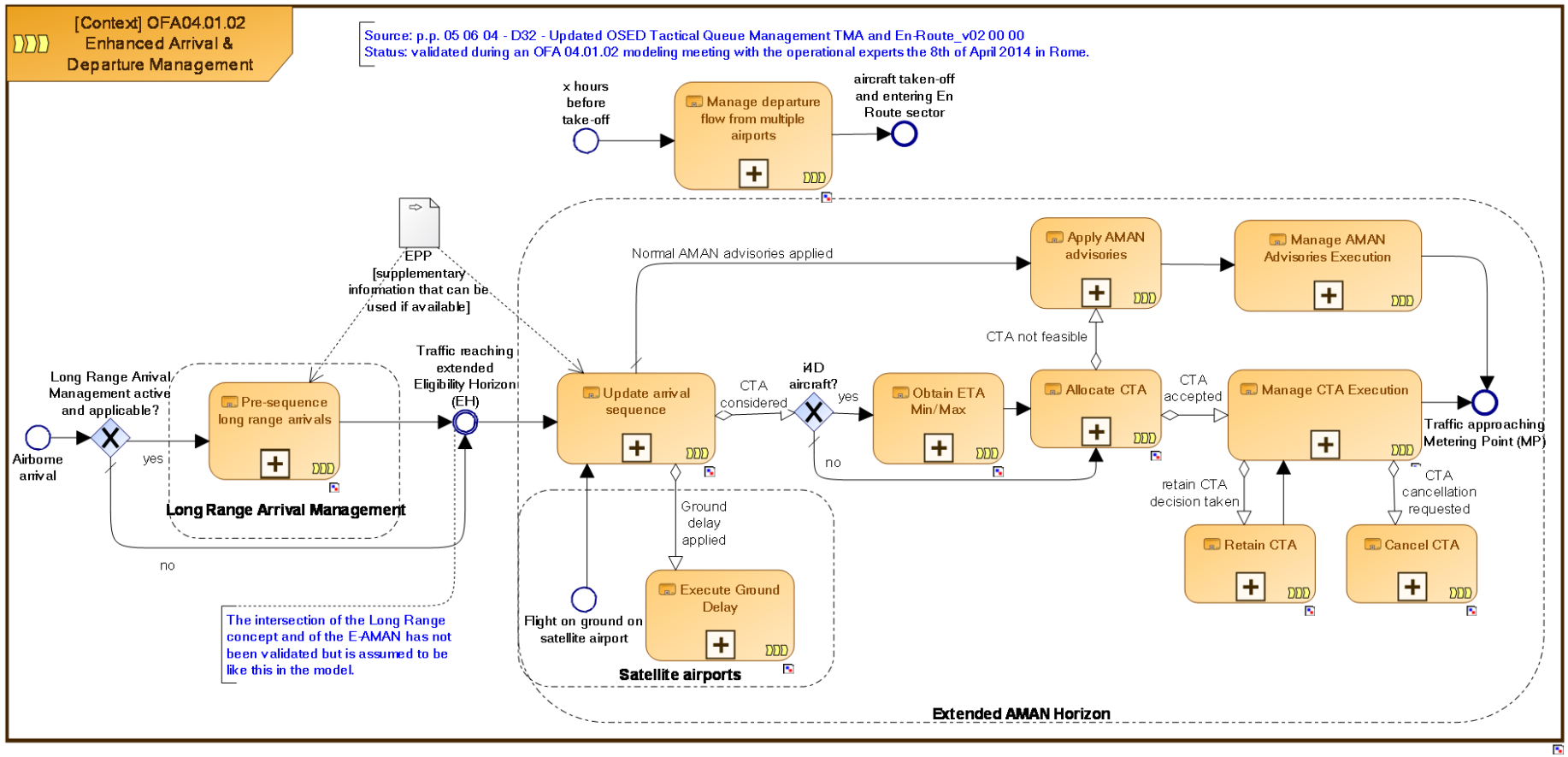

Figure 4: OFA04.01.02 Enhanced Arrival & Departure Management Process Diagram

Sequence and Meter Arrivals using a CTA

Within the OFA process model described in Figure 12, a number of CTA-specific processes were identified by WP5, using P5.6.1 material, and are shown in the following section. *'The models are produced in a bottom-up approach, based on the information found in the OSED 05.06.01 iteration 3 (20/09/2013) and the 4.5/5.5.1 TMF 2014 TN (11/12/2014). It has been linked to B4.2 models to ensure the top-down consistency. It is linked to the OFA 04.01.02 "Enhanced Arrival & Departure Management" and to the OIs TS-0103 and TS-0109 "Controlled Time of Arrival (CTA) in medium density/complexity and high density/complexity respectively.'*

Obtain ETA Min/Max

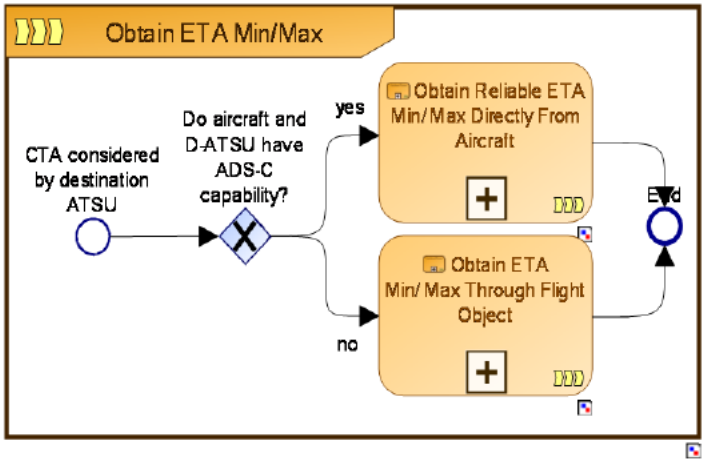

Figure 5: Obtain ETA Min/Max Process Diagram

Activity Name	Activity Description
Obtain Reliable ETA Min/Max Directly From Aircraft	The destination AMAN requests the ETA-min/max for its metering fix. The destination ATSU system automatically requests the ETA-min/max from the aircraft, which downlinks the information. The AMAN receives the information from the destination ATSU system.
Obtain ETA Min/Max Through Flight Object	The destination AMAN requests the ETA-min/max service for its metering fix. C-ATSU system automatically requests the ETA-min/max from the aircraft, which downlinks the information. C-ATSU publishes the ETA-min/max report in the Flight Object, which the destination AMAN retrieves.

Appendix A Table 1: Obtain ETA Min/Max Activity Description

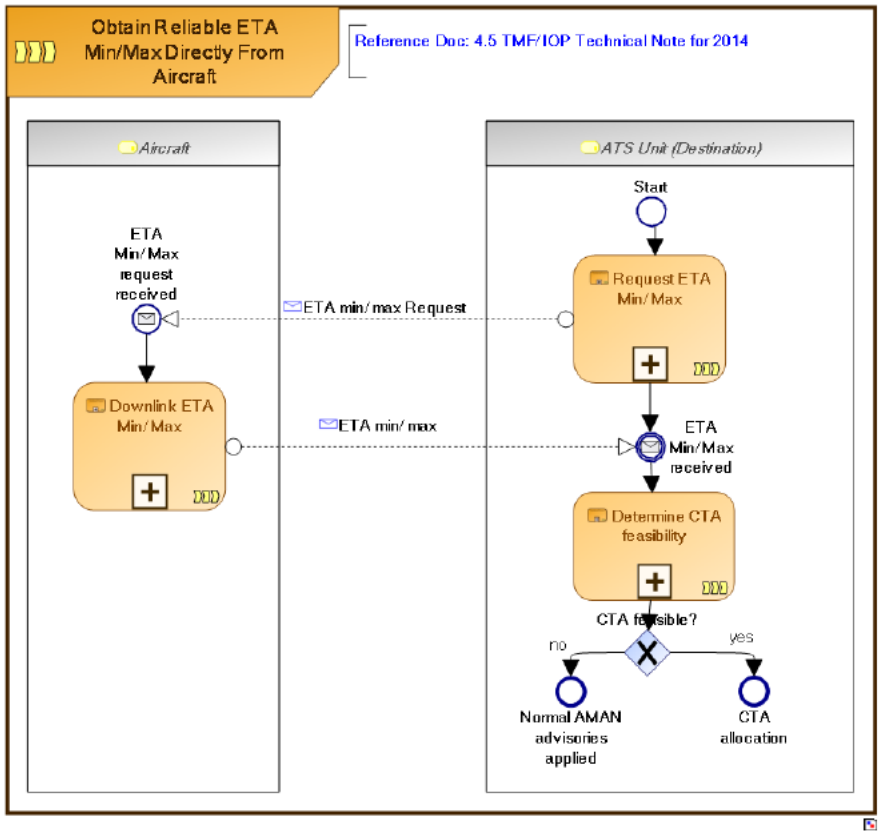

Figure 6: Obtain ETA Min/Max Directly From Aircraft Activity Diagram

Activity Name	Activity Description
Request ETA Min/Max	Upon request of the AMAN, the destination ATS unit automatically sends a request for the reliable ETA min/max for the route point specified by the AMAN.
Downlink Reliable ETA Min/Max	The aircraft downlinks the reliable ETA min/max.
Determine CTA feasibility	The destination ATSU automatically makes the received ETA min/max information available to the AMAN. The AMAN uses the information in determining if a CTA time is feasible or not for the flight.

Table 2: Obtain ETA Min/Max Directly From Aircraft Activity Description

Allocate CTA

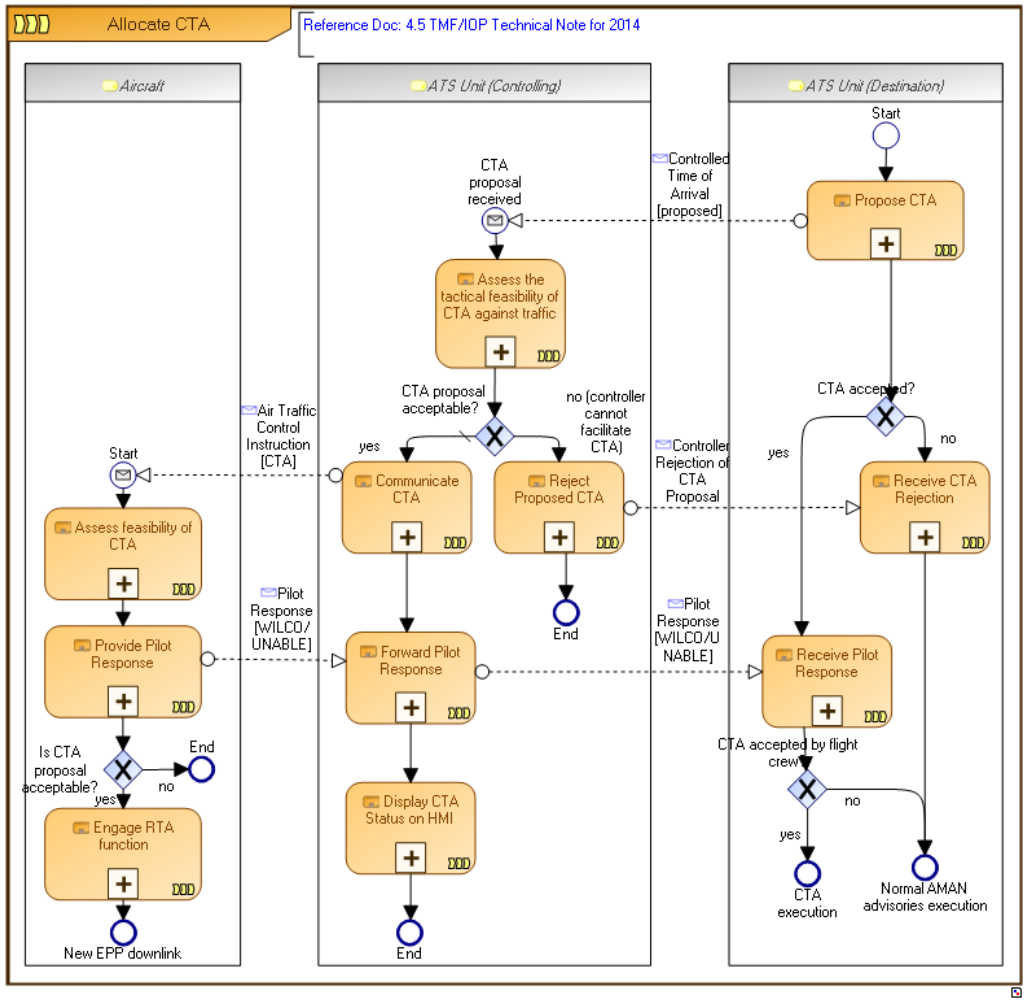

Figure 7: Allocate CTA Process Diagram

Activity Name	Activity Description
Propose CTA	The AMAN of the destination ATSU calculates the required time constraint (time and fix) for the flight determines that a CTA is appropriate and requests its issue to the flight.
Assess the tactical feasibility of CTA against traffic	The current controlling ATS unit retrieves the CTA Proposal from the Flight Object and notifies the controller through the HMI that a request for a CTA has been received. The controller performs an assessment of the potential impact of accepting the proposed CTA.
Reject Proposed CTA	If the controller assesses that they cannot facilitate the aircraft flying on its own speed authority to meet a CTA, (e.g. due to other traffic) they reject the CTA task using the HMI. The controller action to reject the uplink task updates the Flight Object with an indication that the controller has rejected the CTA Proposal.
Receive CTA Rejection (ATCO)	The destination ATS unit retrieves the upstream ATCO's response to the CTA Proposal from the Flight Object and makes it available to the AMAN so that it can update the status of its plan and devise an alternative strategy for the flight. *NOTE. Any intermediate downstream ATS units will also be made aware of the updated CTA operational status through subscription to the Flight Object. Controllers in any intermediate units will need to know if the aircraft is operating under its own speed authority in order to meet a CTA.*
Communicate CTA	The controller communicates the CTA via voice or via CPDLC using the HMI to uplink the appropriate CPDLC message to the aircraft. *NOTE. If used, the CPDLC message is expected to be pre-formatted by the system with the CTA Proposal.*
Assess feas bility of CTA	The Flight Crew determines if the CTA clearance received is acceptable and achievable by entering details into FMS.
Provide Pilot Response	The flight crew respond (either with WILCO or by voice) if the CTA is acceptable. If the CTA is not acceptable the flight crew respond UNABLE and also with voice, to indicate the reason for the rejection.
Engage RTA function	Flight Crew loads the RTA in to the FMS and adjusts the flight's trajectory according to the CTA entered into the FMS as a RTA.

Activity Name	Activity Description
Forward Pilot Response	The current controlling ATS unit automatically updates the operational status of the CTA in the Flight Object based on the flight crew response.
Display CTA Status on HMI	All controllers handling the flight are made aware of the CTA through the HMI. Controllers need to know if the aircraft has accepted a CTA as it will be operating under its own speed authority.
Receive Pilot Response	The destination ATS unit retrieves the flight crew response to the CTA Proposal from the Flight Object and makes it available to the AMAN so that it can update the status of its plan and devise an alternative strategy for the flight (if required as a result of a flight crew UNABLE response). *NOTE. Any intermediate downstream ATS units will also be made aware of the updated CTA operational status through subscription to the Flight Object. Controllers in any intermediate units will need to know if the aircraft is operating under its own speed authority in order to meet a CTA.*

Table 3: Allocate CTA Activity Description

Manage CTA Execution

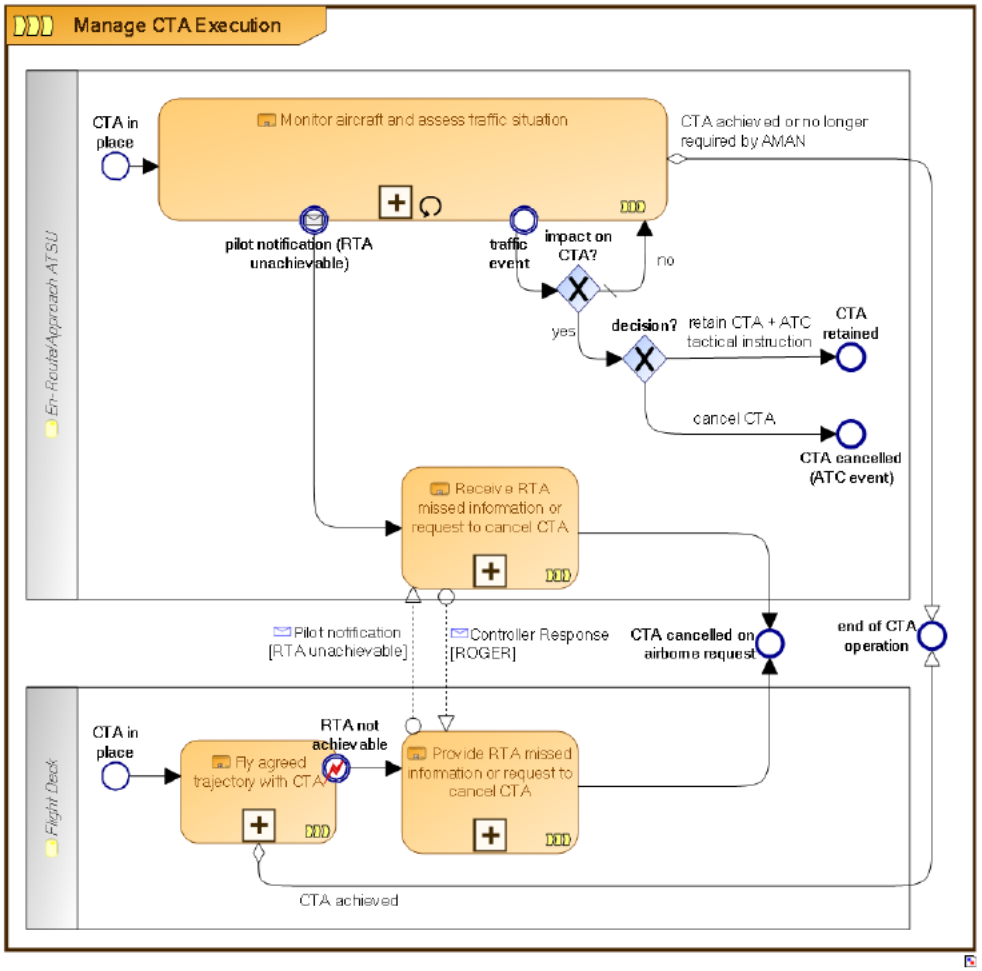

Figure 8: Manage CTA Execution Process Diagram

Activity Name	Activity Description
Monitor aircraft and assess traffic situation	The Executive Controller constantly assesses the traffic situation, monitoring all flights and reacting appropriately to any 'traffic events'.

Activity Name	Activity Description
Fly agreed trajectory with CTA	The flight crew enters a RTA and the FMS controls the aircraft to the time constraint, until the aircraft exits CTA operation and returns to standard operation.
Provide RTA missed or request to cancel CTA	The Flight Crew notifies the C-ATSU that the RTA it is not Achievable, or requests to cancel the agreed CTA.
Receive RTA missed or request to cancel CTA	The ATSU receives from the Aircraft the RTA it is not Achievable, or requests to cancel the agreed CTA.

Table 4: Allocate CTA Activity Description

Retain CTA

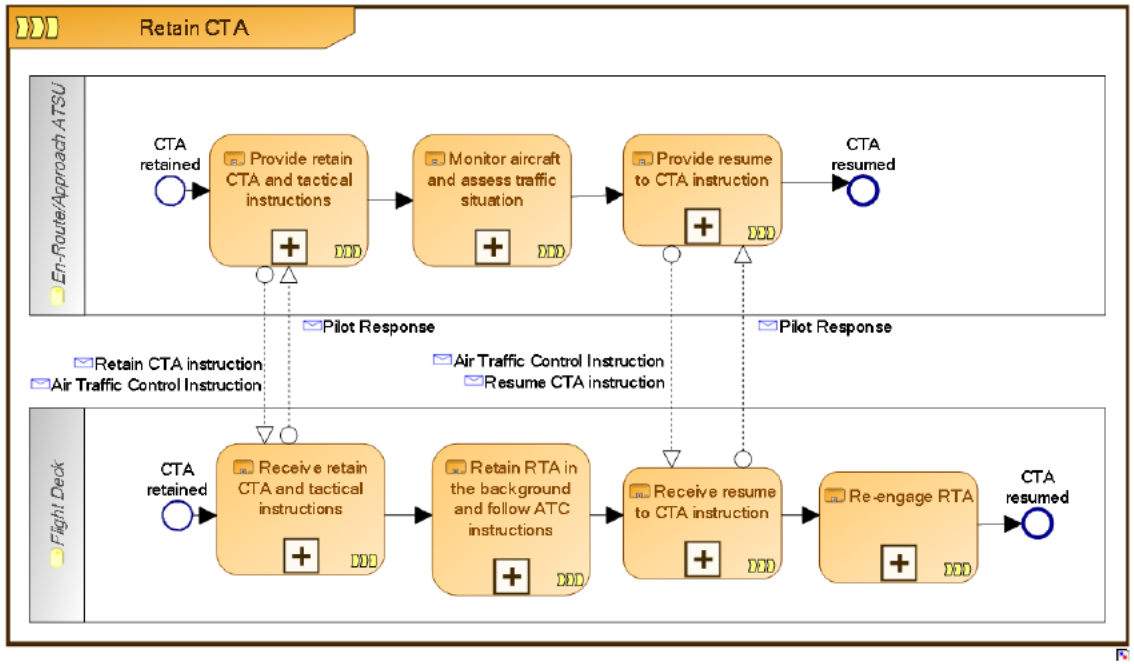

Figure 9: Retain CTA Process Diagram

Activity Name	Activity Description
Provide retain CTA and tactical instructions	The Executive Controller issues an explicit instruction to retain CTA (keep RTA in background) and also issues the required tactical instruction (e.g. heading instruction).
Receive retain CTA and tactical instructions	The flight crew receives and acknowledges explicit instructions to retain CTA (keep RTA in background) and the required tactical instruction (e.g. heading instruction).
Retain RTA in the background and follow ATC instructions	The flight crew retains the RTA (holding it in the background) and executes the ATC instruction.
Monitor aircraft and assess traffic situation	The Executive Controller constantly assesses the traffic situation, monitoring all flights and reacting appropriately to any 'traffic events'. In particular, he also decides when it is appropriate for the flight to resume normal navigation and to resume to its CTA again.
Provide resume to CTA instruction	The Executive Controller instructs the aircraft to resume own navigation and to resume to its required time constraint.
Receive resume to CTA instruction	The flight crew receives and acknowledges instructions to resume own navigation and return to CTA.
Re-engage RTA	(1) The flight crew reinstates the RTA and the FMS updates its trajectory predictions. The flight continues to its CTA. or (2) The flight crew reinstates the RTA and the FMS updates its trajectory predictions. The FMS reports RTA Missed.

Table 5: Retain CTA Activity Description

Cancel CTA

This diagram represents the process followed in order to finally cancel an already agreed CTA. Three different start events could be possible depending on who is the node that requests the cancelation.

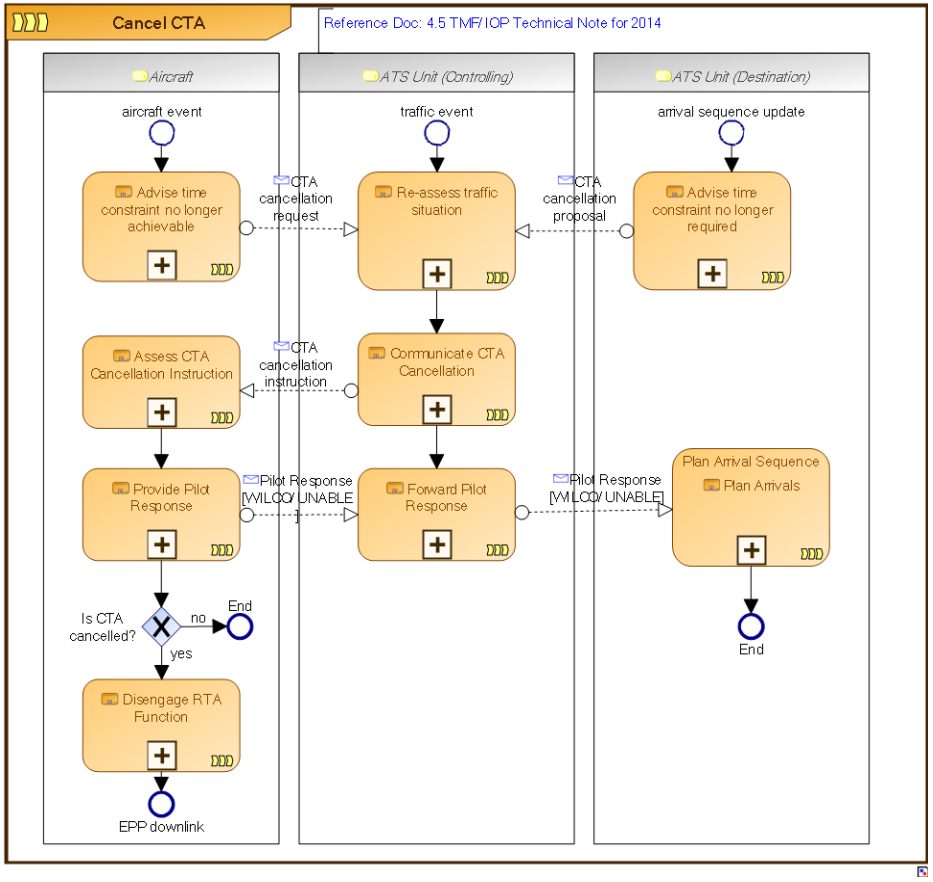

Figure 10: Cancel CTA Process Diagram

Activity Name	Activity Description
Advise time constraint no longer achievable	A/C FMS alerts the crew to a potentially Missed RTA (. E.g. the agreed CTA is considered unlikely to be achievable).
Advise time constraint no longer required	Destination ATSU assesses the sequence and the constraint is no longer needed.
Re-assess traffic situation	The Controlling ATSU, due to the evolving traffic situation, may elect to cancel the CTA.
Communicate CTA Cancellation	The Executive Controller issues an explicit instruction to the flight crew to cancel CTA.
Assess CTA Cancellation Instruction	The flight crew assess the impact of the received CTA cancel instruction
Provide Pilot Response	Flight Crew responds to the CTA Cancellation instruction from the Controlling ATSU.(Normally the flight crew would respond positively to this type of instruction)
Forward Pilot Response	The Controlling ATSU sends the aircrew response back to the Destination ATSU.
Plan Arrival Sequence	The destination ATS unit retrieves the flight crew response to the CTA Cancellation from the Flight Object and makes it available to the AMAN so that it can update the status of its plan. NOTE. Any intermediate downstream ATS units will also be made aware of the cancelled CTA through subscription to the Flight Object.
Disengage RTA Function	The flight crew disengages the RTA function in the FMS. NOTE: As a result of cancelling the CTA a new EPP may be downlinked if an ATS unit has a suitable ADS-C contract.

Table 6: Cancel CTA Activity Description

2.4 Application services, information services and systems

Used to achieve the operational services are CPDLC, ADS-C, AMAN, GROUND Data Distribution, AIRBORNE Data distribution Weather information Provision, Wind/temp info Update Provision [11].

Figure 11 shows the Application Services and Information Services dependency to Operational Processes and Services defined at OSED/DOD level.

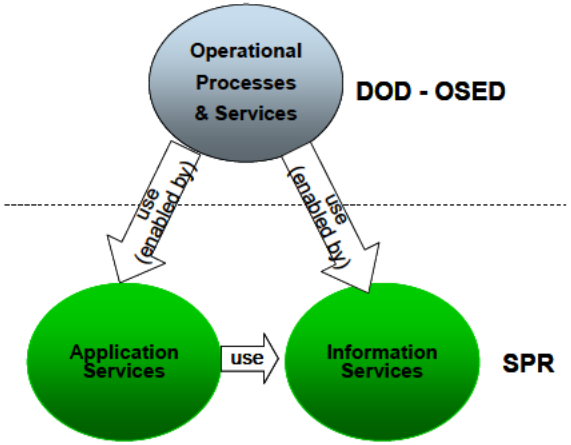

Figure 11: Application Services and Information Services dependency

2.5 Description of Operational Environment

The operating environment for CTA, including i4D, covers both en route and arrival phases of flight and, in the particular context of Project 05.06.01, this is focused on the arrival phase environment within the context of Arrival Management activities.

Assuming that CTA concept is defined to be used by aircraft operating within controlled airspace under IFR conditions, CTA operations begin in en-route controlled airspace, when the aircraft is in the cruise phase of flight, and continue into terminal airspace where the aircraft is delivered to a metering fix serving an arrival runway. In other words, the operational scenario reflects Execution Phase of flight when the aircraft comes within the destination airport's AMAN Horizon (more specifically, in the cruise phase of flight prior to Top of Descent (ToD)).

CTA operations will be explored with an i4D environment and it is therefore useful to consider the airspace characteristics of CTA operations within the context of the concept segments described in Section 2 of the reference OSED [11]:

- Segments 1-6 occur in en-route controlled airspace. The extent of this area can be defined by means of a minimum time threshold of approximately 30 minutes flying time from the CTA point. In terms of distance this equates to approximately 200nm or a few minutes (exact value to be determined) in advance of 10 minutes prior Top of Descent (ToD).
- Segment 7 concerns the modification of the trajectory and may occur in both the en-route phase of flight, as above, or during the descent to meet the CTA point at/within the TMA, as below.
- Segment 8, the end of CTA operations, occurs at the CTA point, the location of which will vary depending on the nature of the operating environment and the specific requirements of the local actors and supporting ATM processes. Typically, where i4D operations are employed to serve medium density, medium complexity nodes the metering fix is expected to be at or within TMA airspace.

It is accepted that different airspace configurations with different levels of traffic density and complexity will make use of CTA operations in different ways. It is entirely possible that some combinations of traffic density and airspace configuration will not require or enable the use of CTA at all. Therefore it can be said that CTA is most appropriate in areas of medium to high density of traffic but it is expected that CTA, within the Step 1 timeframe, will be suitable in low to medium complexity airspace [11]. In the 4.1.1.1 Section of P05.06.01 OSED [11], a list of the most significant factors contributing to TMA complexity is furnished.

As specified into the OSED [11], the following definitions are used to describe the three levels of aircraft capability:

Term	A.1 Definition
Basic CTA aircraft[3]	Aircraft equipped with CPDLC and FMS RTA functionalities of today with less accuracy than i4D/CTA-capable aircraft (RTA accuracy is +- 30s most of the times, however no guarantee is provided as to this accuracy).
I4D aircraft[4]	Aircraft equipped with CPDLC, ADS-C for communication of RTA reliable interval and EPP downlink and enhanced FMS RTA functionality, as

[3] Used interchangeably with the term, 'CTA only' aircraft; considered to be capable of basic CTA operations without i4D capabilities.
[4] Used interchangeably with the term, 'i4D CTA' aircraft; considered to be capable of advanced CTA operations using i4D capabilities.

	developed by Airbus within P09.01, with enhanced accuracy and predictability (Assurance of 95% fulfilment of CTA with +- 10 seconds accuracy).
Non-CTA aircraft[5]	Aircraft unable to participate in CTA operations (neither Basic CTA nor i4D capability).

Table 7: Aircraft Capability Definitions

The i4D service is predicated on the exchange of information between air and ground systems for the purposes of data synchronisation and for subsequent time constraint management where required.

The following tables, derived from OSED [11] paragraph 4.1.2, show the required airborne (for basic CTA aircraft and i4D aircraft) and ground capabilities necessary to implement CTA operations.

Required Airborne Capabilities for CTA Operations (Basic CTA Aircraft)
A datalink connection capability, which supports log-on and information exchanges on CPDLC.
A Controller-Pilot datalink service (CPDLC ACL) which supports: • 'Time constraint at a position' messages (with an HH:MM format), and; • ATC clearances and the corresponding operational reply.
The navigational and avionics capability of aircraft involved in CTA operations shall be, as a minimum: Legacy/current FMS functionality, to include: • Required Time of Arrival (RTA) functionality capable of achieving target within +/- 30 seconds. • P-RNAV capable.

Table 8: Required Airborne Capabilities for CTA Operations (Basic CTA Aircraft)

Required Airborne Capabilities for CTA Operations (i4D Aircraft)
A datalink connection capability, which supports log-on and information exchanges on CPDLC and ADS-C.
A system-to-system data link (ADS-C) which shall be capable to downlink: • A complete list of planned waypoints with associated altitude, ETA and speed (CAS and/or Mach number) for the waypoints, as contained within the Extended Projected Profile (EPP), and; • Reliable RTA Interval (ETA Min/Max); estimated time for one waypoint that has been identified as the metering fix by ATC.
The navigational and avionics capability of aircraft involved in i4D operations shall be, as a minimum: Enhanced FMS functionality, to include: • Required Time of Arrival (RTA) functionality capable of achieving target within +/- 10 seconds with 95% confidence. • Improved granularity and fidelity of Meteorological data.

[5] Used interchangeably with the term, 'non-capable' aircraft; considered to be non-capable of performing CTA operations.

Required Airborne Capabilities for CTA Operations (i4D Aircraft)
• Enhanced Communications functionality, to include: • Automatic Dependant Surveillance – Contract (ADS-C). Note: the number of simultaneous connections is four (4), i.e. a connection (with up to 3 contracts) with 4 separate ATSUs, simultaneously.. • P-RNAV capable.

Table 9: Required Airborne Capabilities for CTA Operations (i4D Aircraft)

Required Ground Capabilities for CTA Operations
An AMAN or other similar Arrival Management system support at the destination airport (for CTA elements).
A datalink connection capability, which supports log-on and information exchanges on CPDLC ACL and ADS-C capability, where necessary available at ATCO workstation, where for example 'Time Constraint at Position' messages may be required.
A system-to-system data link (ADS-C) which supports the required 4D trajectory information exchanges (Including ETA Min/Max) and supports trajectory negotiation.
A system capability to incorporate and make best use of received airborne trajectory information, in terms of improved trajectory prediction, improved Queue Management and improved conflict detection tools.
System support, as locally defined, to assist in the AMAN/CTA calculation and translation.
System support, as locally defined providing a trajectory 'What If' function to aid Controller assessment of impact on trajectory/traffic confliction of proposed CTA uplink.
Ground-ground coordination supporting the distribution of the relevant AMAN and CTA-related messages across systems; • Including CTA time; • CTA position; • CTA/RTA flags; • CTA cancellation etc.

Table 10: Required Ground Capabilities for CTA Operations

3 Requirements

This section collects all the safety and performance requirements derived from the assessment illustrated in Appendix A. The requirements identifiers are set according to the rules defined in the Requirements and V&V Guidelines document [2].

The generic pattern applied is as follows:

<Object type>-<Project code>-<Document code> <Document iteration code>-<Reference KPA>.<Reference number>

Where:

- **<Object type>** is REQ
- **<Project code>** is 05.06.01
- **<Document code>** is Step1 SPR
- **< Document iteration code >** is IT3 if no changes with SPR IT3 version
- **< Reference KPA >** reflects the following organization:
  - o SAF1 – Safety requirements
  - o PRF1 – Performance requirements
  - o SEC1 – Security requirements
- **<Reference number>** is a sequence number incremental by 1.

3.1 Safety Requirements

Safety requirements, coming from the assessment of section A.1, are listed below in the SJU format.

3.1.1 Segment 1 – Datalink Log-on

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0001
Requirement	Ground system of the ATSU_CONTROL shall be able to establish, for either i4D or Basic CTA aircraft, the appropriate datalink communication connections. For i4D aircraft this includes any ADS-C contract requested by the ground, either an automated request by the system for information or a specific contract request by ATCO (EXE or PLN).
Title	ATSU_CONTROL communication
Status	<Validated>
Rationale	GD-DLCOM
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG01.0300	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG01.0400	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#01	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0002
Requirement	• Ground system of the ATSU_DEST shall be able to establish, for either i4D or Basic CTA aircraft, the appropriate datalink communication connections. For i4D aircraft this includes any ADS-C contract requested by the ground, either an automated request by the system for information (e.g. AMAN) or a specific contract

	request by ATCO (EXE or PLN).
Title	ATSU_DEST communication
Status	<Validated>
Rationale	GD-DLCOM
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG01.0400	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#02	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0003
Requirement	Ground datalink communication system shall support the CPDLC necessary set of messages for CTA: • RTA instruction (Cross way point at time).
Title	Ground capability to support CPDLC messages
Status	<Validated>
Rationale	GD-DLCOM- The uplink of CROSS way point at message is done by ATSU-CONTROL using CPDLC UM252 (Uplink Message) if the aircraft is detected as i4D capable; otherwise, the basic UM51 is used. This choice is done irrelevant of whether the trajectories have been previously synchronized. This verification is the role of the CTA/CTO emitter. As per OSED 5.6.1 it3, the uplink message may include the required accuracy, and the UM260 “CROSS [position] AT [RTA time sec] AT AND MAINTAIN [level] AT [speed]” may also instruct a speed after the i4D operation.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	F&P-sR#07	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0004
Requirement	The ATC system shall be able to display on the Controller Working Position (CWP) of each relevant ATCO the appropriate aircraft capability in relation to i4D and CTA.
Title	Aircraft capability displayed on the CWP
Status	<Validated>
Rationale	GD-CWP-As the aircraft enter into the control area of an ATSU and as a consequence of log-on process (for i4D, basic CTA aircrafts) the ATCO CWP should display a/c capability
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	F&P-sR#17	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0005
Requirement	Ground System shall initiate the CPDLC communication with the i4D capable aircraft.
Title	Ground System communication with CTA aircraft
Status	<Validated>
Rationale	Even if this is baseline behaviour, this can be put as a requirement (or eventually assumption) for the i4D operation.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG01.0300	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#45	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0006
Requirement	An indication of aircraft CTA capability (i4D, basic CTA and no CTA capable aircraft) shall be presented on the ATCO CWP.
Title	A/C capability on CWP
Status	<Validated>
Rationale	In order to increase ATCO situational awareness
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG01.0400	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#66	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0007
Requirement	When appropriate, an indication of a received EPP shall be presented on the ATCO CWP.
Title	EPP info status in CWP
Status	<Validated>
Rationale	In order to increase ATCO situational awareness
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	F&P-sR#66	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG01.0400	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0008
Requirement	Controller Pilot Data Link capability required for (optional use of) exchange of CTA and associated messages (covered by mandate).
Title	Basic CTA aircraft communication
Status	<Validated>
Rationale	CTA aircraft, in order to assure CTA functions, should be able of logging-on,

	and communicating with ATSU-CONTROL.
Category	<Safety>
Validation Method	<Expert Group (Judgement Analysis)><Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG01.0100	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0009
Requirement	i4D aircraft shall be capable of logging-on, and communicating with ATSU_CONTROL, both via CPDLC V2 and ADS-C.
Title	i4D aircraft communication capability
Status	<Validated>
Rationale	I4D aircraft, in order to assure CTA functions, should be able of logging-on, and communicating with both ATSU_CONTROL and ATSU_DEST.
Category	<Safety>
Validation Method	<Real Time Simulation><Flight Trial>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG01.0100	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG01.0200	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0010
Requirement	Flight Crew shall commence datalink log-on process as soon as practical when entering a datalink area.
Title	Flight Crew establishing datalink connection
Status	<Validated>
Rationale	In order to assure CTA functions, Flight Crew should start communication with ground
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG01.0500	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

3.1.2 Segment 2 – Ground-Air 2D Route Synchronisation

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0011
Requirement	When systems are providing/utilizing i4D services, upon receipt of an EPP, the FDPS system or associated Trajectory Prediction tool shall check the consistency of the ground trajectory with the aircraft downlinked one and warn the current ATCO in case of discrepancy.
Title	Consistency check
Status	<Validated>
Rationale	Ensuring consistency between airborne and ground held trajectories is a primary driver for the i4D concept.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG02.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG02.0200	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#08	<Partial>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0012
Requirement	For i4D aircrafts, the A/C shall be able to transmit, according to ADS-C contract (periodic, on event, on demand), the EPP containing: • The “flight intent” representing the 4D trajectory as cleared by the ATC (initial filed flight plan modified by subsequent clearances and constraints – vertical 3D and time RTA – input to the FMS) • The “predicted trajectory” adding information computed by the aircraft FMS (speed and time predictions – ETAs-, trajectory change points, etc…) to build the lateral transitions and vertical profiles. • Aircraft derived parameters (gross weight, speed min/max, etc…).
Title	I4D aircraft capability to transmit EPP via ADS-C
Status	<Validated>
Rationale	To ensure the i4D operations the i4D aircrafts shall transmit all relevant information held in the FMS by means of EPP.
Category	<Safety>
Validation Method	<Real Time Simulation><Flight Trial>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG02.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#24	<Partial>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0013
Requirement	Upon detection of an inconsistency between aircraft downlinked trajectory and the FDPS trajectory, the ATCO shall take appropriate actions to correct • the ground trajectory if the ATSU was not aware of recent changes (e.g. non-receipt of a change message), • or the aircraft trajectory if there is a need to revise the last agreed trajectory.
Title	ATCO appropriate actions due to trajectory inconsistency detected
Status	<Validated>

Rationale	The ground system(s) will alert the appropriate Controller should any difference in the 2D lateral path be detected. It is expected that in most cases the trajectories held in the air and on the ground will match. However, in cases where they don't the options to the controller would include: • Accept the airborne trajectory, and alter the ground system trajectory to match the airborne one. • Take steps to bring the airborne system in line with the required ground trajectory.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	F&P-sR#40	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0014
Requirement	ATSU_CONTROL shall be able to: - detect any 2D trajectory discrepancy between the aircraft downlinked trajectory and the trajectory contained in ground FDPS, - inform the ATCO_PLN of the concerned ATSU where the first discrepancy is located, - and transmit a new 2D route to aircraft if necessary.
Title	ATSU-CONTROL systems 2D route synchronization abilities
Status	<Validated>
Rationale	Ground systems shall be able to perform all trajectory synchronization activities
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG02.0200	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG02.0300	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#61	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0015
Requirement	Upon reception of an EPP, the ATCO shall be provided with a warning when a discrepancy that exceeds an agreed value (e.g. NM, feet, seconds) exists between the aircraft trajectory (the received EPP) and the ground system trajectory (in the trajectory prediction tool, including the previously synchronized EPP).
Title	Discrepancy warning on the HMI
Status	<Validated>
Rationale	In order to increase ATCO situational awareness
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG02.0300	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#89	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0016
Requirement	ATCO shall react to a trajectory discrepancy warning in a timely manner
Title	ATCO reaction to a trajectory discrepancy
Status	<Validated>
Rationale	ATCO shall react to a trajectory discrepancy warning in a timely manner in order to assure as soon as possible the consistency between trajectories necessary for safe operations.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG02.0200	<Partial>
<SATISFIES>	<ATMS Requirement>	H-SR#20	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0017
Requirement	For basic CTA aircraft, when trajectory synchronization is not ensured automatically using EPP, ATCO shall detect trajectory discrepancy using the baseline procedure (confirm 2D route at first R/T contact).
Title	ATCO trajectory discrepancy detection for basic CTA aircrafts
Status	<Validated>
Rationale	For basic CTA aircraft, trajectory discrepancy shall be performed using baseline procedures because trajectory synchronization is not ensured automatically using EPP.
Category	<Safety>
Validation Method	<Expert Group (Judgement Analysis)>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	H-SR#21	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0023
Requirement	i4D aircraft trajectory transmissions (EPP) shall include all future waypoints and the corresponding speeds, altitudes and times to destination or at least until the constraint waypoint when a constraint has been established.
Title	EPP transmission
Status	<Validated>
Rationale	To assure the i4D operations relevant information are needed.
Category	<Safety>
Validation Method	<Real Time Simulation><Flight Trial>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG02.0100	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

3.1.3 Segment 3 – 3D Plan Uplink

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0024
Requirement	As baseline procedure, flight crew shall check the feasibility of any uplinked CPDLC instruction before answering WILCO and executing the action. This shall be applicable to any trajectory revision related to i4D operation: 2D route change, 3D vertical constraint, and CTA.
Title	Flight crew feasibility check of CPLDC instruction
Status	<Validated>
Rationale	On receipt of the CPDLC route uplink the fight crew should assess the implications of the uplinked messages on the execution flight and accept or reject it. Moreover, no vertical manoeuvre may take place without explicit clearance from the controller.
Category	<Safety>
Validation Method	<Expert Group (Judgement Analysis)>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	F&P-sR#52	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0029
Requirement	Appropriate procedures shall be defined to consider all surrounding traffic trajectories so that ATCO_PLN does not generate a conflict during resolution of air-ground trajectory discrepancy.
Title	Procedures to consider all surrounding traffic
Status	<Validated>
Rationale	Appropriate procedures are needed in order that ATCO_PLN does not generate a conflict during resolution of air-ground trajectory discrepancy with all surrounding traffic trajectories.
Category	<Safety>
Validation Method	<Expert Group (Judgement Analysis)><Real Time Simulation>
Verification Method	<Review of Design>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	H-SR#19.	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[

3.1.4 Segment 4 – Arrival Time Constraint Requirement

3.1.5 Segment 5 – Determine CTA& Request to Implement

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0037
Requirement	AMAN system shall determine the sequence and compute the CTA at the metering fix.
Title	AMAN system CTA determination
Status	<Validated>
Rationale	The precise location of the metering fix will be computed by the AMAN tool.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#12.	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0039
Requirement	Notwithstanding local arrival management considerations, the CTA Metering Fix shall be associated with a published instrument arrival route.
Title	CTA Metering Fix associated to STAR
Status	<Validated>
Rationale	CTA Metering Fix has to be associated to STAR
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0200	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#12ter	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0040
Requirement	Upon entry of an aircraft into the AMAN horizon, the ATSU_DEST shall determine automatically (or by ATCO_SEQ) the need to allocate a CTA to the aircraft.
Title	ATSU_DEST determination of the need to allocate a CTA
Status	<Validated>
Rationale	The Arrival Management position at destination should assess that a fixed time constraint is required it needs to determine the location of the CTA point and time to be applied. [11]
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0500	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0600	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#56.	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0041
Requirement	The determination of the MF shall be automated (by AMAN and/or associated system support tools) with manual overview/override possibilities.
Title	Automatic determination of the MF
Status	<Validated>
Rationale	The MF shall be determined locally based on AMAN requirements.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#57	<Partial>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0042
Requirement	Once it has been determined by the ground system that a CTA is appropriate for the flight, and that the proposed CTA time is likely to be 'viable' (taking account of aircraft prediction, ETA information when available, local implementation rules, etc.), a request for a CTA to be put in place shall be transmitted to the appropriate ATSU_CONTROL.
Title	CTA request by ATSU_CONTROL
Status	<Validated>
Rationale	The appropriate ATSU_CONTROL shall implement a CTA request once it has been determined that a CTA is appropriate for the flight
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0300	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0400	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0500	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#59	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0043
Requirement	The MF assignment shall be designed according to predefined rules .
Title	MF assignment avoiding generating conflicts
Status	<Validated>
Rationale	The location of MF varies depending on specific requirements of the operating environment.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0200	<Partial>
<SATISFIES>	<ATMS Requirement>	H-SR#15	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0044
Requirement	Ground system shall ensure that the MF used in ETA min-max request (either by human or by system) is consistent with the MF assigned to arrival procedure.
Title	MF consistency
Status	<Validated>
Rationale	MF used in ETA min-max request should be consistent with the MF assigned to arrival procedure.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0200	<Partial>
<SATISFIES>	<ATMS Requirement>	H-SR#23	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0056
Requirement	Where a CTA is to be applied, the ground unit(s) shall complete the process (CTA assigned to and agreed by the Flight Crew) 5-10 minutes prior Top of Descent.
Title	CTA process completion prior ToD
Status	<Validated>
Rationale	A desired “completion time” for CTA process was derived from discussion within P5.6.1 where it was considered appropriate in terms of the number/duration of possible ground/ground interaction. [11]
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0700	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0057
Requirement	A downstream ATSU shall provide the upstream ATSUs with any required time constraint in a time consistent with the requirement to complete the CTA allocation and agreement process 5-10 minutes prior Top of Descent.
Title	Provision of CTA to controlling ATSU
Status	<Validated>
Rationale	A desired “completion time” for CTA process was derived from discussion within P5.6.1 where it was considered appropriate in terms of the number/duration of possible ground/ground interaction.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0800	<Full>

<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

3.1.6 Segment 5a – Use of Reliable RTA in CTA Determination

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0058
Requirement	For i4D aircraft ATSU_DEST and/or ATSU_CONTROL shall check the consistency of the MF in the ETA min-max reply with respect to the selected and requested one.
Title	Ground units consistency check of the MF in the ETA min-max
Status	<Validated>
Rationale	The CTA shall only be proposed when it lies within the ETA min-max window.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05a.0500	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#04.	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0059
Requirement	For i4D service, aircraft communication system shall support the ADS-C messages in particular to get from FMS and transmit on ground request a reliable ETA min-max interval at any waypoint of the trajectory.
Title	I4D aircraft communication system to support ADS-C messages
Status	<Validated>
Rationale	An i4D aircraft communication system shall be supported by ADS-C messages in order to implement the i4D functions
Category	<Safety>
Validation Method	<Real Time Simulation><Flight Trial>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05a.0400	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#26	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0060
Requirement	When/if requested, the ATSU_CONTROL shall transmit to the aircraft an ETA Min/Max request
Title	ATCO ETA Min/Max request
Status	<Validated>
Rationale	When/if requested, the ATSU_CONTROL shall transmit to the aircraft an ETA Min/Max request
Category	<Safety>
Validation Method	<Expert Group (Judgement Analysis)>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05a.0300	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#42	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0061
Requirement	For i4D aircraft, the ground system covering the destination AMAN shall be capable of requesting ON DEMAND downlink of ETA Min/Max information at the selected CTA metering fix, and making this information available to the AMAN and other relevant system support.
Title	Requesting on demand ETA Min/Max information by ATSU_DEST system
Status	<Validated>
Rationale	It is important ON DEMAND to request to downlink ETA Min/Max information at the selected CTA metering fix, and making this information available to the AMAN and other relevant system support.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05a.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#58.	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0062
Requirement	The trajectories shall be synchronized in ATSU-DEST before setting a CTA.
Title	Trajectory synchronization completion before setting a CTA
Status	<Validated>
Rationale	The trajectories should, ideally, be synchronised to avoid unachievable CTA is being proposed, or to minimise CTAs being proposed and then cancelled/missed because of alterations to the trajectory.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05a.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#77	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0063
Requirement	When i4D service is utilized, the trajectory synchronization shall be performed before issuing an ETA min-max request in ATSU_DEST.
Title	Trajectory synchronization completion before issuing an ETA min-max request
Status	<Validated>
Rationale	The trajectories should, ideally, be synchronised to avoid unachievable CTA is being proposed, or to minimise CTAs being proposed and then cancelled/missed because of alterations to the trajectory.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05a.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	H-SR#30	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0065
Requirement	Ground systems and procedures shall ensure that the aircraft has the correct STAR prior to sending a request for ETA Min/Max.
Title	Correct STAR prior ETA Min/Max request
Status	<Validated>
Rationale	To improve the quality of CTA process that the aircraft has the correct STAR prior to sending a request for ETA Min/Max
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05a.0200	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

3.1.7 Segment 6 – Assess and Issue CTA

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0066
Requirement	ATCO_EXE CWP in ATSU_CONTROL shall be able to display the CTA requested by ATSU_DEST and also able to display any other CTA-related information required (to be determined, at a local level).
Title	CTA and related information displayed on ATCO CWP
Status	<Validated>
Rationale	ATSU_CONTROL CWP able to show the CTA to check the impact of the CTA against traffic .
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#13	<Partial>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0067
Requirement	The successive ATCOs who handle aircrafts in their sectors shall be informed that a flight is under CTA contract.
Title	Flight under CTA contract info
Status	<Validated>
Rationale	To improve ATCO situational awareness. Aircraft flying under RTA shall be displayed on ATCO CWP. Separation task shall not be impaired by: • new mental picture by the ATCO of the future behaviour of the aircraft (autonomous variations, trust in new concept/procedures, efficiency of visual scan) • reduced set of instruction that can be addressed to the aircraft • Focalisation in handling DL communications.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0400	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#15	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0068
Requirement	The ATCO shall be aware that a CTA is being negotiated.
Title	CTA negotiated status info
Status	<Validated>
Rationale	Improve ATCO awareness of potential impact of modifying the trajectory of an aircraft which is under CTA/CTO negotiation.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0500	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#16	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0069
Requirement	The ATC system shall be able to display on demand the vertical profile of an a/c trajectory.
Title	Vertical profile displayed on ATC system
Status	<Validated>
Rationale	To improve ATCO situational awareness
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#18	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0072
Requirement	Aircraft systems shall detect if the MF in the ETA min-max request is not on the trajectory. After detection aircraft automatically reject at message reception.
Title	Aircraft systems detection of MF out of trajectory and alert to the crew
Status	<In Progress>
Rationale	Flight Crew shall be informed if the MF is out the trajectory
Category	<Safety>
Validation Method	<Expert Group (Judgement Analysis)>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0300	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0200	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#27	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0073
Requirement	The ATCOs handling (and/or receiving) a CTA flight shall evaluate the impact of the CTA on traffic, sector complexity and conflict resolution as part of their routine operation. In this, they may be supported by automation.
Title	ATCOs evaluation of CTA impact
Status	<Validated>
Rationale	The ATCO shall assess the impact of CTA on her/his traffic situation before issue it to the flight.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance

<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#44	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0074
Requirement	Before accepting too many CTA, ATCO shall evaluate the impact of potential multiple cancellations (in case of failure or large unexpected atmospheric disturbance) and keep margins on his/her workload as well as frequency congestion if many ATC instructions have to be transmitted.
Title	ATCO evaluation of the impact of potential multiple cancellations
Status	<Validated>
Rationale	The ATCO shall assess the impact of CTA on her/his traffic situation before issue it to the flight.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#44bis	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0075
Requirement	ATSU_CONTROL shall inform ATSU_DEST if the CTA is not accepted: • because the ATCO is unable to implement the CTA,, • or because crew is unable to meet the CTA (thus responding UNABLE).
Title	CTA status information between ATSUs
Status	<Validated>
Rationale	ATSU_CONTROL shall inform ATSU_DEST if the CTA is not accepted because it shall be aware of its incoming traffic situation.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0500	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0600	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#48	<Partial>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0076
Requirement	Indication of CTA status shall be presented to all concerned ATCO.
Title	CTA status information presented to ATCOs
Status	<Validated>
Rationale	Controllers shall be informed if the CTA is or not accepted because they shall be aware of traffic situation.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0500	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0600	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#68	<Full>

<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0079
Requirement	Criteria for workload conditions shall be defined to enable the ATCO_EXE to perform an adequate CTA impact assessment on his sector.
Title	Workload conditions in CTA impact assessment
Status	<Validated>
Rationale	Workload conditions has to be considered to make the controller able to perform an adequate CTA impact assessment on his sector
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	H-SR#05	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0081
Requirement	Mitigations shall be defined to prevent ATCO_EXE omission to transmit the CTA.
Title	Mitigations against CTA transmission omission
Status	<Validated>
Rationale	ATCO EXE shall be able to transmit the CTA.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	H-SR#10.	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0082
Requirement	The input of RTA into FMS by pilot shall be supported by automation
Title	RTA input into FMS
Status	<In Progress>
Rationale	RTA input into FMS by pilot shall be supported by automation in order to reduce pilot workload.
Category	<Safety>
Validation Method	<Expert Group (Judgement Analysis)><Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	H-SR#13.	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0083
Requirement	The EPP consistency check by the ground system shall include the verification that the RTA transmitted to the aircraft is included in the EPP.

Title	RTA info in EPP check
Status	<Validated>
Rationale	To assure information completeness ground system shall check that the RTA transmitted to the aircraft is included in the EPP
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	H-SR#24	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0084
Requirement	The CTA impact assessment by ATCO shall be supported by a tool.
Title	Tool to support CTA impact assessment
Status	<Validated>
Rationale	The CTA impact assessment by ATCO shall be supported by a tool in order to make his/her work more easy and secure.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	H-SR#28	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0085
Requirement	En-Route ATSU shall inform ATSU_DEST that a CTA has been set.
Title	CTA status info
Status	<Validated>
Rationale	ATSU_DEST shall be aware that a CTA has been set or not in order to have clarity of its incoming traffic. ***Note:*** *Informing the ASTU_DEST may be either explicit ("I will tell you") or implicit (e.g. "I will tell you only if there is a problem, otherwise assume all is OK"), as determined by local agreement.*
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0500	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0600	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-10.02.01-TS-0005.0040	<Partial>
<SATISFIES>	<ATMS Requirement>	H-SR#31	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0089
Requirement	The ground system shall enable the controlling ATCO to uplink a CTA and its associated Metering Fix to the aircraft or they can be communicated by voice.

Title	Capability to uplink the CTA
Status	<Validated>
Rationale	The controller should have the possibility to communicate the CTA either by voice or by ground system means.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0200	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0090
Requirement	Ground systems and procedures shall ensure that the Standard Instrument Arrival Route (STAR) has been uploaded to the aircraft, prior to sending a proposed CTA.
Title	Uploaded STAR prior CTA proposal
Status	<Validated>
Rationale	The Standard Instrument Arrival Route shall be uploaded to the aircraft prior to sending a proposed CTA.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG06.0300	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

3.1.8 Segment 7 – CTA Execution and Monitoring

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0091
Requirement	The Air and Ground systems shall provide real time monitoring of the flight's potential divergence from the accepted time constraint including alerting functions in case of non-conformance.
Title	Real time flight monitoring
Status	<Validated>
Rationale	Flight crew and pilot shall be aware of situation under their control.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG07.0200	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG07.0300	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#09	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0092
Requirement	For each a/c performing a CTA, the ATC system shall be able to display the predicted ground speed values of the a/c over waypoints from the a/c current position to the Metering Fix (CTA point) derived from EPP or from the ATC ground system trajectory.
Title	Ground speed information
Status	<Validated>
Rationale	ATC system should be able to display the ground speed values of the a/c over waypoints from the a/c current position to the Metering Fix (CTA point) in order to increase ATCO situational awareness.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	F&P-sR#20	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0093
Requirement	Each controller (En-Route and TMA, PLN or EXE) shall be able to display AMAN advisory (including as a minimum the assigned CTA and the metering fix) on the radar display.
Title	AMAN advisory
Status	<Validated>
Rationale	Controllers should be able to display AMAN advisory (including as a minimum the assigned CTA and the metering fix) on the radar display in order to increase their situational awareness
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	F&P-sR#21	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0094
Requirement	Each TMA controller (PLN or EXE) HMI shall display the sequence at Metering Fixes.
Title	Sequence at Metering Fixes
Status	<Validated>
Rationale	Increase their situational awareness
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	F&P-sR#22	<Partial>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0096
Requirement	Requests for EPP downlink shall be made as/when appropriate (On demand contract, for trajectory revision or in the event of a predicted time non conformance), in order for all actors to be informed via EPP downlink.
Title	Requests for EPP downlink
Status	<Validated>
Rationale	In order for all actors to be informed via EPP downlink
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG07.0400	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#39.	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0100
Requirement	The ATCO_PLN CWP of en-route ATSU shall issue an indication to warn the controller that CTA is likely not to be met by an aircraft. Upon receipt of this indication, the controller gets prepared to receive via voice information from the crew and anticipate a recovery strategy (return to baseline operations for this flight) or without or with cancellation of the CTA.
Title	ATCO_PLN CWP CTA missed indication
Status	<Validated>
Rationale	The ATCO shall be aware of the situation under her/his control
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG07.0200	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG07.0300	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#86	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0101
Requirement	In the event of a predicted time constraint non-conformance given by the crew, the ATSUs responsible for the airspace containing the constraint points shall be warned in a timely manner.
Title	ATSU CTA non-conformance indication
Status	<Validated>
Rationale	The ATSUs shall be aware of predicted time constraint non-conformance
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG07.0300	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#95	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0102
Requirement	In case of vectoring while RTA is active, the pilot follows the vectoring instruction (as normal procedure that gives priority to the last received clearance).
Title	Vectoring instruction prioritization
Status	<Validated>
Rationale	The pilot has to give prioritization to vectoring instruction.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Inspection>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	F&P-sR#98a	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

3.1.9 Segment 7a – Downlink Modified Trajectory

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0111
Requirement	ATSU_DEST (ATCO of arrival sector) shall inform ATSU_CONTROL (current ATCO) of any change in the arrival STAR and request a route change to be sent to aircraft.
Title	Change in the arrival STAR
Status	<Validated>
Rationale	ATSUs should be aware of the situation
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-10.02.01-TS-0005.0080	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#38	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0112
Requirement	ATCO shall be informed of the next EPP received after issuing a trajectory revision. The EPP information may be used to see if the received trajectory reflects the last clearance.
Title	Next EPP received after trajectory revision
Status	<Validated>
Rationale	Since the downlinked EPP may be de-correlated from the FMS trajectory, it is important that the ATSU_CONTROL filters the received EPP to discard the out of date ones. But the ATSU_CONTROL must make a distinction between an out of date trajectory and an “update of trajectory”. Therefore, some criteria have to be defined for this filtering (rejection/discarding). It is suggested that any downlinked trajectory be checked against the last clearance. E.g. contains the WPTs of the last route clearance, or the RTA at MP corresponds to the CTA etc. It can also be recommended to use on event contracts and a tighter synchronization of the FMS and downlinked trajectory. The selection of the type of ADS-C contract is an automated process.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-10.02.01-TS-0001.0040	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-10.02.01-TS-0001.0050	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#46	<Partial>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

3.1.10 Segment 8 – Standard Operations

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0113
Requirement	CTA operations shall end when the aircraft sequences the MF.
Title	End of CTA operation
Status	<Validated>
Rationale	As per definition CTA operations will end when the aircraft sequences the MF.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG08.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#31	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0114
Requirement	Upon the aircraft passing a CTA fix located 'in cruise', or upon the cancellation of a CTA while the aircraft is still in the cruise phase (irrespective of whether CTA is located in cruise or in descent), the aircraft shall return to 'normal' operating speed, unless otherwise instructed by ATC.
Title	Speed after CTA operations end, in en-route
Status	<Validated>
Rationale	Speed after CTA operations end (upon the aircraft passing the CTA fix or upon the cancellation of the CTA) has to be considered for safety reasons.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG08.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#33	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0115
Requirement	Upon the aircraft passing the CTA fix in the TMA, or upon the cancellation of the CTA when the aircraft is already in descent, the aircraft shall maintain the last speed required to meet the CTA, unless otherwise instructed by ATC.
Title	Speed after CTA operations end
Status	<Validated>
Rationale	Speed after CTA operations end (upon the aircraft passing the CTA fix in the TMA or upon the cancellation of the CTA) has to be considered for safety reasons.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG08.0100	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#33	<Partial>

<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0116
Requirement	When the CTA is cancelled while the aircraft is still en-route, the ATSU_CONTROL shall inform the ATSU_DEST.
Title	ATSU_DEST awareness of CTA cancelled
Status	<Validated>
Rationale	ATSU_DEST should be informed about its incoming traffic.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG08.0300	<Partial>
<SATISFIES>	<ATMS Requirement>	F&P-sR#94	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0117
Requirement	Air/Ground Communication by voice shall be used to clarify the situation in case of cancellation of RTA (by crew or by controllers)
Title	Voice communication in case of RTA cancellation
Status	<Validated>
Rationale	In case of RTA cancellation voice communication are necessary
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	F&P-sR#97	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

3.1.11 All Segments

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0118
Requirement	ATCO and Flight Crew HMIs shall be designed in order to minimize their potential contribution to human error.
Title	ATCO and Flight Crew HMIs design
Status	<Validated>
Rationale	ATCO and Flight Crew HMIs shall be designed as usable as possible in order to maximize human performances and reduce workload.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	F&P-sR#14.	<Partial>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0120
Requirement	The tactical planners (ATCO_PLN) shall identify in time developing planning conflicts induced by CTA and resolve potential conflicts before they occur. (Potential use of MTCD in ATSU_CONTROL.)
Title	ATCO_PLN planning conflicts identification
Status	<Validated>
Rationale	ATCO_PLN should prevent potential conflict and plan actions accordingly in order to avoid conflict to take place.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	F&P-sR#43	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0121
Requirement	The ATCO_EXE shall monitor the adherence of the aircraft to the established trajectory contract. This includes • lateral and vertical path, • ground estimation of ETA, • monitoring of the downlinked “CTA not reliable” flag.
Title	ATCO EXE monitoring of established trajectory contract
Status	<Validated>
Rationale	ATCO_EXE monitoring of established trajectory contract is important in order to assure situational awareness and automation may help the ATCO_EXE in this task (identification of aircraft under CTA, distance to expected position, alerts).
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance

<SATISFIES>	<ATMS Requirement>	F&P-sR#82	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0122
Requirement	ATCO shall adapt in time, whenever necessary, the conflict resolution strategy that was initially built to allow CTA satisfaction (impact on separation task)
Title	ATCO timely conflict resolution to allow CTA satisfaction
Status	<Validated>
Rationale	ATCO should adapt in time the conflict resolution strategy to allow CTA satisfaction but considering impact on separation task
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	F&P-sR#83	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0123
Requirement	Communication by voice shall be used to clarify the situation in case of rejection (by aircraft) of a CTA proposed via voice by the ATCo.
Title	Voice communication in case of CTA rejection
Status	<Validated>
Rationale	To ensure consistency in communication means used for controller/pilots communications.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	F&P-sR#98	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0125
Requirement	ATCOs coordination shall include procedures to cope with a situation when multiple simultaneous cancellations occur (e.g. unexpected adverse weather).
Title	ATCOs coordination procedures in case of multiple simultaneous cancellations
Status	<Validated>
Rationale	ATCOs coordination procedures should cover all possible aspect in order to make them “trained” about any possible situation.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Review of Design>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	H-SR#14	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0126
Requirement	ATCOs shall resolve tactical conflict without making any differentiating aircraft flying under CTA or not.
Title	Tactical conflict resolution without CTA prioritization
Status	<Validated>
Rationale	Tactical conflict resolution has to be performed without any attention to CTA prioritization assuring safety.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	H-SR#16	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SAF1.0127
Requirement	Conflict resolution shall be supported by a ground system tool in order not to generate another conflict.
Title	Toll support for conflict resolution
Status	<Validated>
Rationale	Tool support is necessary for conflict resolution in order to improve controller's situational awareness and support her/him in decisions.
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-10.02.01-TS-0002.0500	<Partial>
<SATISFIES>	<ATMS Requirement>	H-SR#27	<Full>
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

3.2 Performance Requirements

Here below are presented Performance Requirements for Predictability and Environment KPAs coming from the Operational Performance Assessment presented into Appendix A.4.

Predictability and Environment Requirements

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-PRF1.0001
Requirement	The ground system shall provide an alert to advise ATCO in case of a failure in CTA calculation function.
Title	CTA calculation function failure alert
Status	<Validated>
Rationale	Predictability may decrease and fuel burn increase because CTA not available for any new aircraft coming into the sequence
Category	<Performance>
Validation Method	<Expert Group (Judgement Analysis)>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-PRF1.0002
Requirement	In case of a failure in ground CTA calculation function, new aircrafts arriving into the sequence shall be handled by applying regular AMAN advisories (e.g. TTL/TTG).
Title	Regular AMAN advisories
Status	<Validated>
Rationale	Predictability may decrease and fuel burn increase because CTA not available for any new aircraft coming into the sequence. The A/C is handled as efficiently as possible using standard AMAN advisories
Category	<Performance>
Validation Method	<Expert Group (Judgement Analysis)>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-PRF1.0003
Requirement	In case of a failure in ground CTA calculation function, those aircraft already operating to a CTA shall continue to operate with the CTA.
Title	CTA standard procedures
Status	<Validated>
Rationale	The loss of the function eill nott affect those A/C already issued with CTA
Category	<Performance>
Validation Method	<Expert Group (Judgement Analysis)>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-PRF1.0004

Requirement	The ground system, taking into account aircraft capability, shall only propose CTA which is achievable.
Title	Propose only achievable CTA
Status	<Validated>
Rationale	Predictability may decrease and fuel burn increase: for one a/c minimum impact- if all a/c affected higher impact
Category	<Performance>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG05.0300	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-10.02.01-TS-0001.0010	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-PRF1.0006
Requirement	The air and ground system shall monitor the achievability of the agreed CTA.
Title	CTA monitoring functions
Status	<Validated>
Rationale	Predictability may decrease and fuel burn increase with achievability monitoring lack: for one a/c minimum impact- if several a/c affected higher impact
Category	<Performance>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG07.0200	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-10.02.01-TS-0005.0230	<Partial>
<SATISFIES>	<ATMS Requirement>	REQ-10.02.01-TS-0006.0430	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-PRF1.0007
Requirement	The air and ground HMI shall display alerts in case the agreed CTA is not respected.
Title	CTA not respected HMI alert
Status	<Validated>
Rationale	HMI performances need, in order to support CTA related eventual alerts.
Category	<Performance>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG07.0300	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-PRF1.0008
Requirement	In case an i4D-aircraft does not respect an agreed CTA, it shall provide an updated EPP depending on the type of contract established by ATC.
Title	EPP updating for no respected CTA
Status	<Validated>
Rationale	Predictability may decrease: for one a/c minimum impact - if several a/c

	affected higher impact
Category	<Performance>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.01-OSED-SG07.0400	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-10.02.01-TS-0004.0460	<Partial>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[

3.3 Security Requirements

Here below it is possible to find security requirements that come from the assessment done in section A.2.

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SEC1.0001
Requirement	The ground systems should assure security controls in order to prevent an attacker to modify the integrity of data transmitted.
Title	Ground systems integrity of data
Status	<Validated>
Rationale	The ground system should prevent an attacker to modify the integrity of data transmitted.
Category	<Security>
Validation Method	<Expert Group (Judgement Analysis)>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SEC1.0002
Requirement	The ground systems should assure security controls in order to prevent an attacker to transmit false alerts, clearances to aircrafts.
Title	Erroneous false alerts and clearances preventions
Status	<Validated>
Rationale	The ground system should prevent an attacker to transmit.
Category	<Security>
Validation Method	<Expert Group (Judgement Analysis)>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SEC1.0003
Requirement	The on-board systems should assure security controls in order to prevent an attacker to modify the integrity of data transmitted.
Title	On-board systems integrity of data
Status	<Validated>
Rationale	The on board system should prevent an attacker to modify the integrity of data transmitted
Category	<Security>
Validation Method	<Expert Group (Judgement Analysis)>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.06.01-Step 1SPR IT3-SEC1.0004
Requirement	The on-board systems should assure security controls in order to prevent an attacker to modify downlink messages to trigger unneeded alarms or alert procedures.

Title	Erroneous downlinked messages preventions
Status	<Validated>
Rationale	The on board system should prevent an attacker to modify downlink messages
Category	<Security>
Validation Method	<Expert Group (Judgement Analysis)>
Verification Method	<Test>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

3.4 Information Exchange Requirements (IER)

For more details on Information Exchange Requirements (IER) and associated usage rules the reader is advised to consult the P5.6.4/P5.6.7 documentation since in OSED [62] [63] these Information Exchange Requirements are provided.

4 References and Applicable Documents

4.1 Applicable Documents

[1] Template Toolbox 03.00.00
https://extranet.sesarju.eu/Programme%20Library/SESAR%20Template%20Toolbox.dot

[2] Requirements and V&V Guidelines 03.00.00
https://extranet.sesarju.eu/Programme%20Library/Requirements%20and%20VV%20Guidelines.doc

[3] Templates and Toolbox User Manual 03.00.00
https://extranet.sesarju.eu/Programme%20Library/Forms/Templates.aspx

[4] EUROCONTROL ATM Lexicon
https://extranet.eurocontrol.int/http://atmlexicon.eurocontrol.int/en/index.php/SESAR

4.2 Reference Documents

[5] ED-78A GUIDELINES FOR APPROVAL OF THE PROVISION AND USE OF AIR TRAFFIC SERVICES SUPPORTED BY DATA COMMUNICATIONS.[6]

[6] SESAR B4.1_D39_Updated_Perf_Validation_Targets_S1_S2_V01.00.00_20130621

[7] B.4.3 D95 Architecture Description Document Step 1 V.00.02.02 (2014 edition)

[8] SESAR Safety Reference Material
https://extranet.sesarju.eu/Programme%20Library/Forms/Procedures%20and%20Guidelines.aspx

[9] SESAR Security Reference Material
https://extranet.sesarju.eu/Programme%20Library/Forms/Procedures%20and%20Guidelines.aspx

[10] SESAR Environment Reference Material
https://extranet.sesarju.eu/Programme%20Library/Forms/Procedures%20and%20Guidelines.aspx

[11] SESAR P5.6.1 Ground and Airborne Capabilities to Implement Sequence, 050601-Step 1-Fully Validated OSED, 00.01.00, 13-07-2016

[12] SESAR WP5 TMA Step 1 Detailed Operational Description, D101, 00.01.03, 22-06-2012.

[13] SESAR WP5 Validation Strategy for Concept Step 1 – Time Based Operations, July 2011

[14] SESAR P4.5 Trajectory Management Framework Initial Step 1 Technical Note, D101, 00.01.00, 24-05-2012.

[15] SESAR P5.7.2 i4D in TMA, Impact on Separation Management – Initial Assessment, 00.01.00.

[16] SESAR Operational Focus Area, Programme Guidance, Version 03.00.00, 04-05-2012.

[17] European Air Traffic Management Programme, Initial 4D – 4D Trajectory Data Link (4DTRAD) Concept of Operations, 01-12-2008.

[18] SESAR B4.2 Actors – Roles & Responsibilities, 00.01.05, May 2011.

[19] SESAR B4.2 Initial Transition ConOps Edition 2015.

[20] CASSIS II Extended Concept of Operations of CTA Applications, Version 1.00, 08-12-2009.

[21] AIR NAVIGATION SYSTEM SAFETY ASSESSMENT METHODOLOGY, Ed. 2.0, ref. AF.ET1.ST03.1000-MAN-01, 30 April 2004

[6] *The EUROCAE ED-78A has been used as an initial guidance material. ED-78A is useful, but is not an applicable document, because it mostly addresses the V4-V5 phases, whilst the SESAR R&D programme is focussed on development (V1-V2-V3, and because of its partial compliance with safety regulatory requirements).*

[22]WPB.01 Integrated Roadmap Latest version (DS 15)

[23]WP WG85 ETA MIN MAX window computation-i1EUROCAE

[24]P16.6.1 - i4D+CTA (OFA04.01.05) Safety Assessment Report (SAR)- Iteration 3 - Edition 00.01.00

[25]EXE-05.06.01-VP-207 - Validation Report, D66, Edition 00.02.01

[26]P 04.03 i4D+CTA OSED & Requirements Iteration 1 D12 - Part 3 INTEROP ED 00.01.00

[27]WG78 - SPR – H – Annex A OSA Approach (Input for Validation) - 3 February 2010

[28]Validation Target Allocation for Step 1-Version 00.02.01-D10

[29] Guidance to Apply the SESAR Safety Reference Material- D06-002- Edition 00.01.02

[30] SESAR ATM Security Reference Material - Level 1- Deliverable 16.06.02 D06- Version 02.00.01- Edition 00.02.00

[31] SESAR ATM Security Risk Assessment Method – P16.02.03 - D02- Edition 00.01.01

[32] ISO/IEC 27005:2008, Information technology – Security techniques – Information security risk management

[33] EXE-05.06.01-VP-278 Validation Plan- D70- Edition 00.02.01 – Template Version 03.00.00

[34] EXE-05.06.01-VP-278 Validation Report – D71- Edition 00.02.01 – Template Version 03.00.00

[35] EXE-05.06.01-VP204 Validation Plan - D061- Edition 00.03.01 – Template Version 02.00.00

[36] EXE-05.06.01-VP204 - Final Report- D62- Edition 00.02.01 – Template Version 03.00.00

[37] EXE-05.06.01-VP-326 Validation Plan - D079- Edition 00.02.01 – Template Version 03.00.00

[38] EXE-05.06.01-VP-326 Validation Report- D80- Edition 00.01.00 – Template Version 03.00.00

[39] P5.6.1 Step 1 SPR – Iteration 2- D68 – Edition 00.02.01

[40] P5.6.1 Step 1 SPR – Iteration 3 - M196 – Edition 00.01.00

[41]Description of the Methodology for Step 1 Performance Assessment - Edition 00.01.00- SESAR Project ID B.05.0

[42] SESAR- Safety and Performance Requirements (SPR) Template – Version 03.00.00

[43] P16.6.2 OFA 04.01.05 Security Risk Assessment - Edition 00.00.02 – 24/10/2013.

[44]WP5 Validation Strategy for Concept Step 1 - Time Based Operations, Deliverable ID: D51, Edition: 00.00.05, 2012-12-10.

[45]DEL05.02-M314 - Step 1 DOD Report - Second Release Milestone, Milestone ID 314, Edition 00.01.03

[46]B41 DS10 Re-aligned Validation Targets - 20130913 V2

[47]Guidance on list of Key Performance Indicators for Step 1 Performance Assessment, Edition 00.01.00, 2011-09-30.

[48]P05.06.01_Benefit Mechanisms_00.02.00

[49]SESAR - The Performance Target - D2

[50]16.06.02_D06_ATMSecReferenceMaterial.00.01.00

[51]MSSC – WP 16.02.05 Minimum Set of Security Controls (not yet available at end of 2012)

[52]EUROCONTROL ATM Security Risk Management Toolkit – Guidance material v1.0

[53]ISO/IEC 27005:2008, Information technology – Security techniques – Information security risk management

[54]Security Registers – Work In Progress -https://extranet.sesarju.eu/WP_16/Project_16.06.02

[55]16.02.03 SecRAM and SecRAM Implementation Guidance Material

[56]P16.6.2 OFA 04.01.02 i4D + CTA Security Risk Assessment Report (SecRAR) - Edition 00.00.03– 14/04/2016

[57]SESAR P5.5.1 TMA Trajectory Management Framework Advanced OSED, D09, 00.01.00, 15-08-2011

[58]SESAR P5.6.1 EXE-477 Validation Plan (VALP), D100, 00.03.00, 04-12-2015

[59]SESAR P5.6.1 EXE-477 Validation Report (VALR), D101, 00.03.00, 28-04-2016

[60]SESAR P5.3 EXE-805 Validation Report (VALR), D101, 00.00.04, 13-04-2016

[61]WP10.01.07-D120 -Technical Architecture Description - Cycle 2015

[62]P05.06.04 - D35 Consolidated OSED 02.00.00

[63]P05.06.07 DEL-05 06 07 - D15-Update of 5 6 4 OSED-Step 1

[64] Security Risk Assessment of OFA 04.01.02 SAR Enhanced Arrival & Departure Management in TMA and En Route – Edition 00.00.04 – 25/09/2015

Appendix A Assessment / Justifications

A.1 Safety Assessment

This section provides an overview of all main activities executed to perform the safety assessment used in order to derive the safety requirements listed in Section 3.1.

First of all, it is important to point out that a coordination with OFA i4D + CTA Safety Plan working group was established to perform a preliminary deep screening at project level with the aim of identifying the potential safety impacts concerned with the introduction of the i4D and CTA operations. Preliminary safety assessment was entirely carried out by ENAV due to the amount of effort. Several workshops have been arranged by the OFA i4D & CTA Safety Plan working group with involvement of the P16.6.1, P4.3, P5.6.1 and WG 78 technical and operational experts. The Primary Projects support has been provided for each step of the process from the definition of safety objectives, the identification operational hazards to the definition of Safety Requirements.

One of the first outcomes resulted from that coordination was the elaboration of a proper Operational focus Area Safety Assessment Report (OFA SAR iteration 3) [24] which has received the contribution from P5.6.1 in order to carry out a complete safety assessment analysing the impact of CTA functions on TMA environment and so derive the safety requirements that fulfil P5.6.1 needs.

The idea to join a collaboration with P16.6.1 OFA 4.1.5 Safety Assessment team and to take into account SAR Iteration 3 [24] as reference was been made in order to avoid an overlap of work made at project and OFA level and to be aligned and consistent with the entire Safety Assessment outcomes. Of course, P05.06.01 Step 1 - Fully Validated SPRtakes into account that assessment and details its own in order to cover all P5.6.1 targets (i.e. Step1 TMA scenario aims).

Since the SESAR Safety Reference Material (SRM) [8] provided by P16.06.01 is much broader than SAM [21] or ED78A [5] which are concerned only with failure of the System and not with what the system is required to do in the first place (i.e. its functionality and performance), as done by SAR the safety assessment conduced in this context follows the SRM [8] guidelines. It is important to note that The SESAR SRM does not replace the EUROCONTROL SAM, rather it:

- puts the SAM in into an argument framework, and
- adds a success approach to show whether the concept is intrinsically safe in the absence of failure.

The whole safety assessment process conducted in this context, covers both success and failure viewpoints:

- **Success approach** seeks to assess the achieved level of safety when the system is working as intend (i.e. in absence of failure) referring only to the pre-existing hazards which by definition exist in the operational environment before any form of deconfliction has taken place. It means that the pre-existing hazards are not caused by the system but they are those expected to be eliminated or, at least, mitigated by introducing the system. The success approach is concerned with the positive contribution to aviation safety that the ATM operational services make in the absence of failure of the end-to-end ATM System. In other words, this first step aims at identifying the benefits which should be provided by the system under normal and abnormal conditions of the Operational Environment (Functionality & Performance). This study is linked to what we WANT the system to do in all possible conditions it is designed to live. In our case, the system refers to the CTA operations.
- **Failure approach** seeks to assess the achieved level of safety in the event of failure and is related to system generated hazards. The failure approach is concerned with the negative

contribution to the risk of an accident that the ATM operational services might make in the event of failure of the end-to-end ATM System, however caused (Integrity/Reliability). This assessment is related to what we DO NOT WANT the system to do.

Since the aggregate of the success and failure contributions needs to be at the very least neutral to demonstrate that safety will not deteriorate, it means that not only the failure approach would be incomplete without the complementary success approach but it is also dependent on it - in other words, we cannot define failure until we have fully defined success.

To be noted that the safety assessment performed into the SPR Iteration 2 [39] was limited to the conventional failure approach as per the ED-78A document. For Iteration 3, the safety assessment methodology has been enlarged in order to combine both the former methodology and the broader safety approach developed within the SESAR context.

Being that, the Safety Requirements for CTA operations, showed in section 3.1, have been derived considering the mentioned Operational Safety Assessment methodology. Please find in sections below, the work of activities performed by the collaboration of P16.6.1 and P5.6.1 for OFA i4D+CTA SAR- Iteration 3 [24] and refer to it for further details.

A.2.1 Success Approach

Comprehensive determination of the operational services that are provided by OFA 04.01.05 "i4D+CTA" to address the relevant pre-existing hazards and derivation of Safety Objectives (success approach) in order to mitigate the pre-existing risks under normal operational conditions according to SRM.

The pre-existing hazard individuated as in scope of P5.6.1 is:

Pre-existing Hazard	Name
Hp#1	**Conflicts between pairs of trajectories**

Table 11: Pre-existing Hazard

The first step in identifying Safety Objectives is to split the Operational Services per phase of flight, and analyse what service is provided to mitigate the pre-existing hazard. This consists in identifying what element of the AIM barrier model (Appendix C) is improved by which functionality.

The Operational Services, useful to mitigate the individuated pre-existing hazard are:

- TCA - Trajectory Consistency and Adherence (Synchronization) because it ensures all actors on ground and airspace users share the same agreed trajectory, and when appropriate, exchange additional elements (e.g. vertical profile, ETAs) to support the optimisation of operations. This service is a prerequisite for the two next ones.
- SEQ- Arrival Traffic Sequencing because it improves the arrival queue management by a pre-sequencing of aircraft at a Metering Fix in approach. (For CTO only)
- DCB- Sector Demand & Capacity Balancing because, thanks to the CTO, it is considered an enabler improving the sequencing at the border of an airspace (more efficient management of sector demand and capacity balancing). (For CTO only)
- SEP- Traffic separation because it shall be delivered with the same quality as today ensuring the separation minima to avoid collision.

Moreover, in order to "derive" F&P-SO is has been necessary to collect also information from the description given in the OSED [11] by the analysis of typical flight.

The Success Approach aims to individuate the Functionality & Performance Safety Requirements taking into account also normal and abnormal conditions:

- A *normal condition* refers to i4D+CTA operations as described in the concept in the most typical and frequent cases.
- An abnormal condition refers to an i4D+CTA operation that is cancelled (discrepancies not resolved, meteorological conditions leading to RTA not met...). Some of the abnormal conditions happen when the negotiation process (normal condition) finished without agreement.

  Essentially, these conditions can be grouped into 4 categories:

  - Inability to synchronize trajectory,
  - RTA not met (including unpredicted adverse weather encounter: strong wind and CBs),
  - Cancellation for separation needs
  - Need to first change the route in order to meet the sequence (required delay to fit sequence not in aircraft ETA min-max window, given the current route).

Starting from the work performed in conjunction with OFA 04.01.05 SAR team, a completed list of F&P Safety Objectives have been identified for P5.6.1 targets. The consolidating SOs list is showed in the following table (Table 6).

List of Safety Objectives (success approach) for Normal Operations	
F&P-SO#1	Ground shall establish communications with aircraft and exchange messages to determine aircraft i4D capability and notify the crew of its entry into an i4D area.
F&P-SO#2	The aircraft shall downlink its 4D trajectory according to ADS-C contract
F&P-SO#3	Discrepancies between the airborne and ground trajectory data (2D/3D/4D) shall be identified on ground
F&P-SO#4	The ground shall be able to resolve 2D/3D trajectory discrepancies and uplink trajectory revision to the aircraft if necessary
F&P-SO#5	Ground shall Identify the need and possibility to set a reliable time constraint to the aircraft at a determined position (MF) according to the necessities of the traffic.

F&P-SO#6	Ground shall obtain from aircraft the time window for aircraft crossing a given 2D/3D airspace fix
F&P-SO#7	The i4D ground function shall deliver (computation and ground coordination) the coordinated CTA/CTO.
F&P-SO#8	The ATSU_CONTROL and FC shall agree on CTA/CTO.
F&P-SO#9	After a CTO/CTA has been contracted, the crew shall be able to detect in time if the RTA will be missed, and inform ATC.
F&P-SO#10	After a CTO/CTA has been contracted, the ground shall be able to independently detect in time if the RTA will be missed.
F&P-SO#11	Aircraft shall adjust its speed to a predictable value when returning to standard operations.
F&P-SO#12	Separation shall be ensured by ATSU_CONTROL while applying current techniques.
F&P-SO#13	The crew shall be able to check the feasibility of uplinked trajectory revisions before activating them in FMS
F&P-SO#14	The aircraft shall fly the CTO/CTA constraint while satisfying the navigation requirements issued by Eurocae WG85-RTCA SC227 using the RTA functionality of the FMS.
List of Safety Objectives (success approach) for Abnormal Operations	
F&P-SO#15	Ground and crew shall manage a missed RTA situation
F&P-SO#16	Ground shall be able to cancel a CTA/CTO
F&P-SO#17	Ground shall manage case where delay required not within the ETA min-max

Table 12: List of SOs for normal and abnormal operations in case of success approach

From the qualitative analysis of the Safety Objectives a list of Safety Requirements (Functionality & Performance) and additional Safety Requirements for normal operational conditions and abnormal Operational conditions have been derived following the approach described. Please refer to section 3.1 for the entire list.

A.2.2 Failure Approach

The Failure approach deals solely with the system-generated hazards, caused by the failures of the i4D and CTA functions. The assessment related to the failure approach is the core activity to carry out a complete Operational Safety Assessment Process. The aim is to identify and report the Safety Objectives and Requirements.

The failure approach, as expressed into SRM, has to follow the traditional SAM methodology enriched with the use of P16.1.1 contents.

The FHA process followed can be summarized into the following five steps:

1) Hazard identification which focuses on the failure of the system, also in combination and interactions with other systems in the environment of operations. Detection of what can go wrong is the main scope of this first step.

2) Hazard effects identification in order to establish what are the potential consequences on operations taking into account also potential barriers which could act as mitigation means.

3) Effects severity classification.

4) Safety objectives specification to determine their acceptability in terms of hazard's maximum frequency of occurrence, derived from the severity and the maximum frequency of the hazard's effects. In other words, how safe the system needs to be.

Bearing in mind these steps, the hazards have been identified starting from operational hazards of OFA i4D+CTA SAR (driven with the support of the P16.06.01, P4.3, P05.06.01 and WG 78 technical and operational experts). Initial 4D operation for Step 1 is limited to the sharing of on board 4D trajectory data and to the provision of a single time constraint (refer to 4DTRAD Assumption 8 [17]) at a specific point during the descent/approach phase or at any point en-route including monitoring of its trajectory and conformance to the assigned constraint.

The table below contains the full list of operational hazards reflecting the potential failures that can occur in order to perform i4D+CTA operations.

OPERATIONAL HAZARD ID.	OPERATIONAL HAZARD Name
OH1	"Loss of i4D service for multiple aircraft"
OH2	"Degraded i4D service (without CPDLC)"
OH3	"Degraded i4D service for multiple aircraft (loss of CTA/CTO)"
OH4	"Inappropriate CTA/CTO operation induces planning conflict"
OH5	"Multiple incorrect CTA/CTOs induce multiple planned conflicts"

OH6	**“**Inappropriate CTA/CTO operation induces tactical conflict by speed change unexpected or lately detected by ATC”
OH7	**“**Incorrect trajectory synchronisation induces tactical conflict by lateral deviation in current sector**”**
OH8	“CTA/CTO operation makes conflict resolution more complex”

Table 13: Operational Hazards list

Once identified the operational hazards in TMA contest, bearing in mind the operational effects identified into the OFA 4.1.5 SAR Iteration 3 document APPENDIX D [24], the Severity Class of the most probable effect can be set according to AIM Severity Classification scheme for MID-AIR-COLLISION AIM model showed into Guidance E of Guidance to apply SRM [29].

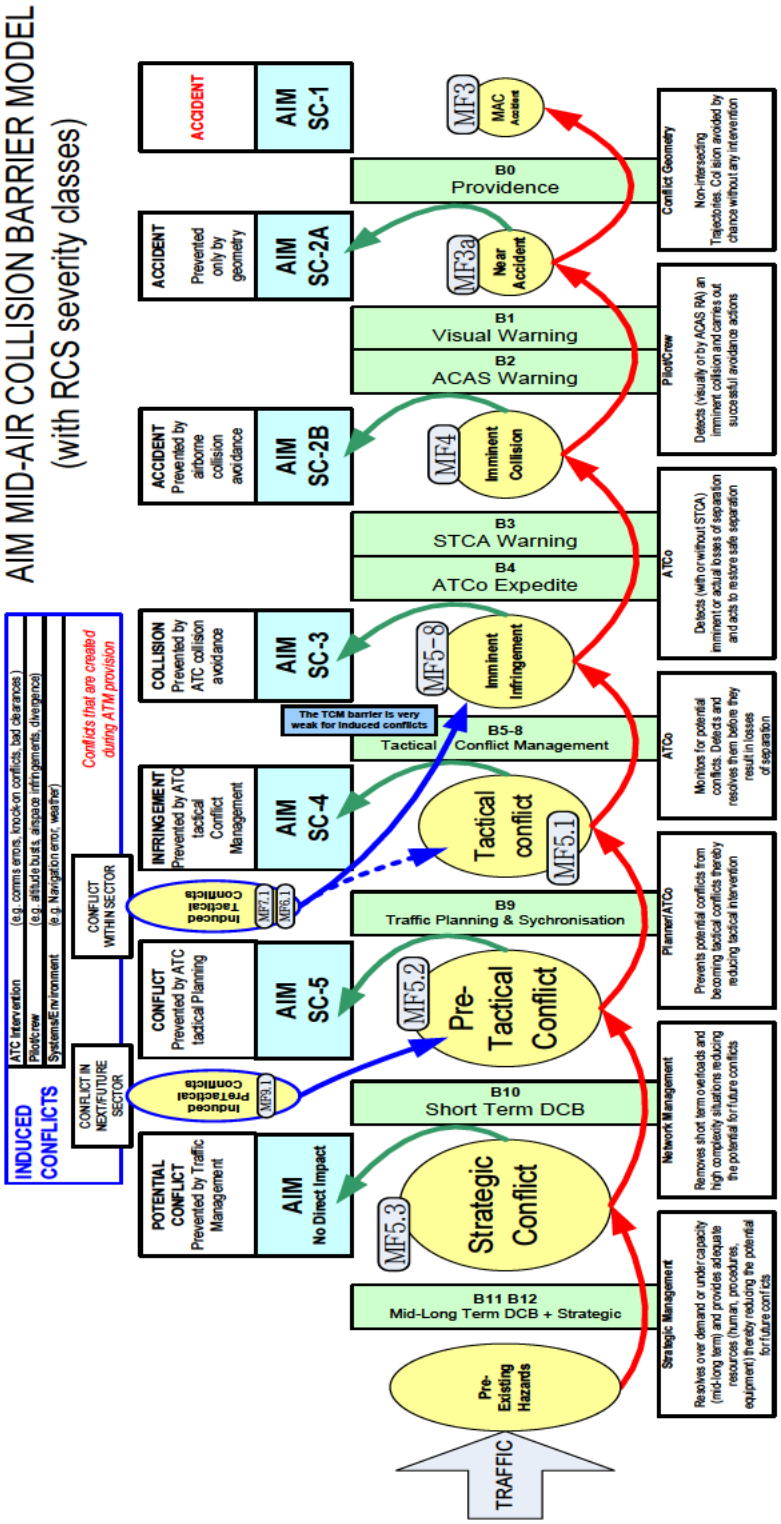

Figure 12: AIM Severity Class Scheme for Mid Air Collision

According to the AIM, the severity class for each OH is expressed in the following table:

OPERATIONAL HAZARD ID.	MAC Severity Class
OH1: "Loss of i4D service for multiple aircraft"	**SC4 (SC4b in new AIM-based RCS)**
OH2: "Degraded i4D service (without CPDLC)"	**SC4 (SC4b in new AIM-based RCS)**
OH3: "Degraded i4D service for multiple aircraft (loss of CTA/CTO)"	**SC4 (SC4b in new AIM-based RCS)**
OH4: "CTA operation induces planned conflict"	**SC4 (SC4b in new AIM-based RCS)**
OH5: "Multiple incorrect CTA/CTOs induce multiple planned conflicts"	**SC4 (SC4b in new AIM-based RCS)**
OH6: "CTA/CTO operation induces tactical conflict by speed change unexpected or lately detected by ATC"	**SC3 (SC4a in new AIM-based RCS)**
OH7: "Incorrect trajectory synchronisation induces tactical conflict by lateral deviation in current sector"	**SC3 (SC4a in new AIM-based RCS)**
OH8: "CTA/CTO operation makes conflict resolution more complex"	**SC4 (SC4b in new AIM-based RCS)**

Table 14: Severity Classes of Operational Hazards

According to SRM, the Safety Objectives of the Worst Credible Effects can be calculated applying the following methodology.

Fixed a Severity Class, then it is possible to use the Risk Classification Scheme for TMA to evaluate the maximum probability of hazard's effect.

MID AIR COLLISION - RISK CLASSIFICATION SCHEME (RCS)				
Severity Class	**AIM Safety Precursor**	**Failure Description**	**Operational Effect of failure**	**Maximum tolerable frequency of occurrence (/flt hr)**
MAC-SC1	**MF3**	A situation where conflict	Accident	

MID AIR COLLISION - RISK CLASSIFICATION SCHEME (RCS)				
Severity Class	**AIM Safety Precursor**	**Failure Description**	**Operational Effect of failure**	**Maximum tolerable frequency of occurrence (/flt hr)**
	MAC	geometry has not prevented physical contact		1 e-9
MAC-SC2a	**MF3a** All ATM failed	A situation where an imminent collision was not mitigated by an airborne collision avoidance	Near collision	1 e-6
MAC-SC2b	**MF4** All ATC failed	A situation where a loss of separation was not mitigated by ATC collision avoidance: STCA, expedite, etc	Imminent collision	1 e-5
MAC-SC3	**MF5-9** Tactical Management failed	A situation where a tactical conflict (coming from planned conflicts or induced conflicts) was not mitigated by ATC conflict management – within the sector (this encompassess situations where a tactical conflict is created by either ATC or crew/aircraft e.g. level bust, bad instructions)	Loss of separation	1 e-4
MAC-SC4	**MF5.1** Planning/ Sequencing Failed MF6.1-9.1 Induced	A situation where a potential conflict, (prior to entering the sector), was not mitigated by traffic planning and synchronisation	Tactical Conflict (planned or induced)	1 e-2
MAC-SC5	**MF5.2** Pre-Tactical Traffic Management Failed	A situation where, on the day of operations, a strategic conflict was not mitigated by airspace managent & DCB. A strategic conflict is typically be a conflict identified 20 mins to 3 hours prior to sector entry.	Pre tactical conflict	1 e-1

Table 15: MAC Risk Classification Scheme

Then the SOs are calculated using the following formula:

$$SO = \frac{Maximum\_Tolerable\_Freq.\_of\_occurrence_{relevant\_severity\_class}}{N \times IM}$$

Where:

- $Maximum\_Tolerable\_Freq.\_of\_occurrence_{relevant\_severity\_class}$ is the maximum probability of the hazard as obtained from the Table 9 above;

- N is the overall number of operational hazard for a given severity class as obtained from the table below for MAC TMA:

Severity Class	"N" Number of hazards per Severity Class per Accident Type for MAC (TMA)
SC1	1
SC2 (a)	5
SC2 (b)	10
SC3	25
SC4	50
SC5	100

Table 16: N number for Severity Class type

- IM is the Impact Modification factor to take account of the Number of aircraft exposed to the operational hazard

> The severity assessment does not include consideration of the number of aircraft exposed to the hazard. This is accounted for through the calculation of the SO i.e. through the outcome frequency / probability on demand with a modification factor related to the number of aircraft exposed to the hazard. This must be estimated operationally. In principle where hazards are generated that affect 10 aircraft, then the SO values must be divided by 10.
>
> IM depends both on the number of aircraft that can be affected by the hazard when it occurs but also on the time period when the hazard is preventing the barrier from functioning. If a hazard is described as complete or partial loss of some system then the IM values should be different for the two cases and different SO should be generated with more stringent safety objective being for the more critical situation (i.e. the complete loss).

Following the previous methodology, the table below expresses the SOs for each OH.

Note that, since the SO is expressed in 1/SHO, it is necessary to convert the frequency of occurrence, expressed in FH (Flight Hour), in SOH (Sector Operating Hour). The conversion is done using the assumption: 1 sector operational hour (SOH) is equivalent to 6 flight hours (FH).

ID	Safety Objectives	Formula / Justification for IM
H-SO#1	- The probability of Loss of i4D service for multiple aircraft shall not exceed 2.4E-04 / SOH	$1E^{-02} * 6/50*5 = 2.4E^{-04}$ / SOH IM = 5. Estimation since the IM cannot be too small because the service would then first be downgraded (Haz#2 and Haz#3).
H-SO#2	- The probability of Degraded i4D service (without CPDLC) shall not exceed 2.4E-04 / SOH	$1E^{-02} * 6/50*5 = 2.4E^{-04}$ / SOH IM = 5. Estimation since when CPDLC is not available, instructions can still be given to a relatively large number of aircraft
H-SO#3	- The probability of Degraded i4D service for multiple aircraft (loss of CTA/CTO) shall not exceed 2.4E-04 / SOH	$1E^{-02} * 6/50*5 = 2.4E^{-04}$ / SOH IM = 5. Estimation since as soon as a few aircraft cannot be accurately pre-sequenced; the sequence is maintained mainly in baseline configuration. Ops projects may decide after exercises to decrease IM down to 3.

ID	Safety Objectives	Formula / Justification for IM
H-SO#4	– The CTA/CTO operation shall not induce more than 1.2E-03 planned conflict per SOH	$1E^{-02} * 6/50*1 = 1.2E^{-03}$ / SOH
H-SO#5	- The probability of Multiple incorrect CTA/CTOs inducing multiple planned conflicts shall not exceed 2.4E-04 / SOH	$1E^{-02} * 6/50*5 = 2.4E^{-04}$ / SOH IM = 5. Estimation since effect on ATCO workload and capability to safely perform its normal duties is impacted as soon as this number of simultaneous conflicts arises. Ops projects may decide after exercises to decrease IM down to 3.
H-SO#6	- The probability of CTA/CTO operation inducing tactical conflict induced by speed change unexpected or lately detected by ATC shall not exceed 2.4E-05 / SOH	$1E^{-04} * 6/25*1 = 2.4E^{-05}$ / SOH
H-SO#7	- The probability of incorrect trajectory synchronization inducing tactical conflict by lateral deviation in current sector shall not exceed 2.4E-05 / SOH	$1E^{-04} * 6/25*1 = 2.4E^{-05}$ / SOH
H-SO#8	- The probability of CTA/CTO operation making conflict resolution more complex shall not exceed 1.2E-03 / SOH	$1E^{-02} * 6/50*1 = 1.2E^{-03}$ / SOH

Table 17: Safety Objectives per Operational Hazard

New mitigations have been formalized during the FHA elaboration process.

ID	Description
F&P-SO#18	EPP synchronization shall be performed before issuing an ETA min-max request in ATSU_DEST.
F&P-SO#19	Feedback loop required: En-Route ATSU shall inform ATSU_DEST that a CTA has been set or not. Note: In Step 1, the "Silent procedure" is applied: ATSU_CONTROL notifies ATSU_DEST only if the CTA has not been successfully agreed. This does not mitigate all cases (e.g. "Lost CTA/CTO for one aircraft" or "ATCO omission to uplink CTA").
F&P-SO#20	Consistency of the MF with trajectory shall be checked at all possible steps: • Aircraft shall check that the MF in the request is in the trajectory (no automatic insertion). • Ground system shall not select a MF that is not on the aircraft trajectory. • ATSU_DEST shall check the consistency of the MF in the ETA min-max reply w.r.t the selected one. • ATSU_DEST shall check that the MF is in the STAR
F&P-SO#21	ATCO procedures shall be defined to confirm trajectory in case of lack of EPP i.e. ATCO clears aircraft across their area of responsibility
F&P-SO#22	The ground system shall warn the Executive Controller (ATCO_EXE) of potential speed changes after RTA is established: information that the speed is likely to change significantly shall be presented to the ATCO. For 5.6.1, in addition to the CTA, information is also provided from the AMAN (TTL/TTG) to assist a controller in assessing a potential speed impact of an RTA being applied.

Table 18: Additional Safety Objectives (functionality and performance) in case of internal failures

A.2.3 Causal analysis

The FHA has identified the operational system-generated hazards and their associated quantitative Safety Objectives.

The aim of the causal analysis is to derive Safety Requirements for the Failure Case in order to ensure the achievability of the Safety Objectives of the Hazards. Performing this analysis, the causes that may lead to each hazard are investigated through fault trees proposing internal mitigations that would prevent their occurrences.

Considering that the safety objective derived from the AIM-based RCS encompasses all types of failures and errors, it is necessary to extend the scope of traditional fault trees to a new type that represents all the contributors whether they are system (hardware), or human (procedure design or execution, complex software design).

The consideration of human contributions in fault trees is useful to state to the maximum possible extent on the tolerability of the human error, permits to have a general view of the risk and to support the apportionment of the risk across domains and stakeholders. This approach allows complementing the traditional systems causal analysis by setting safety requirements also at human level.

The ultimate goal is to derive safety requirements that are:

- Qualitative and quantitative for systems (equipment hardware)
- Qualitative only for humans (operation and software design).

Please refer to SAR IT3 for the complete list of fault tree developed for each operational hazard.

The list of Safety Requirements coming from the presented assessment is collected into OFA SAR document [24].

A.2.4 Safety Requirements derivation

Starting from OFA SAR requirements were filtered and/or modified according to P5.6.1 scope and traceability with P5.6.1 OSED [11].

In case no traceability was found, additional requirements have been introduced.

The final list of SPR requirements is presented in Section 3.1

A.2 Security risk assessment

The security risk assessment was done in conjunction with P16.6.2 team that performed the assessment for OFA 4.1.5 [7]. As said into “SESAR ATM Security Reference Material - Level 1” [30], the primary security risk assessment should be made at OFA level and then detailed for project needs following the steps below:

- ATM Security assessment and assurance activities must be done at OFA level.
- OFA projects shall ensure that ATM Security Assessment and Assurance activities are carried out as part of the engineering and validation processes.
- P16.06.02 has to provide an active and passive support working as an interface for WP4-15 projects

Essentially after performed Minimum Set of Security Controls (MSSC), the Screening and Scoping process identifies such projects and OFAs for which MSSC is not sufficient and so performs Security Risk Assessment and Assurance activities results to be mandatory.

Being the project P5.6.1 part of OFA i4D+CTA, for this OFA, additional controls, a part of MSSC, have to be considered.

The “Security Risk Assessment Methodology (SecRAM)” used to perform the Security Risk Assessment is expressed into the P16.02.03 document “SESAR ATM Security Risk Assessment Method” [31] and can be summarized into the following steps and schematized in Figure 13.

For OFAs in V1 phase - Impact Assessment:

- Identification of their primary assets
- Assessment of the potential impact of a successful attack on the primary assets supported by operational impact scenarios

For OFAs in V2/V3 phase - Risk Assessment:

- Identification of the supporting assets derived from the primary assets
- Identification of the threats targeting the supporting assets and threats scenarios
- Risk level evaluation of the threat scenarios targeting the supporting assets based on the likelihood and the impact of those threat scenarios
- Establishment of a list of additional controls to be achieved to address security risks

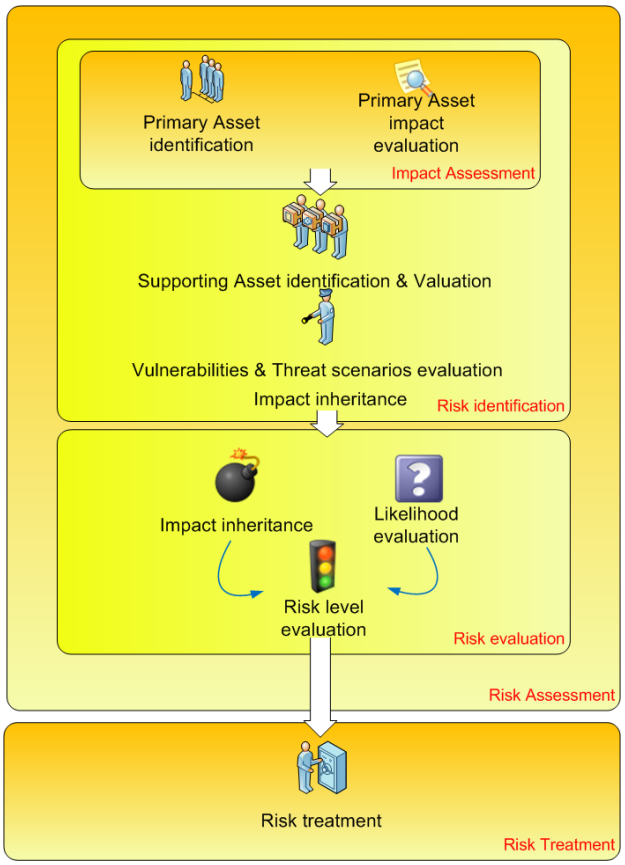

Figure 13: SecRAM process overview

The risk assessment as defined in ISO 27005 [32] ends with the risk level evaluation of the threat scenario but in SESAR area there are four option available for each threat scenario:

- Accept (or Tolerate) the risk, which means that no further action is needed. The risk level is considered low enough to be accepted.
- Reduce (or Treat) the risk to a new level through the selection of controls (additional to the MSSC) so that the residual risk can be reassessed as being acceptable. WP 16.02.05 also provides control catalogues and guidelines to support this selection.

- Avoid (or Terminate) the risk, which means that if the risk is considered too high and the counter-measures to reduce it too costly, then the project can decide to withdraw the activity or change its nature so that the risk is not present anymore.
- Transfer the risk, which means that the project decides that the risk should be transferred to another party that can most effectively manage the particular risk.

In order to perform this security assessment, P5.6.1 received support from P16.6.2 team and the decision for the risk treatment is to reduce the risk proposing security requirements which cover the identified risks since cover also the most critical impacts identified for primary assets and so controls proposed.

In the following paragraphs, the risk assessment performed is shown.

A.2.1 Impact assessment

First of all, the assessment starts with the evaluation of the primary assets PA defining the evaluated scope of the OFA i4D+CTA in terms of security (on confidentiality, integrity and availability-CIA):

For each identified PA, the impact areas with the relative impact value can be evaluated according to Table 13.

	5	4	3	2	1
IMPACT AREAS	**Catastrophic**	**Critical**	**Severe**	**Minor**	**No impact /**
IA1:PERSONNEL	Fatalities	Multiple Severe injuries	Severe injuries	Minor injuries	No injuries
IA2:CAPACITY	Loss of 60%-100% capacity	Loss of 60%-30% capacity	Loss of 30%-10% capacity	Loss of up to 10% capacity	No capacity loss
IA3:PERFORMANCE	Major quality abuse that makes multiple major systems inoperable	Major quality abuse that makes major system inoperable	Severe quality abuse that makes systems partially inoperable	Minor system quality abuse	No quality abuse
IA4:ECONOMIC	Bankruptcy or loss of all income	Serious loss of income	Large loss of income	Minor loss of income	No effect

IA5:BRANDING	Government & international attention	National attention	Complaints and local attention	Minor complaints	No impact
IA6:REGULATORY	Multiple major regulatory infractions	Major regulatory infraction	Multiple minor regulatory infractions	Minor regulatory infraction	No impact
IA7:ENVIRONMENT	Widespread or catastrophic impact on environment	Severe pollution with long term impact on environment	Severe pollution with noticeable impact on environment	Short Term impact on environment	Insignificant

Table 19: SESAR Security Impact areas

Here below it is possible to find Table 14 which summarizes the assessment done per PA with the worst impact level, i.e. maximum value found for Confidentiality, Integrity and Availability considering all Security Impact Areas of Table 13.

PRIMARY ASSETS	C	I	A
PA#1: Provide and Exchange Trajectories	**2**	**5**	**2**
	Operational scenarios		
	Trajectories are made public or transmitted by an attacker and have branding/economic impact on an Airline.	An attacker modifies the integrity of this service in order to affect possibly multiple aircraft trajectories.	An attacker force crew to fall back to voice procedure.
PA#2: On-board trajectory optimization	**C**	**I**	**A**
	3	**5**	**2**
	Operational scenarios		
	An attacker gets access to patented processes of optimization.	An attacker modifies the integrity of this service in order to affect possibly multiple aircraft	An attacker force crew to fall back to non-optimized trajectories.

		trajectories.	
PA#3: Discrepancy detection	**C**	**I**	**A**
	2	**3**	**2**
	Operational scenarios		
	An attacker gets access to patented processes of discrepancy detection.	An attacker can prevent discrepancy detection or provide false alarms	An attacker forces ATC discrepancy detection back to the back-up procedures.
PA#4: Ground coordination between ATSUs	**C**	**I**	**A**
	2	**3**	**3**
	Operational scenarios		
	An attacker publishing precise information about Air Traffic Control could have limiter branding impact on both ATC and Airlines.	An attacker modifying data exchanged between TMA could impact trajectory calculation and distribution.	An attacker could disable TMA communication and force the use of back-up procedures.
PA#5: Provide alerts, clearances and messages	**C**	**I**	**A**
	2	**5**	**2**
	Operational scenarios		
	An attacker could publish confidential alerts or message used by this service.	An attacker modifies the integrity of this service in order to affect alerts and critical	An attacker force crew to fall back to voice procedures.
PA#6: Downlink information	**C**	**I**	**A**
	2	**3**	**2**
	Operational scenarios		
	An attacker could publish confidential information used by this service.	An attacker could modify downlink messages to trigger unneeded alarms or alert procedures.	An attacker forces crew to fall back to voice procedures.

Table 20: Primary assets identified with relative CIA impact

Looking at Table 14, it is possible to consider that there is a high need for integrity and a medium need for confidentiality and availability.

According to the SecRAM, those security needs evaluated by the impact assessment phase are strong enough to conclude that a full risk assessment is needed.

The full risk assessment consists in evaluating the supporting assets associated with the listed primary assets and generates and evaluates the associated threat scenarios.

A.2.2 Risk Assessment

In the security risk assessment phase, for each individuated Primary Assets, Supporting Assets (SA) and Threat scenarios have to be generated and evaluated.

The Supporting Assets selected for each primary asset are shown in Table 15 with the correspondent inherited impact (maximum value of the supporting asset considering all PAs CIA values).

Supporting Assets	PA#1			PA#2			PA#3			PA#4			PA#5			PA#6			C	I	A	Inherited Impact
	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	Max value per PA#			
	2	5	2	3	5	2	2	3	2	2	3	3	2	5	2	2	3	2				
FMS		X			X									X			X		3	5	2	5
On board display units		X			X			X											3	5	2	5
AMAN-DMAN		X																	2	5	2	5
CPDLC		X												X					2	5	2	5
ADS-C																	X		2	3	2	3
VHF Radio		X						X						X			X		2	5	2	5
Gnd/Gnd Communication		X						X			X								2	5	3	5
On-board crew		X			X			X						X					3	5	2	5
On-ground personnel		X						X			X			X			X		2	5	3	5
Control display units		X						X						X			X		2	5	2	5
ATC ground site		X						X			X			X			X		2	5	3	5

Table 21: Supporting assets per Primary assets and related inherited impact

Threat considered generating threat scenarios are collected in Table 16:

Threat
Destruction of equipment or media
Deny of service
Electromagnetic/thermal radiations
Eavesdropping
Theft
Tampering
Limit maintainability
Abuse of rights
Physical intrusion
Social engineering
Jamming

Table 22: Threat considered to set threat scenarios

By applying all selected threats to the relevant supporting assets, threat scenarios were generated and evaluated (see Table 21). In particular, the risk of each threat scenarios, according to SecRAM, was evaluated according to Table 18 where, the impact depends on the threat CIA conditions and likelihood is evaluated with Table 17.

Likelihood	Qualitative and quantitative interpretation
5. Frequent	Likely to occur frequently Above 80% of the time
4. Probable	Will occur several times in the life of the project Above 60%-80% of the time
3.Occasional	Likely to occur a few times in the life of the project 20%-60% of the time
2. Remote	Unlikely but possible to occur in the life of the project 0%-20% of the time
1.Improbable	So unlikely, it can be assumed that occurrence may not be experienced

Table 23: Likelihood evaluation

Risk Level					
	SL Impact				
Likelihood	1	2	3	4	5
5	Medium	High	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Low	Medium	High
1	Low	Low	Low	Medium	Medium

Table 24: Risk evaluation

The following table lists al the threat scenarios and their evaluations.

Threat Scenario	Supporting Asset	Impact	Likelihood	Risk
Tampering with software due to implementation flaw	FMS	5	4	High
Tampering with network due to unsecured protection of data	Ground-Ground communication	5	4	High
Tampering with network due to physical access to media	Ground-Ground communication	5	4	High
Tampering with network due to unsecured protection of data	CPDLC	5	4	High
Tampering with network due to unsecured protection of data	VHF Radio	5	4	High
Tampering with network due to physical access to media	CPDLC	5	4	High
Tampering with network due to physical access to media	VHF Radio	5	4	High
Tampering with network due to flaw in implementation	CPDLC	5	4	High
Abuse available access of the network	CPDLC	5	4	High
Abuse available access of the network	VHF Radio	5	4	High
Tampering with the system during maintenance process	On-board display units	5	3	High
Tampering with software during maintenance/update	FMS	5	3	High
Tampering with the system due to unsecured configuration	On-board display units	5	3	High
Tampering with software due to unsecured configuration	FMS	5	3	High
Tampering with the system due to flaw in the implementation	On-board display units	5	3	High
Tampering with the system before delivery	On-board display units	5	3	High
Tampering with software before delivery	FMS	5	3	High
Tampering with software during disposal process	FMS	5	3	High
Abuse available function of the software	FMS	5	3	High
Gathering of information from staff due to a lack of security awareness	On-board crew	5	3	High
Tampering with network due to flaw in implementation	Ground-Ground communication	5	3	High

Abuse available access of the network	Ground-Ground communication	5	3	High
Gathering of information from staff due to a lack of security awareness	On-ground personnel	5	3	High
Tampering with hardware data of the system	Control display units	5	3	High
Tampering with the system during maintenance process	Control display units	5	3	High
Tampering with the system due to unsecured configuration	Control display units	5	3	High
Tampering with the system due to flaw in the implementation	Control display units	5	3	High
Tampering with the system before delivery	Control display units	5	3	High
Abuse available function of the system	Control display units	5	3	High
Tampering with software due to implementation flaw	AMAN - DMAN	5	3	High
Tampering with software before delivery	AMAN - DMAN	5	3	High
Tampering with software during disposal process	AMAN - DMAN	5	3	High
Abuse available function of the software	AMAN - DMAN	5	3	High
Tampering with hardware data of the system	On-board display units	5	2	High
Tampering with unprotected data in software	FMS	5	2	High
Tampering with the system when inside of secure perimeter	On-board display units	5	2	High
Tampering with the system due to unsecured segregation with other systems	On-board display units	5	2	High
Tampering with software due to unsecured segregation with other software	FMS	5	2	High
Abuse available function of the system	On-board display units	5	2	High
Limit maintainability of the system by preventing periodic replacement or update	On-board display units	5	2	High
Limit maintainability of the software by preventing periodic replacement or update	FMS	5	2	High
Access to a site due to unsecured access control	ATC Ground site	5	2	High
Access to a site due to inefficient physical protection	ATC Ground site	5	2	High

Tampering with the system when inside of secure perimeter	Control display units	5	2	High
Tampering with the system due to unsecured segregation with other systems	Control display units	5	2	High
Limit maintainability of the system by preventing periodic replacement or update	Control display units	5	2	High
Tampering with unprotected data in software	AMAN - DMAN	5	2	High
Tampering with software during maintenance/update	AMAN - DMAN	5	2	High
Tampering with software due to unsecured configuration	AMAN - DMAN	5	2	High
Tampering with software due to unsecured segregation with other software	AMAN - DMAN	5	2	High
Tampering with network due to flaw in implementation	VHF Radio	5	2	High
Limit maintainability of the software by preventing periodic replacement or update	AMAN - DMAN	5	2	High
Tampering with network due to physical access to media	ADS-C	3	4	High
Tampering with network due to flaw in implementation	ADS-C	3	4	High
Tampering with network due to unsecured protection of data	ADS-C	3	4	High
Theft of system during disposal process	On-board display units	3	3	Medium
Theft of confidential information inside the software	FMS	3	3	Medium
Deny of service of the network by flooding due to unsecured segregation with other networks	Ground-Ground communication	3	3	Medium
Abuse available access of the network	ADS-C	3	3	Medium
Eavesdropping of network due to physical access to media	Ground-Ground communication	2	4	Medium
Eavesdropping of network due to unsecured authentication	Ground-Ground communication	2	4	Medium
Eavesdropping of network due to unsecured segregation scheme	Ground-Ground communication	2	4	Medium
Eavesdropping of network due to unsecured confidential information	Ground-Ground communication	2	4	Medium

Eavesdropping of network due to flaw in implementation	Ground-Ground communication	2	4	Medium
Eavesdropping of network due to physical access to media	CPDLC	2	4	Medium
Eavesdropping of network due to physical access to media	VHF Radio	2	4	Medium
Eavesdropping of network due to unsecured authentication	CPDLC	2	4	Medium
Eavesdropping of network due to unsecured authentication	VHF Radio	2	4	Medium
Eavesdropping of network due to unsecured segregation scheme	CPDLC	2	4	Medium
Eavesdropping of network due to unsecured segregation scheme	VHF Radio	2	4	Medium
Eavesdropping of network due to unsecured confidential information	CPDLC	2	4	Medium
Deny of service of the network by flooding due to unsecured segregation with other networks	ADS-C	2	4	Medium
Eavesdropping of network due to physical access to media	ADS-C	2	4	Medium
Eavesdropping of network due to unsecured authentication	ADS-C	2	4	Medium
Eavesdropping of network due to unsecured segregation scheme	ADS-C	2	4	Medium
Eavesdropping of network due to unsecured confidential information	ADS-C	2	4	Medium
Eavesdropping of network due to flaw in implementation	ADS-C	2	4	Medium
Eavesdropping of network due to unsecured configuration	ADS-C	2	4	Medium
Theft of the system	On-board display units	3	2	Low
Destruction of a site due to unsecured access control	ATC Ground site	3	2	Low
Gathering of information from staff due to unsecured authentication of people	On-board crew	3	2	Low
Deny of service of the network due to EMP or thermal radiations	Ground-Ground communication	3	2	Low
Jamming of the network due to physical weaknesses	Ground-Ground communication	3	2	Low
Destruction of a fragile site	ATC Ground site	3	1	Low

Deny of service based on implementation flaw	FMS	2	3	Low
Theft of system during disposal process	Control display units	2	3	Low
Eavesdropping of network due to outdated elements	Ground-Ground communication	2	3	Low
Eavesdropping of network due to unsecured configuration	Ground-Ground communication	2	3	Low
Vandalism using electromagnetic/thermal radiation	Control display units	2	3	Low
Deny of service based on implementation flaw	AMAN - DMAN	2	3	Low
Deny of service of the network by flooding due to unsecured segregation with other networks	CPDLC	2	3	Low
Deny of service of the network due to EMP or thermal radiations	CPDLC	2	3	Low
Eavesdropping of network due to unsecured confidential information	VHF Radio	2	3	Low
Eavesdropping of network due to outdated elements	CPDLC	2	3	Low
Eavesdropping of network due to flaw in implementation	CPDLC	2	3	Low
Eavesdropping of network due to unsecured configuration	CPDLC	2	3	Low
Eavesdropping of network due to unsecured configuration	VHF Radio	2	3	Low
Jamming of the network due to physical weaknesses	VHF Radio	2	3	Low
Eavesdropping of network due to outdated elements	ADS-C	2	3	Low
Jamming of the network due to physical weaknesses	ADS-C	2	3	Low
Vandalism using electromagnetic/thermal radiation	On-board display units	2	2	Low
Theft of the system	Control display units	2	2	Low
Vandalism on fragile system	On-board display units	2	2	Low
Vandalism on fragile system	Control display units	2	2	Low
Gathering of information from staff due to unsecured authentication of people	On-ground personnel	2	2	Low
Theft of confidential information inside the software	AMAN - DMAN	2	2	Low

Deny of service of the network by flooding due to unsecured segregation with other networks	VHF Radio	2	2	Low
Deny of service of the network due to EMP or thermal radiations	VHF Radio	2	2	Low
Eavesdropping of network due to outdated elements	VHF Radio	2	2	Low
Eavesdropping of network due to flaw in implementation	VHF Radio	2	2	Low
Jamming of the network due to physical weaknesses	CPDLC	2	2	Low
Deny of service of the network due to EMP or thermal radiations	ADS-C	2	2	Low

Table 25: Threat scenarios and their risk evaluation [7]

A.2.3 Risk treatment

The possible decisions on risk treatment are:

- **Tolerate** the risk, which means that no further action is needed. The risk level is considered low enough to be accepted.
- **Treat** the risk to a new level through the selection of controls (additional to the MSSC) so that the residual risk can be reassessed as being acceptable.
- **Transfer** the risk, which means that the project decides that the risk should be transferred to another party that can most effectively manage the particular risk.
- **Terminate** the risk, which means that if the risk is considered too high and the counter-measures to reduce it too costly, then the project can decide to withdraw the activity or change its nature so that the risk is not present anymore.

Of the risks evaluated, it is recommended that all are treated through the application of controls.

A number of supporting assets were excluded from the assessment as they are already operational systems or the security requirements have been driven by a different primary capability. The latter point is similar to transferring the risk, although the risk will remain with the respective ANSPs. This approach has had the effect of de-scoping the risk assessment to focus on the areas that are within the influence of OFA 4.1.2.

A.2.4 Recommended controls

This security risk assessment assumes that the MSSCs are applied but has not assessed the applicability of all of the MSSCs. This is a recommended future action as part of ANSPs' security management as it may lead to cost savings on deployment.

[7] Current identified risks still have to be validated by operational people (air traffic controllers and pilots).

The risk assessment has recommended controls that are also within the set of MSSCs, however, these should also be a particular focus for the detailed design and specification work on SESAR Solutions 5 and 6 in particular. These controls are:

AMAN Processor

- Data Input Credibility Checking AND Authentication (MSSC C42)
- Firewall Separation
- Hardware & Software Installation Process
- Standby / Alternate Facilities
- System Accreditation (in this case specifically requiring penetration testing, potentially in the context of the wider base of ATM systems within an ATSU).
- Technical Control (bespoke control design to address the specific threat of cyber intrusion, alongside firewall and system accreditation).
- Viruses & Malware Installation and Patches (MSSC C24)

ADS-C datalink(s)

- Data Input Credibility Checking AND Authentication
- Encoding Data
- Technical Control (bespoke control design to address the specific threats of jamming, spoofing and denial of service).

ADS-C processor

- As for AMAN processor.

The derivation of the above controls is stored in an MS Access database, file ‘ctrl-s_ofa_4_1_2_new_05’.

In addition to the above controls, the following are recommended by the i4D + CTA risk assessment for CPDLC / ADS-C. These are mostly covered by the MSSCs, as follows:

- Review of user access rights (MSSC C15, C17)
- Network routing control (MSSC C26)
- Network connection control (MSSC C26)

- Cabling security (MSSC C19)
- Information labelling and handling (MSSC C10, C11)
- Classification guidelines (MSSC C10, C11)
- Equipment siting and protection
- Segregation in networks (MSSC C39)
- Equipment maintenance (MSSC C21)

A.2.5 Mitigated risks

Application of the recommended controls should lead to the levels of risk identified in the following table. Note that the assessors have determined a reduction in likelihood rather than impact of the threat. The likelihood has been reduced to 1-2 ('very unlikely' / 'unlikely') assuming the recommended controls are in place and maintained within the context of operators Security Management Systems:

Threat	Supporting Asset	Effect on CIA	Mitigated impact	Mitigated likelihood	Mitigated risk
Spoofing	ADS-C datalink(s)	I	4	1	Medium
Denial of service	ADS-C datalink(s)	A	4	2	Medium
Cyber intrusion	ADS-C processor	C I A	4	1	Medium
Malware	ADS-C processor	C I A	4	2	Medium
Cyber intrusion	AMAN processor	C I A	4	1	Medium
Malware	AMAN processor	C I A	4	1	Medium
Jamming	ADS-C datalink(s)	A	4	1	Medium
Abuse of rights and	ADS-C	C I A	4	1	Medium

Threat	Supporting Asset	Effect on CIA	Mitigated impact	Mitigated likelihood	Mitigated risk
privilege escalation	processor				
Corruption of data	ADS-C processor	I A	4	2	Medium
Abuse of rights and privilege escalation	AMAN processor	C I A	4	2	Medium
Corruption of data	AMAN processor	I A	4	2	Low

A.2.6 Conclusions

The security risk assessment at OFA 4.1.2 level has highlighted a number of key risks to the following Supporting Assets: AMAN Processor, ADS-C datalink(s) and ADS-C processor. Whilst there are several other key systems involved in supporting OFA 4.2.1 Primary Assets, these have been excluded from the scope of the assessment as they are either in current operation or the security requirements will be driven by a higher order capability than Extended AMAN. A small set of controls has therefore been recommended.

As it has been assumed that the SESAR Minimum Set of Security Controls (MSSCs) will be applied, these should also be taken forward (with the recommended controls) into the next stage of system development.

All the information about the security issues OFA 04.01.02 related are wider described in P16.06.02 *Security Risk Assessment of OFA 04.01.02 Enhanced Arrival & Departure Management in TMA and En Route* [64].

A.2.7 Security Requirements

Here below it is possible to find P5.6.1 security requirements that, from a top-down perspective, being linked to Primary Assets impact evaluation cover controls provided and so reduce the level risk.

1. The ground systems should assure security controls in order to prevent an attacker to modify the integrity of data transmitted. (covers PA #1- PA #3)

2. The ground systems should assure security controls in order to prevent an attacker to transmit false alerts, clearances to aircrafts. (covers PA #5)

3. The on-board systems should assure security controls in order to prevent an attacker to modify the integrity of data transmitted. (covers PA #2- PA #4)

4. The on-board systems should assure security controls in order to prevent an attacker to modify downlink messages to trigger unneeded alarms or alert procedures. (covers PA #6)

Those requirements are provided in the correct SJU format in section 3.3.

A.3 Environment impact assessment

For the environmental assessment please refer to the operational performance assessment section A.4.4.

A.4 Operational Performance Assessment

A.4.1 OPA methodology for SPR

The performance assessment process, shown in B05 Performance Assessment Methodology for Step1 SESAR timeframe [41] (Figure 13), is divided into four main phases, which are performance framework definition, qualitative assessment, quantitative assessment, and analysis. In details the four steps are as follows.

- For the **performance framework definition** the scope is defined first, which means selecting the KPAs, Key Performance Indicators (KPIs) and Influencing Factors (IFs) considered in the performance assessment. Based on the selected KPAs, Influence Diagrams have to be developed, chosen from previous work, or obtained from WP B.4.1.

- The **qualitative assessment** contains two subparts. At first, an assessment of the impact of individual Operational Improvements (OI) steps on influencing factors has to be made by

means of defining benefits mechanisms, followed by a qualitative aggregation of OI steps' benefits to influencing factors.

- For the **quantitative assessment**, first quantitative models have to be established from qualitative ones. Then, the quantitative evidence has to be collected from validation experiments, or estimated with help of expert groups. Finally, the quantitative benefits are aggregated to the KPA level.
- The **analysis** starts with a maturity assessment, which is collecting additional information for passing the transition criteria of the V3 validation phase. The subsequent gap analysis will be limited to a subset KPAs and KPIs for which draft targets will be defined by B4.1. The analysis phase finishes with conclusions drawing and recommendations provision.

Bearing in mind this classification, the technique proposed for this SPR covers aspects of this B05 performance process. Since in SESAR SPR template [42] is not specified any technique to obtain performance requirements, in this context has been set a simple methodology that, following the B05 idea, performs a first qualitative performance assessment thanks to brainstorming sessions based on contents coming from project Benefit and Impact Mechanism, OSED and Validation Reports documentations and joined from expert people internal to the project.

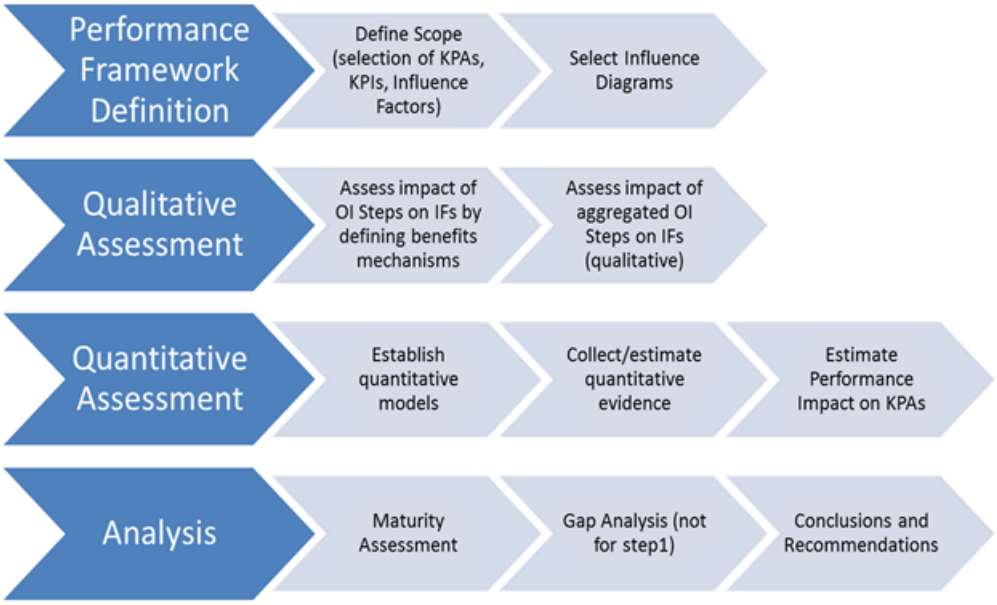

Figure 14: B05 performance assessment process

As shown in Figure 13, the Operational Performance Assessment (OPA) proposed for P5.6.1 SPR follows transversally the B05 OPA Process supported by a simple and schematic approach and enriched with brainstorming sessions based on concept description and validation experience done at project level and it has the aim to obtain performance requirements that should mitigate/prevent some operational issues impacting the key performance area under assessment.

The methodology presented can be considered as simple tool that guide the users to set performance requirements. As input, it considers concept description of OSED (*Operational Service and Environment description*), *exercise Validation Reports* (VALRs) and benefit and impact Mechanism

documents produced at project level. Thanks to brainstorming sessions joined by project experts, valuing any possible operational issues that may affect the performance level that is expected to be achieved by the concept under investigation (i.e. CTA). As output, it proposes mitigations and/or preventions (formally expressed by performance requirements) that, reducing the severity of the negative impact on performances, aim to satisfy the established performance project expectations. In other words, the Operational Performance Methodology for SPR can be executed considering the following steps:

- Benefit and Impact Mechanism consultation in order to select KPA to be investigated.
- Brainstorming sessions based on KPA and relevant project documentations (e.g. OSED, Validation Reports, Benefit and Impact Mechanism) in order to identify operational performance issues and sub-issues that have a negative impact on the level of performance expectation
- Evaluation of performance issues impact on selected KPA
- Identification of specific mitigation/preventions based on identified issues impact
- Identification of formal Performance Requirements

Figure below shows schematically the overall assessment steps.

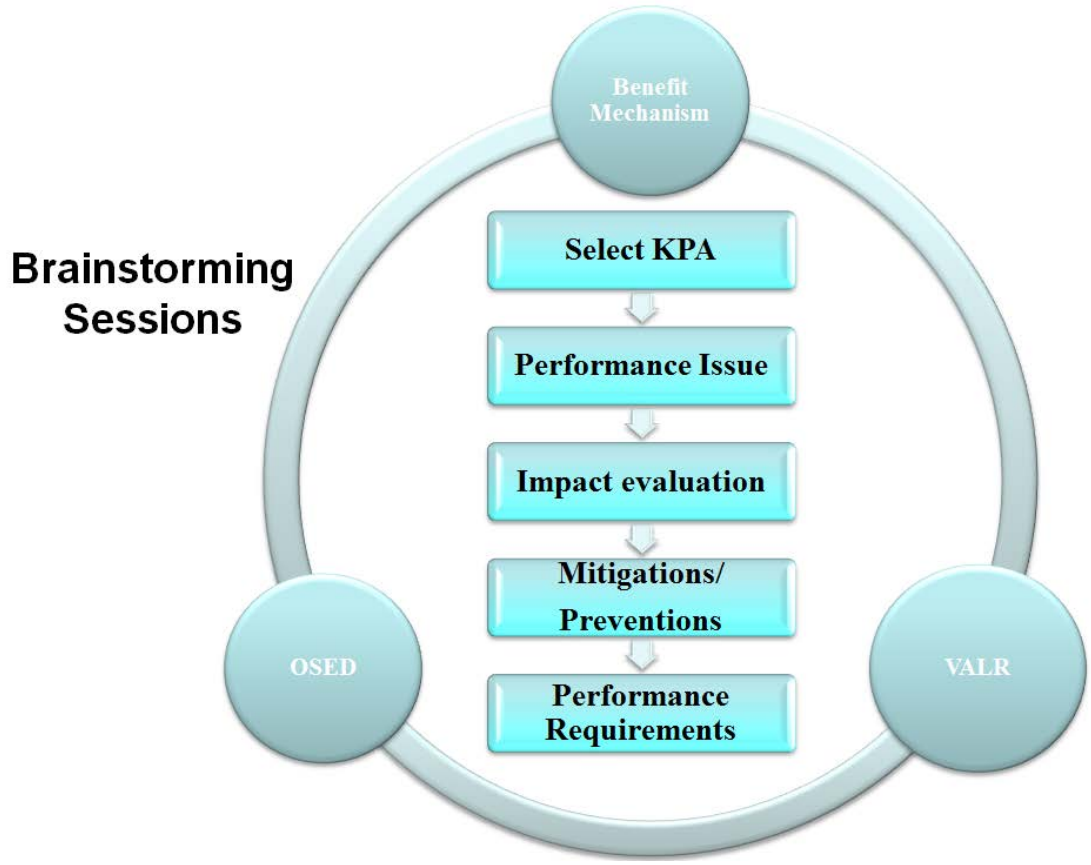

Figure 15: OPA methodology adopted for SPR

It is important to note that the process can be implemented in an iterative way, executed per storyboard concept steps or per different editions of document, until achieve the desired level of performance expectations.

The simple tool that guides the user to follow the methodology of the *Operational Performance Assessment* used for SPR is expressed by Table 20.

KPA	Performance Issue	Performance Sub-Issue	Impact	Mitigations/Preventions	Performance Requirements[8]

Table 26: Operational Performance Assessment for SPR

Here below, are presented the guidelines useful for to fill in the table appropriately:

- ***KPA:*** *is the key performance area under assessment for which the OPA is performed*
- ***Performance Issue:*** *is a possible operational situation that, if not avoided with properly preventions and/or mitigations, may cause operational effects that can reduce the performance expectations of the project.*
- ***Performance Sub-Issue:*** *details of Operational Performance Issue (if applicable).*
- ***Impact:*** *is the potential operational effect that expresses how the issue can reduce the level of performance.*
- ***Mitigations/Preventions:*** *are necessary to overcome the identified performance issues and so mitigate or prevent the related impact that they have on performances under assessment.*
- ***Performance Requirements:*** *specify formally mitigations/preventions provided.*

As the SPR template mentions, the OPA has to refer to any Operational Performance other than Safety, Security and Environment that have been addressed in other dedicated sections of the document. In this regard, the performance assessment methodology proposed here for SPR provides guidelines to obtain Performance Requirements (PRs) for performance areas not already investigated.

The presented technique can be considered as an optimization technique, since it takes on board concrete results of validation exercises and concept analysis and evaluating possible operational performance issues makes an evaluation of concept maturity and gaps respect to performance expectations and try to reduce gaps setting Performance Requirements

Thanks to this technique, the user can have a simple and schematic table which guides to set desired performance requirements aiming to overcome any operational performance issues identified. Moreover, it must be noted that once the requirements have been set, the process has not to be seen as concluded since it triggers the starting of a new cycle re-starting the OPA process in order to refine the concept developed until it achieves the desired performance level.

[8] The obtained performance requirements are presented into section 3 with the correct SJU format where is specified also the traceability to relevant interesting document as *OSED*, *VALR* or others.

A.4.2 Performing Operational Performance Assessment

To perform the OPA methodology for SPR, starting from the assessment of P5.6.1 Benefit Mechanism [48], KPAs under assessment must be selected.

In Step 1 P05.02 Validation Strategy [44], the OFA originally responsible for the OI related to CTA operations (OFA04.01.05 i4D+CTA) was required to provide results for the KPAs:

- Predictability
- Efficiency

It shall also be noted that in Step 1 P05.02 DOD [45] the only Performance Objective defined is related to Predictability for OFA 04.01.05.

However, the VALS [44] and DOD [45] were written when OFA04.01.05 existed as a standalone OFA. Now OFA 04.01.05 has been consolidated into the new OFA04.01.02 Enhanced Arrival and Departure management. This has had an impact on the KPAs to be addressed at OFA-level and in accordance with B04.01 material [46] the following KPAs are now to be addressed:

- Predictability (PRE)
- Environment/Fuel Efficiency (ENV)
- Airspace Capacity (TMA, En-route and Airport) (CAP)
- Cost Effectiveness (CEF)
- Safety (SAF)

P05.06.01 is developing and examining the use of the Controlled Time of Arrival (CTA) concept, which includes i4D, in an arrival management context with medium complexity and medium capacity. This corresponds to Operational Improvement (OI) TS-0103. Application of this OI is identified to have potential impact on (following ref 1):

- Predictability (PRE)
- Environment/Fuel Efficiency (ENV)
- Airspace Capacity TMA (CAP)

Within P05.06.01, CTA is not regarded as a specific (airspace) capacity enhancer. It is seen more as a possible method of providing better efficiency in arrival management, without a negative impact on (runway) capacity.

Validations done within the project have indicated that it seems possible to perform CTA operations, in a medium-density, medium-complexity environment, without reducing capacity.

Bearing in mind the previous explanation, for the SPR the OPA deals with:

- Predictability (PRE)
- Environment/Fuel Efficiency (ENV)

Note that the KPAs are considered according to definition provided in “The Performance Target D2” [49] document and B.04.01 [46].

Once selected the KPAs, brainstorming session, based on OSED and VALR contents, help to individuate a list of operational performance issues and sub-issues and their relative negative impact on the level of performance expectation. From a deep assessment of these impacts, it is possible to provide possible mitigations and/or preventions and then derive the associated Operational Performance Requirements.

The purpose of the *Operational Performance Assessment (OPA) for SPR* is to make a qualitative evaluation of working effectiveness and suitability of the CTA (and some selected i4D) functions.

Following this methodology, the sections below show the performance assessment developed for Predictability and Environment/Fuel Efficiency (ENV). Moreover, it is important to specify that the impacts described in the following sections are possible impacts to a solution scenario only, i.e. to a scenario in which the foreseen technology (CTA) is already applied. This means the impact is considered to be a decrease in the benefit of the solution scenario compared to the reference (baseline) one. The according issue will only decrease this benefit, but cannot lead to a situation worse than the reference scenario. This is because the fallback for all issues is a return (partly or wholly, for part or all of the fleet) to the reference scenario, in which the new technology (CTA) is simply not applied at all. Thus, if only impacts to the reference scenario were considered, there would not be any impact at all. The project has therefore decided to investigate the possible impacts to the solution scenario, i.e. impacts that will decrease the full possible benefit of the reference scenario.

Performance requirements are listed below in the table and reported in section 3.2.

A.4.3 OPA n°1 : Predictability

Predictability addresses the ability of the ATM system to ensure a reliable and consistent level of 4D trajectory performance. In other words: across many flights, the ability to control the variability of the deviation between the actually flown 4D trajectories of aircraft in relationship to the Reference Business Trajectory [49].The negative impact of this KPA must be seen when predictability decrease.

KPA	*Performance Issue*	*Performance Sub-Issue*	*Impact*	*Mitigation/Preventions*	*Performance Requirements*[9]
Predictability	1) CTA Time Function not available	1.a) AMAN itself fail	1.a) predictability decrease because CTA not available for any new aircraft coming into the sequence	1) No mitigation since the assumption is that AMAN works correctly (aircraft would be handled according to whatever measures were dictated at the time by the AMAN failure itself)	No additional REQs
		1.b) CTA calculation failure (even if the AMAN is working correctly)	1.b) predictability decrease because CTA not available for any new aircraft coming into the sequence	1.b.1) The ground system should provide an alert to advise ATCO that there is a failure in CTA calculation function. 1.b.2) New aircrafts arriving into the sequence should be handled by standard AMAN TTL/TTG procedures. 1.b.3) Those aircraft already operating to a CTA should be handled by standard CTA procedures	1.b.1) The ground system should provide an alert to advise ATCO in case of a failure in CTA calculation function. 1.b.2) In case of a failure in CTA calculation function, new aircrafts arriving into the sequence should be handled by applying regular AMAN advisories (e.g. TTL/TTG). 1.b.3) In case of a failure in CTA calculation function, those aircraft already operating to a CTA should be handled by standard CTA procedures.

[9] The obtained performance requirements are presented into section 3 with the correct SJU format where is specified also the traceability to relevant interesting document as OSED, VALR or others.

KPA	Performance Issue	Performance Sub-Issue	Impact	Mitigation/Preventions	Performance Requirements'
	2) INCORRECT CTA CALCULATION FUNCTIONS	2.a) CTA proposed not achievable	2.a) for one a/c minimum impact- if all a/c affected higher impact	2.a) the ground system should only propose CTA which is achievable	The ground system, taking into account aircraft capability, should only propose CTA which is achievable.
		2.b) CTA proposed not appropriate (e.g. CTA is not respecting spacing requirements)	2b) predictability decrease for aircrafts involved	2.b) system function must calculate a correct CTA for a correct sequence implementation	Ground system function must calculate a correct CTA for correct sequence implementation.
	3) RTA ACHIEVABILITY FOR A SINGLE A/C	3.a) RTA not available	3.a) minimum impact	3.a) No mitigation since minimum impact	No additional REQs
		3.b) RTA assessed as not achievable	3.b) minimum impact	3.b) No mitigation since minimum impact	No additional REQs
		3.c) RTA agreed but then not achievable	3.c) minimum impact	3.c) No mitigation since minimum impact	No additional REQs
		3.d) RTA agreed but then not respected	3.d) for one a/c minimum impact- if several a/c affected higher impact	3.d.1) The air and ground system shall monitor the achievability of the agreed CTA [traceability REQ-05.06.01-OSED-SG07.0200] 3.d.2) The air and ground HMI shall display alerts in case the agreed CTA is not respected [traceability REQ-05.06.01-OSED-SG07.0300] 3.d.3) In case an i4D-aircraft does not respect an agreed CTA, it shall provide an updated EPP [traceability REQ-05.06.01-OSED-SG07.0400]	3.d.1) The air and ground system shall monitor the achievability of the agreed CTA. 3.d.2) The air and ground HMI shall display alerts in case the agreed CTA is not respected. 3.d.3) In case an i4D-aircraft does not respect an agreed CTA, it shall provide an updated EPP.
	4) OPERATIONAL CIRCUSTANCIES THAT MAKE CTA TO BE CANCELLED		4) predictability decrease	4.a) controller tools may mitigate against cancellation for traffic spacing	Controller tools may mitigate against cancellation for traffic spacing.

Table 27: OPA 1: Predictability

A.4.4 OPA n°2 : Environment

The fuel-benefit of the CTA concept has been demonstrated for the individual aircraft that is assigned a CTA and is allowed to self-manage its descent profile and speed to meet the constraint in the most fuel efficient way. However, and as explained earlier in the document and in the OSED, even in a 100% equipage CTA operations environment, it is expected that it will not be feasible that not all aircraft in a sequence are managed by CTA, and it is therefore necessary to consider the impact of the concept in the overall fuel-burn in a traffic scenario (including aircraft handles with CTA as well as those that can't be handled with CTA). Validation activities have evaluated this overall impact on fuel burn of CTA operations and have found no evidence of it being negative.

The following table examines the operational issues that affect the potential for CTA to enable fuel savings for individual flights.
Aviation has a diverse impact on the environment, but not all aspects can be influenced by the ATM system. The Environmental sustainability addresses the role of ATM in the management and control of environmental impacts. The aims are to reduce adverse environmental impacts (average per flight); to ensure that air traffic related environmental considerations are respected; and, that as far as possible new environmentally driven non-optimal operations and constraints are avoided or optimised as far as possible. This focus on environment must take place within a wider "sustainability" scope that takes account of socio-economic effects and the synergies and trade-offs between different sustainability impacts. This KPA is affected by the same operational issues of predictability but the negative impact must be seen when the fuel burn increase [49].

KPA	*Performance Issue*	*Performance Sub-Issue*	*Impact*	*Mitigation/Preventions*	*Performance Requirements*[10]
Environmental Sustainability	1) CTA Time Function not available	1.a) AMAN itself fail	1.a) fuel burn increase because CTA not available for any new aircraft coming into the sequence. Vectoring and speed adjustment procedures are needed.	1) No mitigation since the assumption is that AMAN works correctly (aircraft would be handled according to whatever measures were dictated at the time by the AMAN failure itself)	No additional REQs
		1.b) CTA calculation failure (even if the AMAN is working correctly)	1.b) fuel burn increase because CTA not available for any new aircraft coming into the sequence	1.b.1) The ground system should provide an alert to advise ATCO that there is a failure in CTA calculation function. 1.b.2) New aircrafts arriving into the	1.b.1) The ground system should provide an alert to advise ATCO in case of a failure in CTA calculation function. 1.b.2) In case of a failure in

[10] The obtained performance requirements are presented into section 3 with the correct SJU format where is specified also the traceability to relevant document as *OSED*, *VALR* and other interesting documents (these references are useful to justify the assessment conducted at SPR level).

KPA	Performance Issue	Performance Sub-Issue	Impact	Mitigation/Preventions	Performance Requirements[10]
				sequence should be handled by standard AMAN TTL/TTG procedures. 1.b.3) Those aircraft already operating to a CTA should be handled by standard CTA procedures	CTA calculation function, new aircrafts arriving into the sequence should be handled applying regular AMAN advisories (e.g. TTL/TTG). 1.b.3) In case of a failure in CTA calculation function, those aircraft already operating to a CTA should be handled by standard CTA procedures.
	2) Incorrect CTA calculation functions	2.a) CTA proposed not achievable	2.a) for one a/c minimum impact- if all a/c affected higher impact	2.a) the ground system should only propose CTA which is achievable	The ground, taking into account the aircraft capability, system should only propose CTA which is achievable.
		2.b) CTA proposed not appropriate (e.g. CTA is not respecting AMAN spacing requirements)	2b) fuel burn increase for aircrafts involved	2.b) system function must calculate a correct CTA for a correct sequence implementation	Ground system function must calculate a correct CTA for correct sequence implementation.
	3) RAT achievability for a single a/c	3.a) RTA not available	3.a) minimum impact	3.a) No mitigation since minimum impact	No additional REQs
		3.b) RTA assessed as not achievable	3.b) minimum impact	3.b) No mitigation since minimum impact	No additional REQs
		3.c) RTA agreed but then not achievable	3.c) minimum impact	3.c) No mitigation since minimum impact	No additional REQs
		3.d) RTA agreed but then not respected	3.d) for one a/c minimum impact- if several a/c affected higher impact	3.d) OSED req:07.0200/07.0300/07.0400	3.d.1) The air and ground system shall monitor the achievability of the agreed CTA. 3.d.2) The air and ground HMI shall display alerts in case the agreed CTA is not

KPA	Performance Issue	Performance Sub-Issue	Impact	Mitigation/Preventions	Performance Requirements[10]
					respected. 3.d.3) In case an i4D-aircraft does not respect an agreed CTA, it shall provide an updated EPP.
	4) Operational circumstancies that make CTA to be cancelled		4) fuel burn increase	4.a) controller tools may mitigate against cancellation for traffic spacing	Controller tools may mitigate against cancellation for traffic spacing.

Table 28: OPA 1: Environment

Appendix B Accident Incident Model for Mid Air Collision

Because of the CTA operations start in En-Route and terminate after the CTA fix situated into the TMA space, the barrier model used for the Safety Assessment are the ones for Mid-Air Collision both in En-Route and TMA environments. They can be summarized as presented in Figure 16 developed by P16.1.1 and presented into SRM Guidance Material [29]:

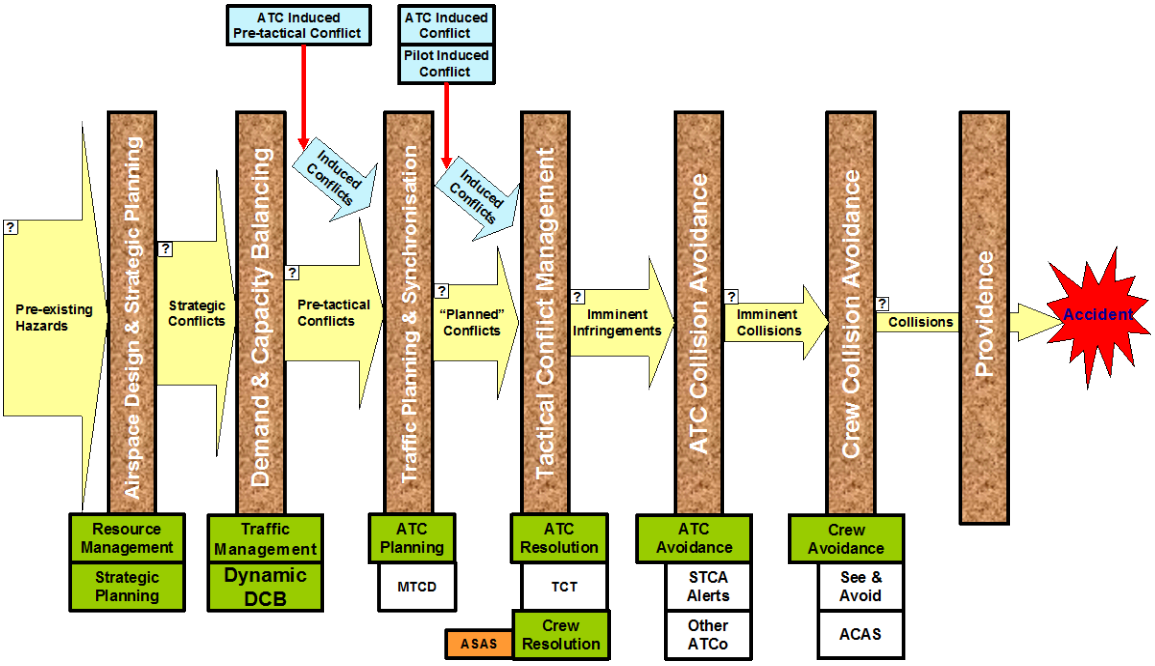

Figure 16: MAC model from AIM

The mentioned models can be detailed as in sections below.

B.1 En-Route

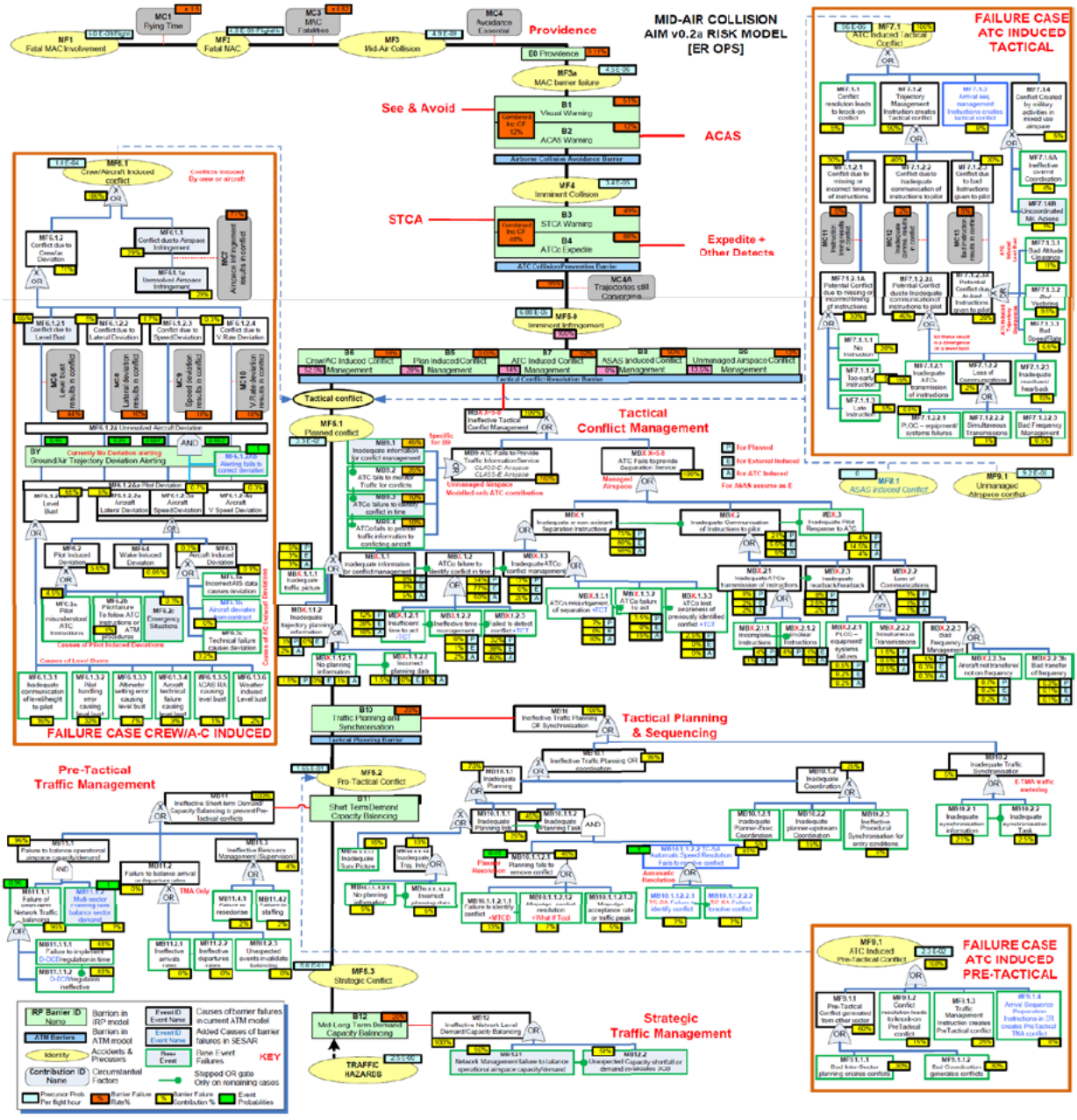

Figure 17: AIM model Mid-Air Collision En-Route

B.2 TMA

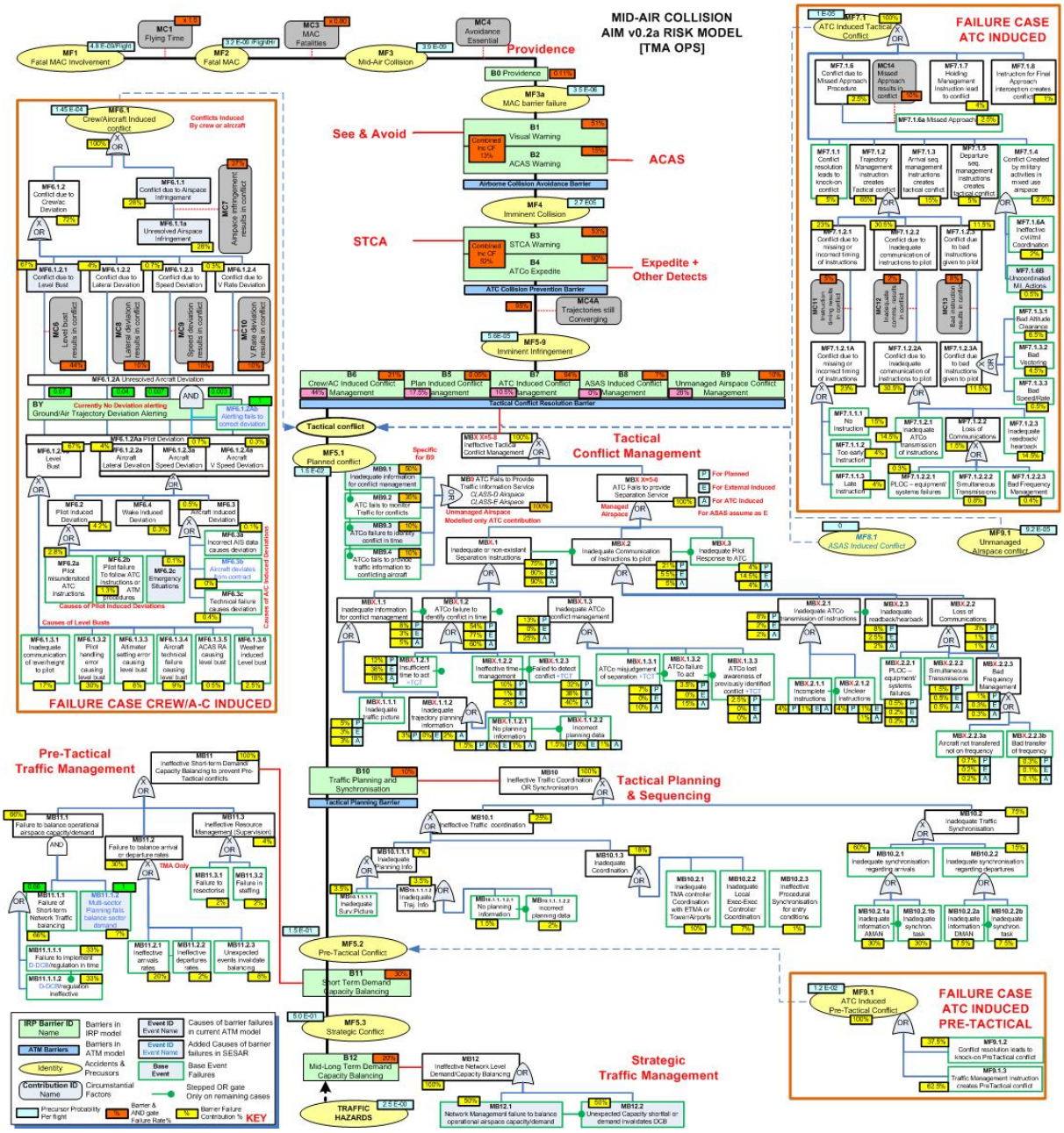

Figure 18: AIM model Mid-Air Collision in TMA

Appendix C Functional Blocking breakdown from Technical Architecture Description - Cycle 2015 [61]

The functional analysis has been performed on the basis of operational requirements from projects 4.3, 4.5, 4.7.1, 4.7.2, 4.8.1, 5.6.1, 5.6.4, 5.6.6, 6.8.1, 6.8.4 and 7.5.2. Corresponding technical specifications from projects 10.2.1, 10.2.5, 10.3.2, 10.4.1, 10.4.3, 10.4.4, 10.5.1, 10.7.1, 10.8.1, 10.9.1, 10.9.2 and 10.9.4 were reviewed.

The purpose of the functional decomposition is to provide a common structure for the specification of technical requirements by the WP10 primary projects, which will then facilitate the assurance of completeness and consistency of specifications and the eventual consolidation of requirements.

As such, this can be considered a “generic logical decomposition” and no inference shall be made as to the actual physical implementation. Similarly, where data-flows are identified between functional blocks, their purpose is to clarify the scope of the functional blocks, their inter-relationships and to provide a level of validation of the requirements. However, these do not currently indicate the standardisation of internal exchanges, as only external exchanges at the domain systems level are currently viewed as needing to be commonly provided – i.e. standardised.

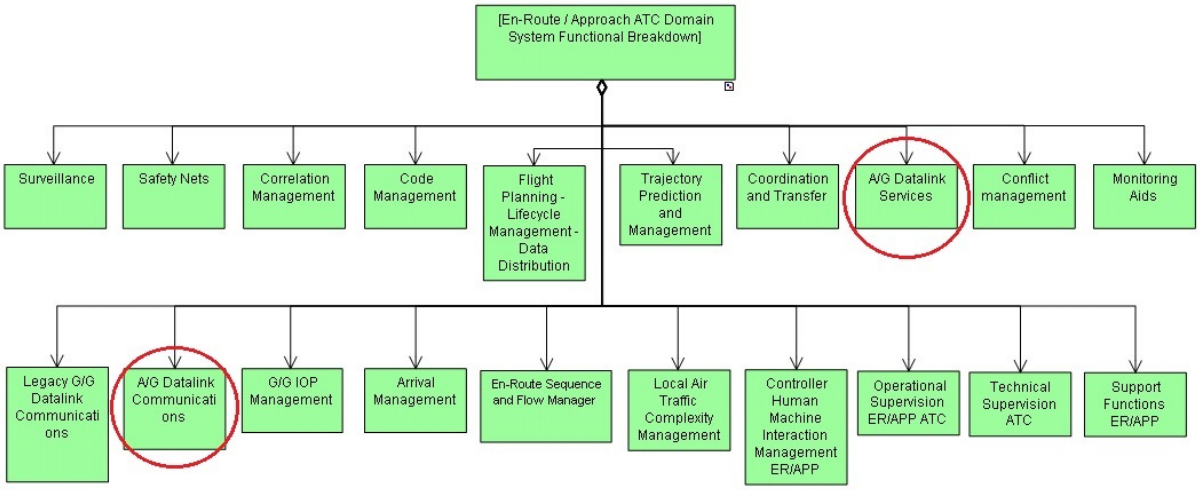

Figure 19: Functional Block Tree Diagram from EATMA

The **Air-Ground Datalink Communication** functional block comprises the communication function that provides the means to exchange air-ground datalink communication and surveillance messages through standardised datalink communication protocols, relayed by external air-ground data communication networks (i.e. the ATN and/or the ACARS networks).

The **Air-Ground Datalink Services** functional block provides the air-ground datalink services and applications:

- DLIC Service based on the CM Application (AFN Application for ACARS);
- Services based on the CPDLC Application: ACM, ACL, AMC, 4DTRAD, etc.);
- Services based on ADS-C application:

- Uplink of contract requests to the aircraft
- Consistency checks between downlinked data and ground data (e.g. 2D route check) and dissemination of the corresponding inconsistency notifications if any
- Dissemination of the downlinked data to subscribers, including TP&M for synchronisation of the ground and air trajectories.

Appendix D Additional Considerations

The following recommendations have to be considered out of the scope of this Project 05.06.01. They have been developed during the brainstorming and assessment sessions of the *Ground & Airborne Capabilities to Implement Sequence based on the Controlled Time of Arrival (CTA)* activities. In consideration of the operational competences and of the processes that have stimulated the initial definition of this recommendations and, step by step, their final specification, the aim of this Appendix D is to record additional considerations that could represent useful inputs for future projects related to similar scopes.

Recommendation	When assessing whether a CTA can be proposed for a flight, AMAN shall consider factors such as known G/G latency, and other relevant factors, as required.
Title	G/G transmission latency (to/and from AMAN unit) in CTA proposal process
Rationale	To provide a known g/g latency figure to be considered by AMAN within the CTA assessment process

Recommendation	The probability of loss of G/G communication shall not exceed 5E-05 / SOH.
Title	Probability of loss of G/G communication
Rationale	Fault tree analysis

Recommendation	The probability of systematic excessive latency in G/G transmission, making the CTA not within the ETA min-max window shall not exceed 1E-05 / SOH (Sector Operating Hour). [Sg05.0600]
Title	Probability of systematic excessive latency in G/G transmission,
Rationale	Fault tree analysis

Requirement	Ground/ground communication systems of ATSU_DEST and ATSU_CONTROL shall be able to respectively transmit and receive the CTA in a ground/ground message in a timely manner.
Title	Ground/ground communication completion in a timely manner
Status	<Validated>
Rationale	CTA related messages should be transmitted and received in a timely manner to avoid unachievable CTA's being proposed, or to minimise CTAs being proposed and then cancelled/missed because of alterations to the trajectory
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Test>

-END OF DOCUMENT-