Step 1 Final SPR

Document information	
Project Title	Co-Operative Planning in the TMA
Project Number	05.04.02
Project Manager	DFS
Deliverable Name	Step 1 Final SPR
Deliverable ID	D05
Edition	00.01.03
Template Version	03.00.00
Task contributors	
DFS Deutsche Flugsicherung GmbH	

Abstract

This document presents Safety, Performance and Interoperability Requirements for the Operational Improvement Step TS-0303 "Arrival Management into Multiple Airports" (SESAR Solution #08) on operational level that have been developed to full V3 maturity within SESAR Step 1 as part of OFA04.01.02. It is based on a safety assessment documented in the embedded Safety Assessment Report. It further draws from outcome of two of validation exercises executed in project 05.04.02.

In case of a multi-airport TMA, the capabilities of present AMAN systems are not sufficient to cope with the complexity of traffic and airspace. To avoid spontaneous increases in complexity and thus workload in the E-TMA ACC sectors, an extension to the AMAN concept that helps to prevent overload in sectors with converging inbound flows has been investigated. The extended AMAN horizon (SESAR Solution #05) has been identified as an important environment element in which this solution shall be deployed, consequently both SAR and SPR build upon the work of projects 05.06.04 and 05.06.07.

Authoring & Approval

Prepared By - *Authors of the document.*		
Name & Company	Position & Title	Date
[redacted] DFS	[redacted]	04/03/2016

Reviewed By - *Reviewers internal to the project.*		
Name & Company	Position & Title	Date
[redacted] NATS	[redacted]	16/03/2016
[redacted] DFS		04/03/2016

Reviewed By - *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date
[redacted] NATS	[redacted]	No feedback received
[redacted] DFS		15/03/2016
[redacted] SOPRA STERIA		No feedback received
[redacted] Thales		No feedback received
[redacted] Thales		No feedback received
[redacted] Germanwings		22/03/2016
[redacted] Airbus		17/03/2016
[redacted] Enaire		21/03/2016
[redacted] EUROCONTROL		No feedback received
[redacted] EUROCONTROL (Winsland)		16/04/2016

Approved for submission to the SJU By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
[redacted] DFS	[redacted]	22/03/2016
[redacted] NATS		23/03/2016
[redacted] EUROCONTROL		16/03/2016

Document History

Edition	Date	Status	Author	Justification
00.00.01	27/10/2015	Draft	[redacted]	Initial Draft
00.00.20	04/03/2016	Draft		Draft for external review
00.01.00	22/03/2016	Final		Updated after external review
00.01.01	19/05/2016	Final		Updated after SJU assessment
00.01.02	10/06/2016	Final		E-AMAN Req. only referenced
00.01.03	28/06/2016	Final		Ch. 2 updated after SE#3 review

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

List of tables

List of figures

Executive summary

This document presents Safety, Performance and Interoperability Requirements for the Operational Improvement Step TS-0303 “Arrival Management into Multiple Airports” (SESAR Solution #08) on operational level that have been developed to full V3 maturity within SESAR Step 1 as part of OFA04.01.02. It is based on a safety assessment documented in the embedded Safety Assessment Report having applied SESAR Safety Reference Methodology under guidance from P16.06.01 safety experts. It further draws from outcome of two of validation exercises executed in project 05.04.02.

In OFA level coordination it was agreed that this SPR / INTEROP activity should restrict itself to a purely operational view; as per the SESAR framework the work is to be continued by technical projects.

The extended AMAN horizon (SESAR Solution #05) has been identified as an important environment element in which this solution shall be deployed, consequently both SAR and SPR build upon the work of projects 05.06.04 and 05.06.07. For completeness, the relevant requirements of Solution #05 are listed as reference in the Appendix.

While there are AMAN solutions available for a foresighted, cross-sectorial arrival planning, the current capabilities of these AMAN systems are not sufficient for the complexity of traffic and airspace structure of this extended TMA with converging inbound streams. The main issue of such a multi-airport TMA is the small size of the TMA sectors and their adjacent en-route sectors which does not allow the controllers to implement sufficient TTL without both a drastic increase in workload and decrease of flight efficiency. Additionally, despite proper network flow management measures based on average traffic count within 20min intervals of a predefined traffic volume, bunching can occur. If this happens simultaneously and traffic streams converge, spontaneous overload situations can be the consequence. To prevent this from happening, capacity buffers must be kept and thus the available airspace capacity is not fully utilized. This in turn can lead to situations where the E-TMA sector becomes the bottleneck of the multi-airport TMA and thus runway capacity is not fully utilized, too.

Therefore, an additional arrival planning component “Center Manager” (CMAN) which accompanies the AMANs of the individual airports was developed. The system generates a combined planning for several arrival streams into different airports by calculating the sequence of aircraft flying towards an area in the E-TMA en-route sector where their routes intersect. By imposing an adequate spacing of the aircraft in that area (“sector flow”), a time-to-lose (TT)L for the appropriate upstream ACC sector is calculated to meet this constraint. The controller in the upstream sector will be presented with the superimposed TTL from the AMAN and the CMAN, i.e. the highest amount of necessary TTL of either AMAN or CMAN will be shown. In the en-route sectors adjacent to the TMAs which do not serve both airports, TTL based on runway capacity is presented to the controllers.

It is expected that the results of this Solution will have relevance for many areas of Europe that have complex E-TMAs serving several airports within close proximity (e.g. Düsseldorf/Cologne, Madrid, Paris, London), and that it could also support flow control measures in regions with complex traffic interactions (e.g. French – German Border and Switzerland).

1 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 by P05.04.02 D04 “Step 1 Final OSED – Volume 2: TS-0303” [14]. The SPR also provides their allocation to Functional Blocks. They shall identify the requirements needed to fulfil each KPA and include, or reference, the sources justifying those requirements.

1.2 Scope

This document supports the operational service and concept elements identified in the Operational Service and Environment Definition (OSED), [14]. This service is expected to be operational (IOC) in the 2020-2024 time-frame according to DS 15 and are representing SESAR Solution #08.

As this solution makes use of the AMAN extended horizon concept it relies heavily on SESAR Solution #05 as documented in the P05.06.07 OSED [15] and is based on both related SAR and SPR [16].

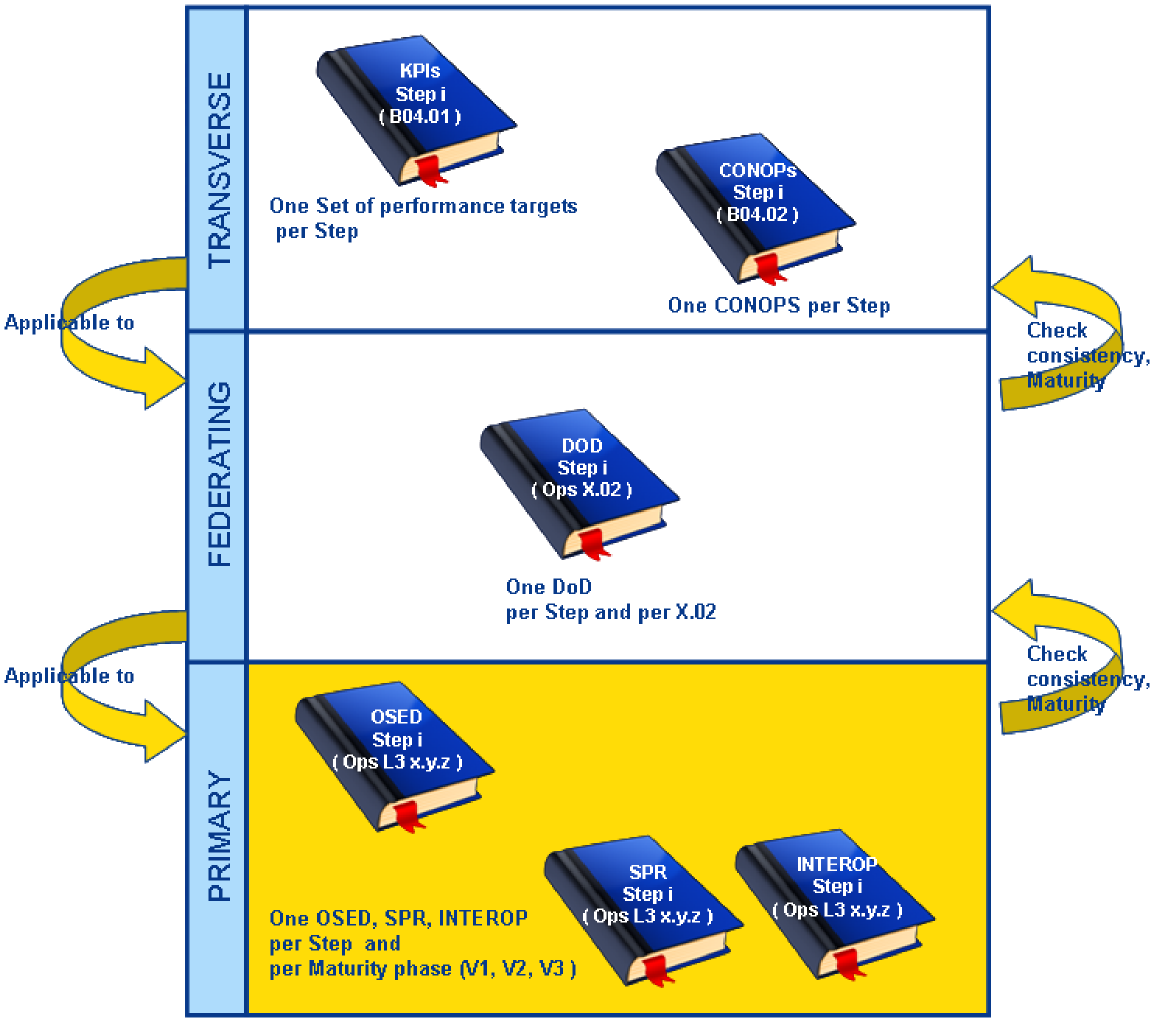

Figure 1: SPR document with regards to other SESAR deliverables

In Figure 1, the Steps are driven by the OI Steps addressed by the project in the Integrated Roadmap document [13].

1.3 Intended readership

The intended audience of this document consists of both the related operational and technical projects as well as OFA & Sub-Workpackage Leads and the transversal projects:

OFA 04.01.02 Lead

SWP 5.2 Project Leader

P 05.06.07 Project Manager

10.9.2 Project Manager

10.09 Lead

16.06.01

B05

10.01.07 Project Manager

1.4 Structure of the document

This document follows the SESAR SPR template. The structure is as follows:

- **Chapter 1:** Provides general information about the document.
- **Chapter 2:** Provides a summary of the operational concept described in P05.04.02 Step 1 OSED – Volume 2 [14].
- **Chapter 3**: Provides the performance and safety requirements of solution #08.
- **Chapter 4:** Provides the list of both applicable and referenced documents.
- **Appendix A:** Provides the Safety and Performance Assessments
- **Appendix B:** Provides a reference to the original E-AMAN / solution #05 requirements relevant to solution #08

1.5 Background

As this solution makes use of the AMAN extended horizon concept it relies heavily on SESAR Solution #05 as documented in the related SPR [16].

Additionally, a continuous coordination with P05.06.07 and P16.06.01 was established and useful to identify the potential safety impacts of solution #08 and to align the approach on the safety assessment.

1.6 Glossary of terms

n/a

1.7 Acronyms and Terminology

Term	Definition
AAH	Active Advisory Horizon
A/C	Aircraft
AC#	Abnormal Condition

Term	Definition
AIM	Accident-Incident Model
AMA	Arrival Message
AMAN	Arrival Manager (Equipment)
ANSP	Air Navigation Service Provider
APP	Approach (control sector/position)
APR	Automatic Position Report(-ing)
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATM	Air Traffic Management
ATSU	Air Traffic Service Unit
ATSU DEST	ATSU Destination
CFMU	Central Flow Management Unit
CMAN	Center Manager
CNS	Communication, Navigation, Surveillance domains of the ATM system
COTR	Coordination and Transfer (equipment)
CTA	Controlled Time of Arrival
CWP	Controller Working Position
DCB	Dynamic Capacity Balancing
DMAN	Departure Manager
DOD	Detailed Operational Description
E-AMAN	Extended AMAN
EATMA	European ATM Architecture
EH	Eligibility Horizon
ENR	En-route
ENT	Entity
E-OCVM	European Operational Concept Validation Methodology
E-R	En-route (in AIM context)
ETA	Estimated Time of Arrival

Term	Definition
EXE	Executive controller
EXE-nnn	SESAR Validation Exercise VP-nnn
FCN	Function
FDPS	Flight Data Processing System
FH	Flight Hour *also styled as flt hr*
FHA	Functional Hazard Analysis
FIR	Flight Information Region
FL	Flight level
FM	Functional Model
FPL	Flight plan
FTA	Fault Tree Analysis
HAZID	Hazard Identification
HF	Human Factor(s)
HFTA	Hybrid Fault Tree Analysis *also styled as H-FTA*
HMI	Human Machine Interface
HP	Human Performance
ICAO	International Civil Aviation Organisation
IE	Information Exchange
IFR	Instrument Flight Rules
IMH	Initial Metering Horizon
IMP	Initial Metering Point
INTEROP	Interoperability Requirements
MAC	Mid-Air Collision, type of AIM
MET	Meteorological information (data source)
MM	Mitigation Means
MP	Metering Point
MTFoO	Maximum Tolerable Frequency of Occurrence

Term	Definition
NM	Nautical Mile
OFA	Operational Focus Area
OH#	Operational Hazard
OI	Operational Improvement (Step)
OLDI	On-Line data Interchange
OSED	Operational Services and Environment Description
PLN	Planning controller
RT	Radio Telephony *also styled as R/T*
RTA	Required Time of Arrival
RWY	runway
SAC	SAfety Criteria
SAR	Safety Assessment Report
SDPS	Surveillance Data Processing System
SEQ_MAN	Sequence Manager (role)
SERA	Standardized European Rules of the Air
SESAR	Single European Sky ATM Research Programme
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SO#	Safety Objective
SO# (F&P)	Safety Objective – Functionality and Performance (Success approach) *also styled as F&P SO#*
SOH	Sector Operating Hour
SPR	Safety and Performance Requirements
SR	Safety Requirement
SR (F&P)	Safety Requirement – Functionality and Performance (Success approach)
SRC	Data source
SRM	SESAR Safety Reference Material
STAR	Standard Arrival Route
SWIM	System-Wide Information Management

Term	Definition
TMA	Terminal (Manoeuvring) Area
TOBT	Target Off Block Time
ToD	Top of Descent
TP	Trajectory Predictor (or Prediction)
TSA	Temporary Segregated Airspace/Area
TTG	Time to Gain
TTL	Time to Lose
VALS	Validation Strategy
VFR	Visual Flight Rules
WIA	Wake Induced Accident
WVE	Wake Vortex Encounter
WX	weather

2 Summary of Operational Concept (from OSED)

This chapter provides a brief summary of the operational concept described in P05.04.02 Step 1 OSED – Volume 2 [14].

2.1 Description of the Concept Element

The Queue Management process is presented with traffic that is the result of Network Management processes and as such is dependent on the quality of that traffic. If the traffic delivery is significantly higher that the capacity of the resource (normally a runway) there is limit to what queue management can achieve. However, if presented with traffic that is reasonably balanced with capacity, tactical queue management can:

- assist in providing more efficient trajectories for Airspace Users by absorbing delay at more efficient altitudes thereby reducing fuel burn.
- improve the predictability of traffic delivery to the TMA;
- provide a traffic delivery that is optimised for wake vortex sequencing, thereby increasing runway throughput
- improve the organisation of the traffic delivery to the TMA, thereby decreasing TMA controller
  workload whilst minimising any increased task load on upstream sectors

The main method of achieving these aims is by earlier planning of arrival (and related departure) operations.

Although there are AMAN solutions available for a foresighted, cross-sectorial arrival planning, the current capabilities of these AMAN systems are not sufficient for the special case of a multi-airport environment where numerous arrival- and departure streams are handled to the various airports in close vicinity. The main issue of such a multi-airport environment is the small size of both the TMA sectors and their adjacent en-route Extended-TMA sectors which does not allow the controllers to implement sufficient TTL without both a drastic increase in workload and decrease of flight efficiency.

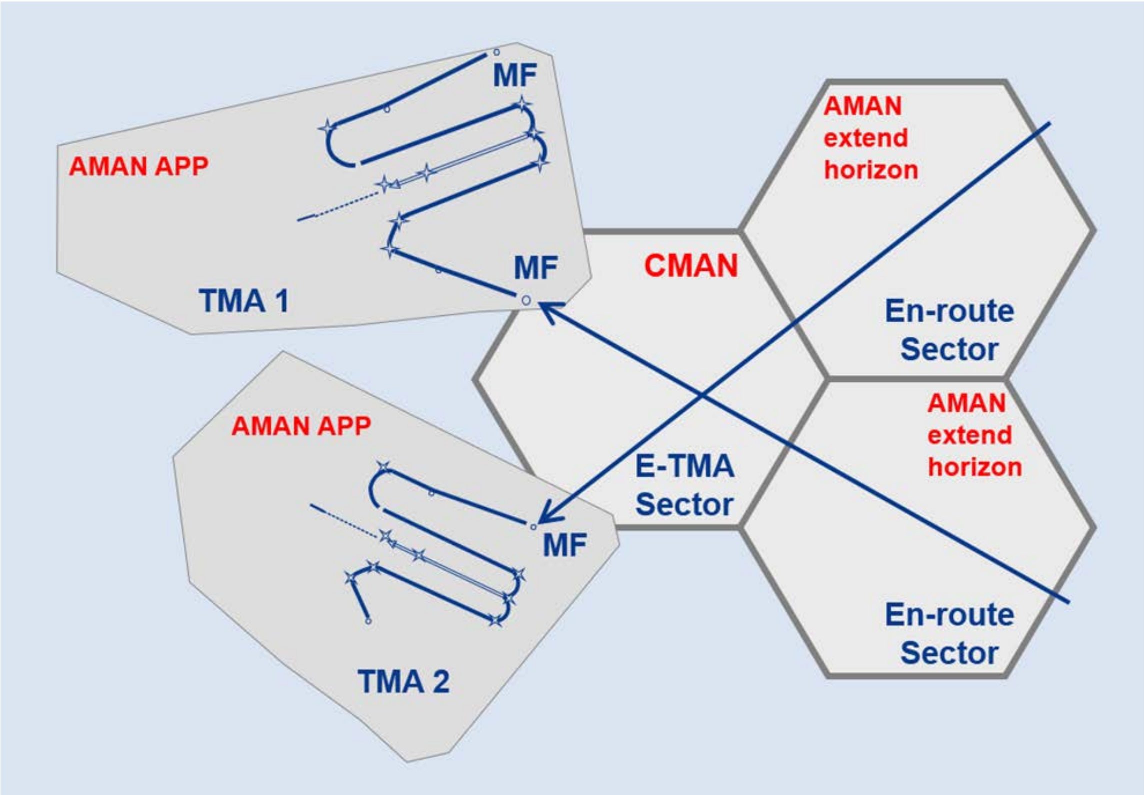

Figure 2: Extended TMA with multiple airports and AMAN extended horizon

Therefore, an additional arrival planning component “Center Manager” (CMAN) which accompanies the AMANs of the airports was developed. It aims to support coordination of traffic flows into multiple airports in the same vicinity to enable smooth delivery to the runways and enable the controller to manage the interaction of flows in an efficient way without overload situations.

The system generates a combined planning for several arrival streams into different airports by calculating the sequence of aircraft flying towards an area in an E-TMA en-route sector where their routes intersect. By imposing an adequate spacing of the aircraft in that area (“sector flow”), a TTL for the appropriate upstream ACC sector is calculated to meet this constraint. The controller in the upstream sector will be presented with the superimposed TTL from the AMAN and the CMAN, i.e. the highest amount of necessary TTL of either AMAN or CMAN will be shown. In the en-route sectors adjacent to the TMAs which do not serve both airports, TTL based on runway capacity is presented to the controllers. Thus, CMAN allows timely avoidance of traffic bunching in the E-TMA sectors.

Both E-TMA and upstream ACC ATCOs consider the arrival sequence information and advisory in order to absorb delay as follows:

- Upstream ACC:
  Speed reduction, less directs, earlier descent instructions. Path stretching and orbital holding are excluded;
- E-TMA:
  Speed reduction, path stretching, instruct or suspend directs; orbital holding is performed only if TMA holdings are full, and will be taken over by APP ATCO.

With the help of solution #08 the E-TMA sectors will obtain more homogenous traffic flows from upstream ACC sectors which in turn enables the E-TMA sectors to provide the TMA sectors with optimal arrival sequences according to AMAN.

2.2 Description of Operational Services

The processes / services are developed and updated within EATMA. The relevant process model is “Synchronize Traffic” and “Update Arrival Sequence in Multi-Airport Environment”.

Although the EATMA Portal is now the authoritative source, process models are included in this document for the purposes of both ensuring readability of the concept within one document, and also of ensuring that the models are available to view in their entirety even for readers who may not be familiar with navigating the EATMA portal.

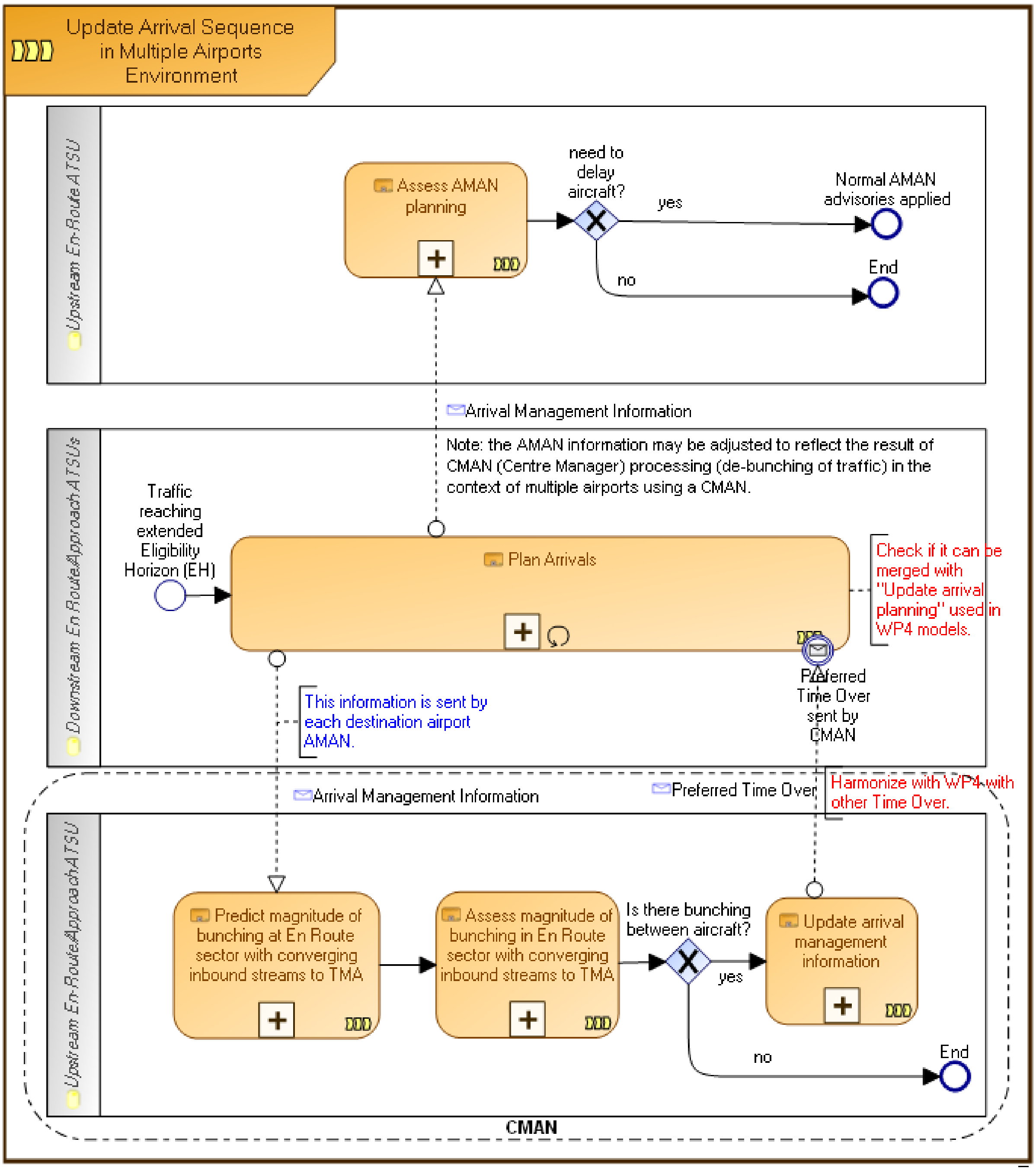
Update Arrival Sequence in Multiple Airports Environment
Upstream En-Route ATSU
Assess AMAN planning
need to delay aircraft?
yes
Normal AMAN advisories applied
no
End
Arrival Management Information
Downstream En Route/Approach ATSUs
Note: the AMAN information may be adjusted to reflect the result of CMAN (Centre Manager) processing (de-bunching of traffic) in the context of multiple airports using a CMAN.
Traffic reaching extended Eligibility Horizon (EH)
Plan Arrivals
Check if it can be merged with "Update arrival planning" used in WP4 models.
Preferred Time Over sent by CMAN
This information is sent by each destination airport AMAN.
Arrival Management Information
Preferred Time Over
Harmonize with WP4 with other Time Over.
Upstream En-Route/Approach ATSU
Predict magnitude of bunching at En Route sector with converging inbound streams to TMA
Assess magnitude of bunching in En Route sector with converging inbound streams to TMA
Is there bunching between aircraft?
yes
Update arrival management information
no
End
CMAN

Figure 3: Process Model – Update Arrival Sequence in Multiple Airport Environment (TS-0303)

2.3 Description of Operational Environment

It is recognised that the SESAR TMA concept will not be a “one size fits all” solution; rather, various TMA types are identified, each with their respective operational characteristics. SWP 5.2 has used the TMA characterisation identified by TMA 2010+ as a baseline. These characterisations are based on the constraining factor identified for any given TMA. It is assumed that an unconstrained TMA does not exist. Although a TMA may not have immediate constraints which result in major capacity or efficiency reductions, these TMAs will at a low level have some constraining factor which will appear in extreme circumstances. Therefore, every TMA will be able to identify with one or more of the identified constraining factors, the blend of which will make up each TMA type.

The TMA characterisation proposed by TMA 2010+ are:

- Environmentally Constrained TMA
- Airspace Constrained TMA
- Traffic Volume and Variation Constrained TMA
- Airfield Interaction Constrained TMA
- ATC Staff or Equipment Constrained TMA

These are the 5 types of Operational Environment. Each TMA can be considered as a composition of one of more of these Operational Environment types.

These TMA characteristics describe the main constraining factor to that environment. There is an additional variable of *complexity level* to also be considered. Complexity is specific to each TMA regardless of the constraining group it lies in and can be a function of any or a mixture of the following factors:

Airspace

- Number of airfields
- Number of runways
- Number of entry points
- Number of arrival/departure streams to be merged or separated and their interaction
- Presence of small angle crossing point(s) – that is, where two flows of traffic cross at a small angle, not a right angle
- Proximity of crossing/conflict/merge point(s) to the TMA boundary
- TMA at FIR boundary (so traffic handed to/from neighbouring FIR)
- Number of holding areas in use (e.g. stacks, path-stretch)
- Lack of space for vectoring, path stretching or holds

Traffic Characteristics

- Amount of traffic
- Callsign confusion
- Mix of traffic types (e.g. wake vortex category/speed/manoeuvrability), leading to sequencing or metering problems
- Mix of aircraft equipage or traffic type (e.g. civil/military) leading to different handling procedures
- Need for many heading changes/vectoring/level changes (e.g. for de-confliction, over and above the normal turning onto base and final)
- Lack of predictability of traffic (e.g. when avoiding weather, windshear)

Air Traffic Operations

- Amount of non-standard traffic (e.g. police, survey, hospital, state flights, flights requiring special co-ordination)
- Amount of flights not meeting standing agreements/Flight Level allocations so requiring co-ordination
- R/T frequency congestion

Weather

- Significant weather occurrences: de-icing, low visibility, convective activity, cross-winds, strong head-wind, extreme heat
- Variations in weather leading to differing airspace structures, procedures.

The operational environment considered to benefit most from solution #08 is an Extended-TMA consisting of several airports with a blend of the following two, generic characteristics:

1) **Airspace Constrained TMA**

   The Airspace Constrained TMA is characterised by its size and shape which is determined by the surrounding sectors or physical constraints. The TMA is often made to fit in between the existing en-route, airport and military airspace, rather than being specifically designed from a TMA perspective. The size and shape of the TMA has an impact on the space and time available for TMA controllers to affect the flights. The greater the number of abutting sectors to the TMA the more handovers that need to be performed.

   Due to the high number of abutting sectors this airspace is likely to be highly complex with a high number of structured routes. These routes have probably developed over time as a result of circumstance and may include some PBN routes introduced to manage complexity. The airspace has evolved over time to meet changing demands, but has not been proactively designed as a TMA leading to highly tactical day to day operations.

2) **Airfield Constrained TMA**

   The Airfield Constrained TMA is characterised by having a number of airfields providing a mix of aircraft types. Particular complications arise due to aircraft being in different phases of flight (i.e. arrivals and departures) and capable of differing performance.

   Simply having a large number of airfields in close proximity is not a complexity factor itself. It is conceivable that all of the airports could have similar demands and common approaches. However, because the airports normally work autonomously and have no coordination with each other this can lead to conflicts within the TMA.

   The level of complexity increases with the combination of the relative positioning of each of the airfields, the capacity of each of the airfields and the mix of aircraft frequenting each airport.Due to the proximity of airfields in this TMA it is likely to be highly complex due to a number of interacting SIDs and STARs.

The defining characteristics of the target environment are in particular:

- Two airports in close vicinity but with individual TMAs / transitions.
- One or more E-TMA en-route sectors adjacent to both airports
- Size, route structure and traffic complexity of this / these E-TMA sector(s) does not allow for sufficient delay absorption to provide the TMAs with proper AMAN sub-sequences at the individual metering-fixes.
- Despite solution #05 “AMAN with extended horizon” for *single* airports will already be deployed it cannot be successfully utilized in this particular environment consisting of *multiple* airports without solution #08.

On the other hand, this solution #08 does not target operational environments where for example:

- The airports are several hundred miles apart and only the edges of their AMAN horizons overlap.
- The airports are only a view miles apart, thus all arrivals share a common sequence on final.

However, it is accepted that different airspace configurations with different levels of traffic density and complexity might make use of solution #08 in different ways. It is entirely possible that some combinations of traffic density and airspace configuration will not require or enable the use of solution #08 at all.

3 Requirements

This section describes the safety and performance requirements. The SPR requirements show traceability to the operational requirements (applicable to Processes and Services (P&S)) as described in the OSED.

The numbering scheme follows the example of 05.06.07. Following the well-established practice of referencing relevant requirements from other projects / solutions, this Appendix B also contains references with their original identifier to E-AMAN requirements 05.06.07 inherited from 05.06.04 that are applicable for solution #08.

Base string: REQ-05.04.02-SPR-0005.XXXX

Block ranges for XXXX:

0001 through 0099	Safety requirements derived in SAR success approach
0100	Reserved
0101 through 0199	Safety requirements derived in SAR failure approach
0200	Reserved
0201 through 0299	Performance requirements
0300	Reserved
0347	Is included in the group of safety requirements derived in SAR success approach.
0400	Reserved
0401 through 0499[1]	New CMAN Requirements

3.1 Operational Service "Update Arrival Sequence in Multi Airport Environment"

3.1.1 Safety Requirements

Note: Following requirements contain likelihood figures that may require further consolidation during implementation. Validation results do not refine the expressed needs further. Figures have been achieved by expert assessment.

[REQ]

Identifier	REQ-05.04.02-SPR-0005.0101
Requirement	The likelihood of E-AMAN being not available or unserviceable shall be no more than 2e-4 SOH, approximately once every 7 months.
Title	E-AMAN unserviceable
Status	<Validated>
Rationale	D05-001-SAR-SR-101; E-AMAN Requirement REQ-05.06.04-SPR-0005.0101 from 5.6.4 / 5.6.7 SPR but with different likelihood figures
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Analysis>

[1] Except 0347 safety requirement that is included in the group of safety requirements derived in SAR success approach.

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.04-OSED-0028.0010	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.04-OSED-0028.0040	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.04-OSED-0028.0110	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.04-OSED-0028.0660	<Full>
<ALLOCATED TO>	<Functional block>	Arrival Mgt (AMAN)	N/A
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.04.02-SPR-0005.0102
Requirement	The likelihood of E-AMAN operating on an incorrect time reference shall be no more than 2e-4 SOH, approximately once every 7 months.
Title	E-AMAN incorrect time reference
Status	<Validated>
Rationale	D05-001-SAR-SR-102; E-AMAN Requirement REQ-05.06.04-SPR-0005.0102 from 5.6.4 / 5.6.7 SPR but with different likelihood figures
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Analysis>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.04-OSED-0028.0010	<Full>
<ALLOCATED TO>	<Functional block>	Arrival Mgt (AMAN)	N/A
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.04.02-SPR-0005.0104
Requirement	The likelihood of E-AMAN incorrectly assessing need for delay or expedition shall be no more than 2e-4 SOH, approximately once every 7 months.
Title	E-AMAN incorrect need for delay assessed
Status	<Validated>
Rationale	D05-001-SAR-SR-104; E-AMAN Requirement REQ-05.06.04-SPR-0005.0104 from 5.6.4 / 5.6.7 SPR but with different likelihood figures
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Analysis>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.06.04-OSED-0028.0010	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-05.06.04-OSED-0028.0110	<Full>
<ALLOCATED TO>	<Functional block>	Arrival Mgt (AMAN)	N/A
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

CMAN REQ 401-499

[REQ]

Identifier	REQ-05.04.02-SPR-0005.0401
Requirement	CMAN shall continuously monitor and diagnose its operation and alert Sequence manager if its operational status has exceeded applicable operational parameters. *Note: Operational service parameters will result from SPR-INTEROP, technical design and local implementations.*

Title	CMAN self monitor and diagnose
Status	<Validated>
Rationale	D05-001-SAR-SR-50 D05-001-SAR-SR-52
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Review of Design>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.04.02-OSED-CMAN.0030	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-05.04.02-OSED-CMAN.0050	<Full>
<ALLOCATED_TO>	<Functional block>	Enroute Sequence and Flow Manager (ESFM)	N/A
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.04.02-SPR-0005.0402
Requirement	CMAN shall continuously monitor the quality of its input data and alert Sequence manager if input data quality is suspect.
Title	CMAN input data check
Status	<Validated>
Rationale	D05-001-SAR-SR-51 D05-001-SAR-SR-52
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Review of Design>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.04.02-OSED-CMAN.0030	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-05.04.02-OSED-CMAN.0050	<Full>
<ALLOCATED_TO>	<Functional block>	Enroute Sequence and Flow Manager (ESFM)	N/A
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.04.02-SPR-0005.0403
Requirement	For each inserted flight CMAN shall determine whether there exists a need to delay the flight.
Title	Assess need for delay
Status	<Validated>
Rationale	D05-001-SAR-SR-53
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Review of Design>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.04.02-OSED-CMAN.0030	<Full>
<ALLOCATED_TO>	<Functional block>	Enroute Sequence and Flow Manager (ESFM)	N/A
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.04.02-SPR-0005.0404
Requirement	CMAN shall receive arrival management information from E-AMAN.
Title	CMAN to receive arrival management information
Status	<Validated>

Rationale	D05-001-SAR-SR-54
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Review of Design>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.04.02-OSED-CMAN.0030	<Full>
<ALLOCATED_TO>	<Functional block>	Enroute Sequence and Flow Manager (ESFM)	N/A
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.04.02-SPR-0005.0405
Requirement	E-AMAN shall receive updated arrival management information from CMAN.
Title	E-AMAN to receive updated arrival management information
Status	<Validated>
Rationale	D05-001-SAR-SR-55
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Review of Design>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.04.02-OSED-CMAN.0050	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-05.04.02-OSED-CMAN.0080	<Full>
<ALLOCATED_TO>	<Functional block>	Arrival Mgt (AMAN)	N/A
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.04.02-SPR-0005.0406
Requirement	Configuration of CMAN shall be validated and verified prior to operational deployment.
Title	Validate configuration
Status	<Validated>
Rationale	D05-001-SAR-CMAN-N01
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Review of Design>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.04.02-OSED-CMAN.0030	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-05.04.02-OSED-CMAN.0050	<Full>
<ALLOCATED_TO>	<Functional block>	Enroute Sequence and Flow Manager (ESFM)	N/A
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

Note: For the following group of requirements a tolerable level of risk cannot be prescribed nor demonstrated in the form of failure rates or conditions per unit of time or operation as would be the case in functional elements of mechanical or electrical character. Instead, the tolerable level of risk must be designed into the software by ensuring that proper design validation, verification and assurance procedures are followed. A Software Assurance Level (SWAL) implicitly recognizes that in software design, defined in ESARR. The level is indicated in each relevant requirement.

[REQ]

Identifier	REQ-05.04.02-SPR-0005.0451
Requirement	The likelihood of CMAN being not available or unserviceable shall be no

	more than 2e-4 SOH, approximately once every 7 months.
Title	CMAN unserviceable
Status	<Validated>
Rationale	D05-001-SAR-SR-153
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Analysis>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.04.02-OSED-CMAN.0030	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-05.04.02-OSED-CMAN.0050	<Full>
<ALLOCATED_TO>	<Functional block>	Enroute Sequence and Flow Manager (ESFM)	N/A
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A

[REQ]

Identifier	REQ-05.04.02-SPR-0005.0452
Requirement	The likelihood of CMAN incorrectly assessing need for delay or expedition shall be no more than 2e-4 SOH, approximately once every 7 months.
Title	CMAN incorrect need for delay assessed
Status	<Validated>
Rationale	D05-001-SAR-SR-154
Category	<Safety>
Validation Method	<Real Time Simulation>
Verification Method	<Analysis>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.04.02-OSED-CMAN.0030	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-05.04.02-OSED-CMAN.0050	<Full>
<ALLOCATED_TO>	<Functional block>	Enroute Sequence and Flow Manager (ESFM)	N/A
<APPLIES TO>	<Operational Focus Area>	OFA04.01.02	N/A

3.1.2 Performance Requirements

The performance requirements defined for solution #05 are applicable to solution #08. They are referenced in Appendix B.

3.2 Information Exchange Requirements (IER)

Information Elements specific to the OI-Step TS-303 addressed within 05.04.02 are included in this section

3.2.1 Overview

From a documentation point of view, it is difficult to disentangle the human and system roles contributing to the Use Cases, as the partitioning (as well as the actual role involved) may depend on local implementation choices. Therefore, in the representation of the IERs the "Issuer" and "Addressee" column are filled using "mixed entities" defined in the following table:

Issuer / Addressee	Constituent CONOPS[2]/DOD[3]/OSED[4] Roles	Constituent Systems
Arrival Management	Sequence Manager[5]	AMAN Tool
Centre Management	Centre Manager	CMAN Tool
Stakeholder ATSU	Executive Controller in TMA or Enroute Centre Planning Controller in TMA or Enroute Centre Flow Management Position (i.e. any approach and upstream enroute sector, within the same ACC or in other ACCs)	Centre FDPS / Controller HMI
Aircraft	Flight Crew	a/c systems

Table 1: Entity Table

The diagram on the next page provides an overview of the information. It also relies on the requirements against the current "baseline" AMAN operations described in 05.06.07 OSED.

Note: Numbers refer to the identifiers used in the tabular description of the requirements.

[2] See document B4.2 - SESAR Concept of Operations Step 1 – Appendix D

[3] 5.2 DOD refers to B4.2 Conops as well

[4] See Section 3.2.2

[5] See 05.06.04 OSED

The following diagram is provided to facilitate the understanding of information exchanges in the context of centre management in this document only. Therefore, it is not subject to the operational improvement description.

Notes on the content:

- As the current OI step interfaces with the upstream ATSUs using mechanisms described in the 05.06.07 OSED, it is convenient to include the relevant information exchanges in this diagram. The IERs and IEs of 05.06.07 OSED are not affected by the present OI step, as there is only a change in data quality of the AMAN advisories send out to upstream ATSUs.

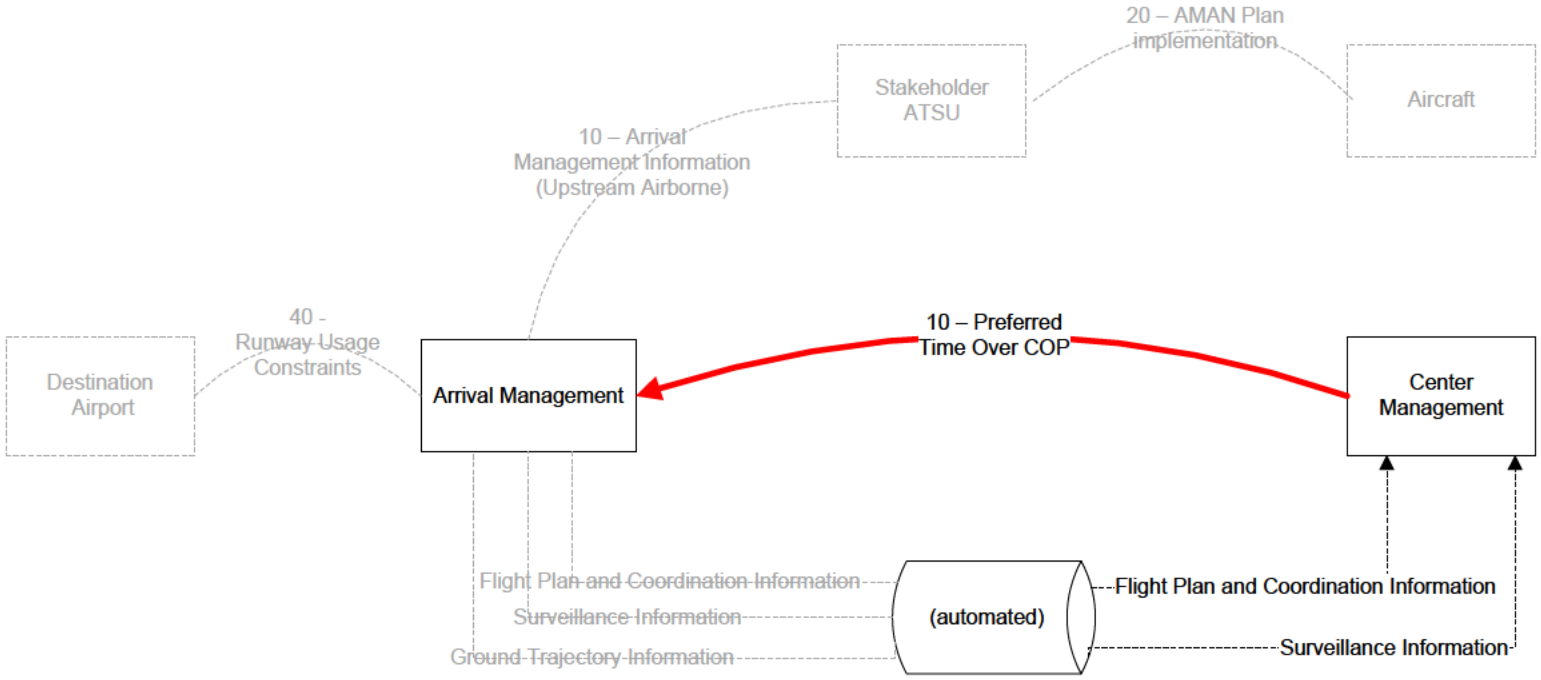
20 – AMAN Plan implementation
Stakeholder ATSU
Aircraft
10 – Arrival Management Information (Upstream Airborne)
40 - Runway Usage Constraints
Destination Airport
Arrival Management
10 – Preferred Time Over COP
Center Management
Flight Plan and Coordination Information
Surveillance Information
Ground Trajectory Information
(automated)
Flight Plan and Coordination Information
Surveillance Information

Figure 4: Overview of Information Exchanges

There are two interaction exchange types

- "red" – CMAN: The AMAN outputs are provided to air traffic controllers, who implement the sequence. The extension of the AMAN horizons delivers information to upstream controllers. .

- "grey" – some Extended AMAN Horizon flows described in 05.06.07 OSED are displayed for completeness as explained above
- **black**" – Reference data (contextual information) required by the CMAN tool to determine the preferred time for an inbound flight to enter the airspace region for which the Center Manager has been set up.

3.2.2 IER Overview Table

The following table lists the Information Exchange Requirements implied in the OSED requirements. The IERs have been classified in two groups:

- CMAN operations,
- Reference information (information sources for CMAN tool).

Identifier	Name	Issuer	Intended Addressees	Information Element	Involved Operational Activities	Interaction Rules and Policy	Status	Rationale	Satisfied DOD Requirement Identifier	Service Identifier
Information Exchanges for CMAN operations										
IER-5.4.2-IERS-CMAN-0010	Preferred Time Over COP	Center Manager	Arrival Manager	Preferred Time Over	Provide Arrival Information	See below	<In Progress>	REQ-05.04.02-OSED-CMAN.0080	REQ-05.02-DOD-OPR1-0011 <Partial>	n/a
Reference Information Exchanges required by the CMAN Tool										
For info only!	Flight Plan and Coordination Information	(automated)	Arrival Management	Flight Plan Messages	Implement Updated Arrival Sequence	See below	<In Progress>	REQ-05.04.02-OSED-CMAN.0030	REQ-05.02-DOD-OPR1-0004/-0011/-0014<Partial>	n/a
For info only!	Surveillance Information	(automated)	Arrival Management	Track Data	Implement Updated Arrival Sequence	See below	<In Progress>	REQ-05.04.02-OSED-CMAN.0030	REQ-05.02-DOD-OPR1-0004/-0011/-<Partial>	n/a

Table 2: IER overview

3.2.3 Interaction Rules and Policies

In this table details of the draft interaction rules and policies of the previous IERs defined in section 3.2.2 are provided:

[IER]

Identifier	Name	Issuer	Intended Addressees	Interaction Rules and Policy					
				Interaction Type	Frequency	Maximum Time of Delivery	Confidentiality	Safety Criticality	Comments
Information Exchanges for CMAN operations									
IER-5.4.2-IERS-CMAN-0010	Preferred Time Over	Center Management	Arrival Management	<One-way>	Ad hoc (at each recalculation with significant impact on Preferred Time Over)	< 10 s (enroute center)	<public>	<minor>	Incorrect information would lead to a sub-optimal advisory being issued to the a/c in the upstream ATSU, with potential workload and capacity effects.
Reference Information Exchanges required by the CMAN Tool									
For info only!	Flight Plan and Coordination Information	(automated)	Arrival Management	<One-way>	<ad hoc>	< 10s	<public>	<major>	Loss of flight plan information impedes the sequence prediction, leading to major loss of efficiency

Identifier	Name	Issuer	Intended Addressees	Interaction Rules and Policy					
				Interaction Type	Frequency	Maximum Time of Delivery	Confiden-tiality	Safety Criticality	Comments
For info only!	Surveillance Information	(automated)	Arrival Management	<One-way>	<periodical >l	~ 5s (radar update)	<restricted >	See note	Loss of surveillance input compromises the AMAN trajectory. So major for the AMAN but not so critical from an overall perspective (i.e. compared to other implications of this failure) Note assumption that AMAN is not responsible for missed approach detection.

Table 3: IER Interaction Rules and Policies

Notes:

- All values are based on present-day operations and are subject to revision by safety assessment.
- 'Public' is to be understood as 'No restrictions for actors in the operational activity'.
- 'Maximum Time of Delivery' has schematically been set to <1s for local, < 10s for remote ground and < 20 s for airborne communication partners. This is not based on any technology considerations.

3.2.4 New Information Elements

An Information Element specific to OI-Step TS-303 addressed within 05.04.02 are included in this section.

Identifier	IE-5.4.2-0032-0001
Name	Preferred Time Over
Description	The time, computed and optimised by the CMAN Tool at which the flight would ideally arrive at the reference coordination point from a Centre Management point of view.
Properties	Aerodrome(s) for which the horizon is used. Defined by ICAO (see AIRM).
Rules applied	
Comments	Abbreviation: PTO

4 References and Applicable Documents

This section identifies the documents (name, reference, source project) the SPR has to comply to or to be used as additional inputs for the SPR.

4.1 Applicable Documents

This SPR complies with the requirements set out in the following 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/Templates%20and%20Toolbox%20User%20Manual.doc

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

4.2 Reference Documents

The following documents were used to provide input / guidance / further information / other:

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

[6] B.4.1 Performance Framework (validation targets, influence diagrams), Edition 2.

[7] B.4.3 Architecture Description Document, Edition 2014

[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 Human Performance Reference Material
https://extranet.sesarju.eu/Programme%20Library/Forms/Procedures%20and%20Guidelines.aspx

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

[13] WPB.01 Integrated Roadmap Dataset 15

[14] P05.04.02 D04 “Final OSED Step 1 – Volume 2: TS-0303”

[15] P05.06.07 D015 “Update of 5.6.4 OSED Step 1” (TS-0305-A)

[16] P05.06.07 D53 “Update of 5.6.4 SPR Step 1 – Edition 2” (TS-0305-A)

Appendix A Assessment / Justifications

A.1 Safety and Performance Assessments

A.1.1 Safety assessment

Safety Assessment was conducted under the supervision from 16.06.01 and applying the SRM [8]. Its outcome is detailed in the embedded document hereafter:

Safety Assessment Report

Document information	
Project title	Co-Operative Planning in the TMA
Project N°	05.04.02
Project Manager	DFS
Deliverable Name	SAR
Deliverable ID	
Edition	00.01.00
Task contributors	
DFS Deutsche Flugsicherung GmbH	

Abstract

This document records the results of the Safety Assessment for TMA-1 Co-Operative Planning in the TMA in OFA 04.01.02 "Enhanced Arrival & Departure Management in TMA and En Route". It addresses the Step 1 Operational Improvement Step TS-0303 "AMAN into Multiple Airports" at E-OCVM validation phase V3 (SESAR 1 Solution #8).

It is based on the D53-05.06.07 SAR for TS-0305-A and adds aspects relevant to TS-0303 supported by a series of real-time validation exercises performed within project 05.04.02.

This report serves as an input document for 05.04.02 D05 "Step 1 Final SPR".

Authoring & Approval

Prepared By		
Name & company	Position / Title	Date
[redacted] DFS	[redacted]	07/03/2016
[redacted] DFS	[redacted]	07/03/2016

Reviewed By		
Name & company	Position / Title	Date
Reviewed as part of the SPR		

Approved By		
Name & company	Position / Title	Date

Document History

Edition	Date	Status	Author	Justification
00.00.01	14/10/2015	Initial draft	[redacted]	Initial version
00.00.02	08/01/2016	Draft	[redacted]	Updated to reflect new version of 05.06.07 SAR
00.00.20	07/03/2016	Draft for external review	[redacted]	To be reviewed as part of the SPR
00.01.00	22/03/2016	Final	[redacted]	Updated after external review of SPR/SAR

IPR (foreground)

This deliverable consists of SJU foreground.

Table of Contents

List of tables

List of figures

Executive summary

This document records the results of the Safety Assessment for TMA-1 Co-Operative Planning in the TMA in OFA 04.01.02 “Enhanced Arrival & Departure Management in TMA and En Route”. It addresses the Step 1 Operational Improvement Step TS-0303 “AMAN into Multiple Airports” at E-OCVM validation phase V3 (SESAR 1 Solution #8).

It is based on the D53-05.06.07 SAR for TS-0305-A and adds aspects relevant to TS-0303 supported by a series of real-time validation exercises performed within project 05.04.02. Please note that in the context of 05.04.02 the validation of TS-0303 was restricted to the OFA concept elements E-AMAN and CMAN, leaving Long-Range AMAN, Satellite Airports, CTA and Departures from Multiple Airports out of the scope.

The assessment applied SESAR Safety Reference Methodology under guidance from P16.06.01 safety experts. As part of the process, an adaptation of Fault Tree, termed Hybrid Fault Tree Analysis, was applied in order to resolve the issue of quantitative requirements as imposed on the human factor.

In OFA level coordination it was agreed that the assessment and the ensuing SPR and INTEROP activities should restrict themselves to a purely operational view; as per the SESAR framework the work is to be continued by technical projects.

This report serves as an input document for 05.04.02 D05 “Step 1 Final SPR”.

1 Introduction

1.1 Background

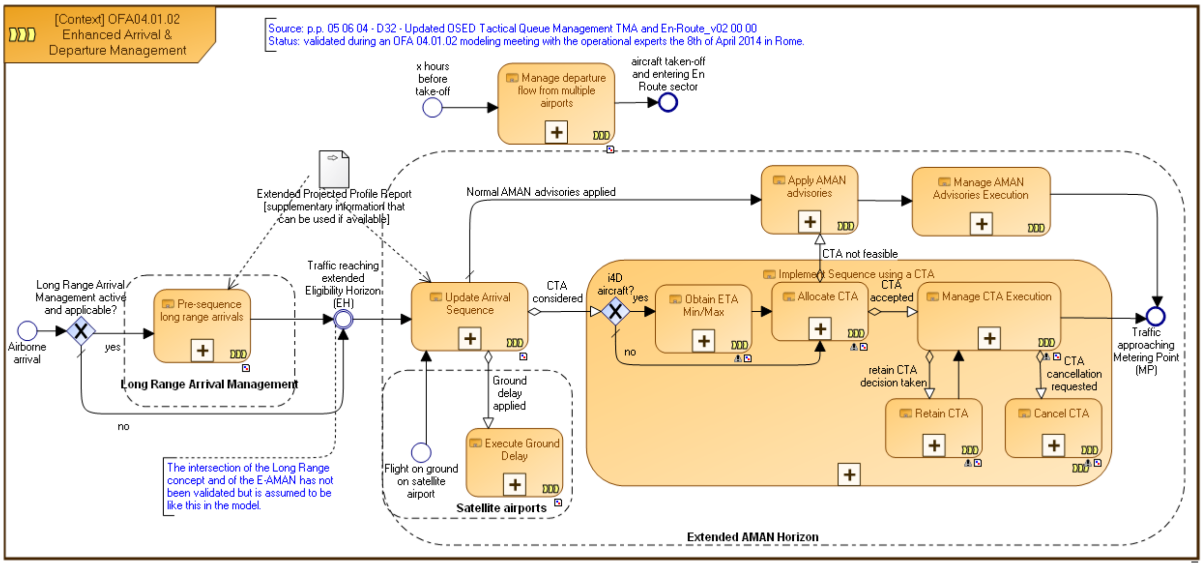
[Context] OFA04.01.02
Enhanced Arrival &
Departure Management
Source: p.p. 05 06 04 - D32 - Updated OSED Tactical Queue Management TMA and En-Route_v02 00 00
Status: validated during an OFA 04.01.02 modeling meeting with the operational experts the 8th of April 2014 in Rome.
x hours before take-off
Manage departure flow from multiple airports
aircraft taken-off and entering En Route sector
Extended Projected Profile Report [supplementary information that can be used if available]
Normal AMAN advisories applied
Apply AMAN advisories
Manage AMAN Advisories Execution
CTA not feasible
Long Range Arrival Management active and applicable?
Airborne arrival
yes
no
Pre-sequence long range arrivals
Long Range Arrival Management
Traffic reaching extended Eligibility Horizon (EH)
Update Arrival Sequence
CTA considered
i4D aircraft?
yes
no
Implement Sequence using a CTA
Obtain ETA Min/Max
Allocate CTA
CTA accepted
Manage CTA Execution
retain CTA decision taken
Retain CTA
CTA cancellation requested
Cancel CTA
Traffic approaching Metering Point (MP)
Ground delay applied
Execute Ground Delay
Flight on ground on satellite airport
Satellite airports
The intersection of the Long Range concept and of the E-AMAN has not been validated but is assumed to be like this in the model.
Extended AMAN Horizon

Figure 5 - OFA 04.02.01 EATMA Modell

Whereas SESAR projects 05.06.04 and 05.06.7 extensively dealt with all implications of extending the AMAN planning horizon, the Operational Improvement Step TS-0303 considers the special case of a multi-airport environment.

In case of several proximate TMAs and E-TMA sectors which handle several arrival traffic streams into the multiple TMAs, dependencies between these streams are usually not taken into account by the individual AMANs. Thus, despite proper network flow management measures based on average traffic count within 20min intervals of a predefined traffic volume, bunching can occur. This in turn can lead to situations where the E-TMA sector becomes the bottleneck of the multi-airport TMA and thus runway capacity is not fully utilized, too. Therefore, an additional arrival planning component “Center Manager” (CMAN) which accompanies the individual AMANs of the airports was investigated.

On the basis of E-AMAN and CMAN, arrival planning information and advice will be sent to the upstream sectors utilizing the concept of AMAN extended horizon. Including upstream sectors in the arrival management process could create an optimal utilization of the available airspace capacity and help to avoid short-term overload situations.

TS-0303 impacts the OFA 04.02.01 EATMA model (Figure 1) only in the sub-process “Update Arrival Sequence” (Figure 2 and Figure 3).

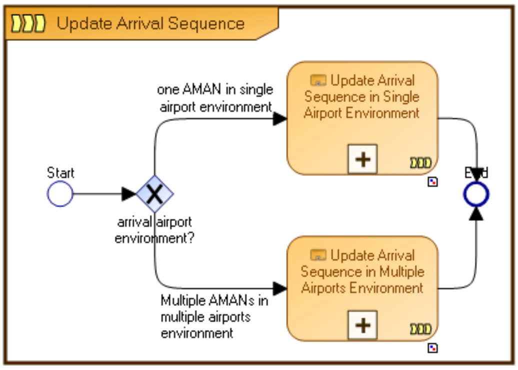
Update Arrival Sequence
one AMAN in single airport environment
Update Arrival Sequence in Single Airport Environment
Start
End
arrival airport environment?
Update Arrival Sequence in Multiple Airports Environment
Multiple AMANs in multiple airports environment

Figure 6 - OFA 04.0.2.01 Process Model: Sub-process "Update Arrival Sequence"

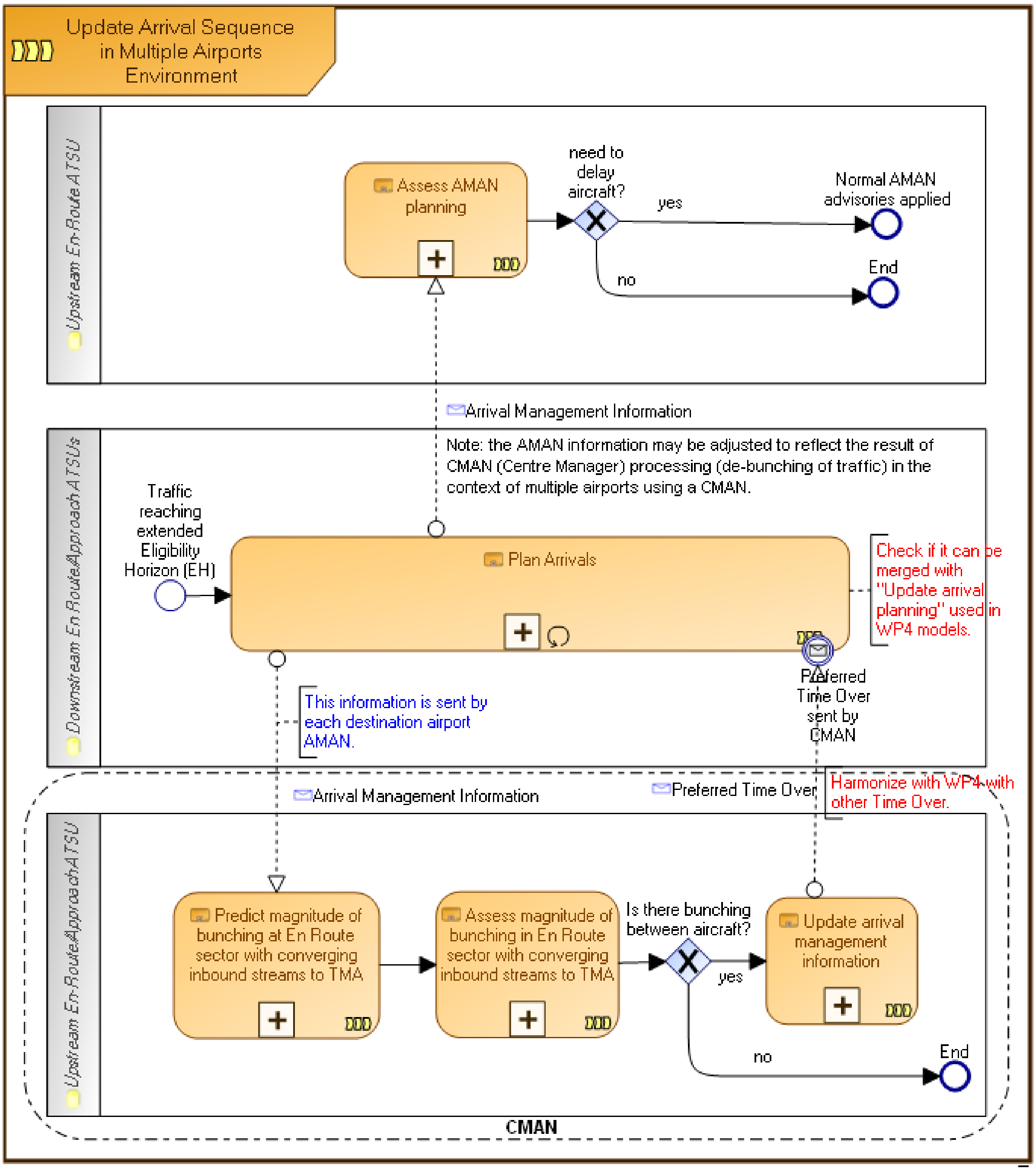
Update Arrival Sequence in Multiple Airports Environment
Upstream En-Route ATSU
Assess AMAN planning
need to delay aircraft?
yes
Normal AMAN advisories applied
no
End
Arrival Management Information
Downstream En Route/Approach ATSUs
Note: the AMAN information may be adjusted to reflect the result of CMAN (Centre Manager) processing (de-bunching of traffic) in the context of multiple airports using a CMAN.
Traffic reaching extended Eligibility Horizon (EH)
Plan Arrivals
Check if it can be merged with "Update arrival planning" used in WP4 models.
Preferred Time Over sent by CMAN
This information is sent by each destination airport AMAN.
Arrival Management Information
Preferred Time Over
Harmonize with WP4 with other Time Over.
Upstream En-Route/Approach ATSU
Predict magnitude of bunching at En Route sector with converging inbound streams to TMA
Assess magnitude of bunching in En Route sector with converging inbound streams to TMA
Is there bunching between aircraft?
yes
Update arrival management information
no
End
CMAN

Figure 7 - Sub-process "Update Arrival Sequence in Multiple Airport Environment"

Please note that in the context of 05.04.02 the validation of TS-0303 was restricted to the OFA concept elements E-AMAN and CMAN, leaving Long-Range AMAN, Satellite Airports, CTA and Departures from Multiple Airports out of the scope. See details in P05.06.07 OSED [8] and P05.04.02 OSED [10].

1.2 General Approach to Safety Assessment

1.2.1 A Broader approach

The SESAR Safety Reference Material has been used as guidance for performing this Safety Assessment. This harmonisation of the methodology throughout the SESAR OFAs ensures that:

- The "success" approach has been applied to derive Functional and Performance Safety Requirements (F&P SR); the KPIs determined by P B.04.01 are considered when expressing the Safety Criteria of the OFA, the completeness of the argumentation can be justified,
- The failure approach is handled considering the effect of failures at operational level.

1.3 Scope of the Safety Assessment

As stated in section 1.1 the Safety Assessment of TS-0303 was restricted to the OFA concept elements E-AMAN and CMAN, leaving Long-Range AMAN, Satellite Airports, CTA and Departures from Multiple Airports out of the scope.

1.4 Layout of the Document

The document follows the standard SESAR SAR template; Chapter 2 introduces and elaborates on the concept, determines safety criteria, pre-existing hazards and culminates in the definition of safety objectives for either approach. Chapter 3 details the construction of a functional model and a SPR level model and sets safety requirements for either approach. Coordination at OFA level delegated the technical design phase to a related technical project, resulting in Chapter 4 left blank.

1.5 References

[1]. SESAR P16.06.01, SESAR Safety Reference Material, Edition 00.03.01, 09/03/2015

[2]. SESAR P16.06.01, Guidance to Apply the SESAR Safety Reference Material, Edition 00.02.01, 09/03/2015

[3]. SESAR P16.06.01 Guidance X – Hybrid Fault Tree v0.3, 13/11/2015

[4]. SESAR P05.04.02 D01-Preliminary OSED Step 1.00.03.01, 14/072015

[5]. SESAR P04.02 D101 WP4 Detailed Operational Description Step 1 00.06.03 31/05/2013

[6]. SESAR SWP5.2 TMA Detailed Operational Description Step 1, D84 edition 00.01.01, 30.04.2015.

[7]. SERA – Standardized European Rules of the Air, Commission Implementing Regulation (EU) No 923/2012

[8]. SESAR P05.06.07 D53 "Update of 5.6.4 SPR Step 1 – Edition 2" (TS-0305-A) –including SAR

[9]. SESAR P05.06.07 D015 "Update of 5.6.4 OSED Step 1" (TS-0305-A)

[10]. SESAR P05.04.02 D04 "Final OSED Step 1 – Volume 2: TS-0303"

[11]. P05.04.02 D03 "Step 1 V2 VAL-Report TS-0303" (Exercise VP-333)

[12]. P05.04.02 D34 "Step 1 V3 VAL-Report TS-0303" (Exercise VP-778)

1.6 List of acronyms

Term	Definition

Term	Definition
AAH	Active Advisory Horizon
A/C	Aircraft
AC#	Abnormal Condition
AIM	Accident-Incident Model
AMA	Arrival Message
AMAN	Arrival Manager (Equipment)
ANSP	Air Navigation Service Provider
APP	Approach (control sector/position)
APR	Automatic Position Report(-ing)
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATM	Air Traffic Management
ATSU	Air Traffic Service Unit
ATSU DEST	ATSU Destination
CFMU	Central Flow Management Unit
CMAN	Center Manager
CNS	Communication, Navigation, Surveillance domains of the ATM system
COTR	Coordination and Transfer (equipment)
CTA	Controlled Time of Arrival
CWP	Controller Working Position
DCB	Dynamic Capacity Balancing
DMAN	Departure Manager
DOD	Detailed Operational Description
E-AMAN	Extended AMAN
EATMA	European ATM Architecture
EH	Eligibility Horizon

Term	Definition
ENR	En-route
ENT	Entity
E-OCVM	European Operational Concept Validation Methodology
E-R	En-route (in AIM context)
ETA	Estimated Time of Arrival
EXE	Executive controller
EXE-nnn	SESAR Validation Exercise VP-nnn
FCN	Function
FDPS	Flight Data Processing System
FH	Flight Hour *also styled as flt hr*
FHA	Functional Hazard Analysis
FIR	Flight Information Region
FL	Flight level
FM	Functional Model
FPL	Flight plan
FTA	Fault Tree Analysis
HAZID	Hazard Identification
HF	Human Factor(s)
HFTA	Hybrid Fault Tree Analysis *also styled as H-FTA*
HMI	Human Machine Interface
HP	Human Performance
ICAO	International Civil Aviation Organisation
IFR	Instrument Flight Rules
IMH	Initial Metering Horizon
IMP	Initial Metering Point

Term	Definition
INTEROP	Interoperability Requirements
MAC	Mid-Air Collision, type of AIM
MET	Meteorological information (data source)
MM	Mitigation Means
MP	Metering Point
MTFoO	Maximum Tolerable Frequency of Occurrence
NM	Nautical Mile
OFA	Operational Focus Area
OH#	Operational Hazard
OI	Operational Improvement (Step)
OLDI	On-Line data Interchange
OSED	Operational Services and Environment Description
PLN	Planning controller
RT	Radio Telephony *also styled as R/T*
RTA	Required Time of Arrival
RWY	runway
SAC	SAfety Criteria
SAR	Safety Assessment Report
SDPS	Surveillance Data Processing System
SEQ_MAN	Sequence Manager (role)
SERA	Standardized European Rules of the Air
SESAR	Single European Sky ATM Research Programme
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SO#	Safety Objective
SO# (F&P)	Safety Objective – Functionality and Performance (Success approach) *also styled as F&P SO#*

Term	Definition
SOH	Sector Operating Hour
SPR	Safety and Performance Requirements
SR	Safety Requirement
SR (F&P)	Safety Requirement – Functionality and Performance (Success approach)
SRC	Data source
SRM	SESAR Safety Reference Material
STAR	Standard Arrival Route
SWIM	System-Wide Information Management
TMA	Terminal (Manoeuvring) Area
TOBT	Target Off Block Time
ToD	Top of Descent
TP	Trajectory Predictor (or Prediction)
TSA	Temporary Segregated Airspace/Area
TTG	Time to Gain
TTL	Time to Lose
VALS	Validation Strategy
VFR	Visual Flight Rules
WIA	Wake Induced Accident
WVE	Wake Vortex Encounter
WX	weather

2 Safety specifications at the OSED Level

2.1 Scope

This section documents the following activities:

- Description of the Operational Environment as deemed relevant to the Safety assessment, in 2.2
- Summary of airspace user requirements, in 2.3
- Determination of the Safety Criteria, in 2.4
- Identification of pre-existing hazards
- Identification of operational services and derivation of Safety Objectives (success approach) in order to mitigate pre-existing risks under normal operational conditions, in 2.6 and 2.7
- Assessment of Services provided for handling of abnormal scenarios, in 2.7
- Derivation of Safety Objectives (failure approach), in 2.8

2.2 OFA 04.01.02 Operational Environment and Key Properties

Refer to Environment definition, Section 3 of both P04.02 DOD [5] and P05.02 Step 1 DOD [6], and in more detail, to Section 4 of P 05.04.02 OSED [4].

2.2.1 Types of Airspace – ICAO Classification

The envisaged environment is controlled En-route and TMA environment (classes A to E), classified as Medium/Medium and High/High Density/Complexity

2.2.2 Airspace Users – Flight Rules

SERA – Standardized European Rules of the Air, Commission Implementing Regulation (EU) No 923/2012 [7] is the underlying legal framework for conduct of flight operations.

Note: SERA defines “downstream clearance”, a type of clearance that may be employed by the operating method.

Airspace users operating IFR are the envisaged users of the service. While there is no explicit mechanism barring a suitably equipped and approved VFR from receiving the service, there are a number of disqualifying conditions:

- The arrival process relies on instrument arrival procedures.
- The arrival process begins in En-route airspace typically well above FL100 (except satellite airports).
- The arrival process relies on DCB and flow management for which an IFR flight plan is expected to be a prerequisite (see assumption A-110).

A VFR flight can theoretically be afforded AMAN service only if the above conditions are met. In the context of this safety assessment, VFR flights are assumed as excluded.

2.2.3 Traffic Levels and complexity

The SESAR operating method is not explicitly constrained by traffic density and complexity. The method relies on strategic and pre-tactical mechanisms such as DCB and Network Optimization (see assumption A-110) and associated procedures, training and contingency means to ensure that demands on the service are adequate with the existing capacity.

Usability of the method is expected to be governed by airspace complexity in practice. We assume:

- Single arrival runway operations to the central airport

-ATSU/FIR borders may need to be accommodated in relation to the extended AMAN horizon.

- Closed loop STARs are preferred though not required. Expected path must be known up until the Metering Fix or its Reference Point. With open loop STAR, AMAN has to be able to rely on standardized vectoring paths with associated flight times.

2.2.4 Aircraft ATM capabilities

n/a

2.2.5 Terrain Features - Obstacles

n/a

2.2.6 CNS Aids

None required explicitly, however the method requires the expected CNS in place; at least voice communications for the provision of ATC service; the navigational infrastructure to support flight operations on the present route structure and the surveillance infrastructure to generate the required input to the ATC service, including arrival management.

2.2.7 Separation Minima

The concept imposes no restriction or adaptation to the use of separation minima. In considering a typical flight, standard radar horizontal minima are assumed; 10 or 5 NM en-route, 3 NM in TMA and 2.5 NM on final approach. A vertical minimum of 1000 ft RVSM is assumed as the applicable vertical separation.

2.2.8 Operational services

The following requirements or expectations are imposed by the service:

- ATC roles: legacy Executive / Planning (EXE/PLN) setup as required, plus the Sequence Manager (SEQ_MAN) position.

- Controllers use “Provide planning separation assurance” process or other sufficient method for planned de-confliction.

2.3 Airspace Users Requirements

The benefit for the Airspace Users follows along the lines of the E-AMAN except that TS-0303 enables these benefits even in a multi-airport environment:

- Improved delay management, implemented earlier in flight, will have a positive impact on time predictability (plan is implemented earlier, and adhered to for longer) and trajectory optimization (better delay management earlier, with fewer interventions at lower levels, which can add time/unpredictability to flight ops, also see assumption A-110).

- Improved flight predictability and delay management will lead to improved fuel efficiency, (fewer flight control measures needed at lower altitude for sequencing etc. will lead to reduced fuel burn at lower altitudes).

- Improved flight predictability and delay management will lead to improved aircrew workload (fewer aircrew flight control measures needed at lower altitude for sequencing etc.), and combined with better flight predictability will lead to better resource efficiency management (improved crew workload, improved planning for aircraft on stand, baggage, catering etc.).

Additionally, benefit in terms of safety is expected through reduction in complexity, earlier detection and resolution of potential conflict medium term in the planning phase, and greater scope for conflict reduction in the sequence implementation phase through improved air/ground trajectory coherence.

2.4 Safety Criteria

The Preliminary 05.06.04 SPR identified a list of seven SAC for TS-0305-A and TS-0303.

In the course of the operational projects 05.06.04 and 05.06.04, 16.06.01 subsequently reviewed and refined the list leaving only three relevant SAC.

Reference	SAC
SAC#4	There will be an 5% reduction in the number of ATC induced conflicts in the TMA environment
SAC#5	There will be no increase in the number of ATC Induced conflicts in the en-route environment
SAC#7	There will be an 5% reduction in pre-tactical conflicts in the TMA environment

In an initial safety assessment impact analysis performed by 16.06.01 on the impact of the services and operational processes defined in the 05.04.02 OSED for TS-0303, these SAC as defined for a single airport E-AMAN were found to remain applicable for AMAN into Multiple Airports.

The selected SAC are linked to the Functional Model (see 7.2) as follows:

All contributing ATSU's En route establish an optimized Sequence for Arrivals. This additional task should not have negative impact on tactical conflict in E-R. [SAC#5].
Note: As this is considered to be the bottleneck in a multi-airport environment, the core of TS-0303 is related to this SAC.

ATSU En route delivers and ordered, optimized and metered arrival sequence to ATSU TMA. This task should have positive impact on pre-tactical conflicts in TMA / [SAC#7]
Note: The benefit stems from the pre-existence of a plan of an optimized sequence at the point of transfer. The benefit is considered to be the same for both single- and multi-airport environment

ATSU TMA maintains and actively controls the sequence. This task should have positive impact on tactical conflict in TMA [SAC#4]
Note: The benefit stems from the existence of an implemented optimized metering and sequence. The benefit is considered to be the same for both single- and multi-airport environment.

Correlation against AIM models is established as follows:

- AIM MAC En-Route and AIM MAC TMA were assessed as the applicable AIM models.
- SAC#4 is related to MF 7.1 “ATC Induced Tactical Conflict” [Barrier 10].
- SAC#5 is related to MF 5.1 “Planned Conflict” [Barrier 10].
- SAC#7 is related to MF 5.2 “ATC Induced Pre-Tactical Conflict” [Barrier 10].

2.5 Relevant Pre-existing Hazards

As per SRM, Guidance F, section F 2.2 for Terminal Area and En-route operations, the pre-existing hazards will normally include the following:

- a situation in which the intended trajectories of two or more aircraft are in conflict (Hp#1)
- a situation where the intended trajectory of an aircraft is in conflict with terrain or an obstacle
- penetration of restricted airspace – this category is quite distinct from MAC for military danger areas where the end effect could be being shot down
- wake vortex encounters (WVE) (Hp#2)
- encounters with adverse weather(Hp#3)

From this List of pre-existing hazards as, it has been identified and agreed by P 05.06.04 that the Operational services: Traffic Synchronization and Arrival Sequencing and Metering, mitigate the following pre-existing hazards[7]:

Hp#1 Conflicts between pairs of trajectories

This is the predominant type of hazard related to the concept and the defined operational services.

Hp#2 Wake vortex encounters

In pre-SESAR operations, the optimization of the sequence at the runway for Wake vortex is done by approach controllers in the TMA; in the SESAR operating method, AMAN does this work as part of its sequence build. Notwithstanding the effect this shift has on the workload of the various ATCO positions involved, there is no appreciable impact on the services. The likelihood that an aircraft will encounter wake turbulence generated by a preceding aircraft is unchanged.

Hp#3 Adverse weather

Adverse weather at the central airport, typically thunderstorm activity, changing wind, drifting fog, may result in frequent or unplanned runway closures or runway changes, which the concept interprets as changes in runway capacity. When a runway capacity changes, the entire existing sequence becomes invalid and a new sequence is progressively established.

➔ Aircraft previously in sequence are now subjected to full tactical control, impacting the following services,
  - o TMA / Control Arrival Sequence
  - o ENR / Control Airspace

  Validation exercises have confirmed the resulting tendency towards an appreciable spike in controller workload. If the spike cannot be safely managed, hazard occurs.

[7] CFIT and flight into unauthorized areas (Airspace Infringement) are not mitigated by AMAN into multiple Airports.

- ➔ If operationally feasible, a subset of aircraft previously in sequence may be re-sequenced to fit the new operational conditions, with subsequent impact on all defined operational services and controller workload as in the previous case.

Adverse weather aloft (CB clouds, winds, jet stream) may also impact the following processes:

- ➔ ENR-TMA / Apply AMAN advisories
- ➔ ENR-TMA / Control arrival sequence

The effect of such weather is entirely dependent on the severity of the encountered phenomenon. In the worst case scenario the sequence becomes unworkable and is abandoned in favor of more intensive control methods involving holding stacks, resulting in an abruptly increasing controller workload.

2.6 Mitigation of the Pre-existing Risks – Normal Operations

2.6.1 Operational Services to Address the Pre-existing Hazards

Service “Provide Separation Assurance” is not specific to the TS-0303 and is not further explored in this document.

ID	Service Objective	Pre-existing Hazards
1	ENR, TMA / Provide Separation assurance [6].	Hp#1, HP#2, Hp#3
2	ENR, TMA / Synchronize Traffic [6].	Hp#1, HP#2, Hp#3

Table 4: ATM services and Pre-existing Hazards

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

As there are no changes to operations from the controller point of view besides the fact that the far-Upstream ATSU controllers might get some more time-to-lose displayed, no additional SO related to TS-0303 were identified. Thus all SO related to E-AMAN inherited from TS-305-A remain applicable.

However, it has to be noted, that the SO are now relevant not just for a single E-AMAN but for all E-AMAN which are part of the multi-airport environment.

Note: F&P SO#01 through 05 were identified as present in the baseline and reference method and were not addressed in the assessment. They are integral part of Service Objective ID1: “ENR, TMA / Provide Separation assurance” and hence judged to be outside the scope of TS-0303. As such, they are treated as assumptions in this SAR, see Table 18.

While it can be argued that some of the remaining services, starting with #1 and in scope of the SAR, are found in the baseline method as well, it was judged by the SAR team that the design or definitions of the services has been sufficiently impacted to consider them as part of the New SESAR operating method and related to service objective “Synchronize Traffic”.

Note: Services and objectives inherited from baseline AMAN marked in grey italics.

Ref	Phase of Fight / Operational Service	Related AIM Barrier	Achieved by / Safety Objective [SO xx]
0.1	*Control airspace*	*B5 – Planned Induced Conflict*	*F&P SO#01*
0.2	*Determine STAR/RWY*	*B10 – Traffic Planning and Synchronization*	*F&P SO#02* *F&P SO#03*
0.3	*Update Air and Ground Trajectory*	*B10 – Traffic Planning and Synchronization*	*F&P SO#04* *F&P SO#05*
1	ENR / Sequence and Meter Arrivals - Synchronize Traffic	B10 – Traffic Planning and Synchronization	F&P SO#06
2	ENR / Insert Flight reaching extended eligibility horizon into Arrival Sequence	B10 – Traffic Planning and Synchronization	F&P SO#07
3	TMA / Adjust AMAN as necessary	B10 – Traffic Planning and Synchronization	F&P SO#08
5	ENR / Update Arrival Sequence	B10 – Traffic Planning and Synchronization	F&P SO#10
6	ENR / Assess Delay	B10 – Traffic Planning and Synchronization	F&P SO#11
7	ENR / Deliver Arrival Sequence	B10 – Traffic Planning and Synchronization	F&P SO#12
8	ENR / Apply Delay (TTL/TTG)	B10 – Traffic Planning and Synchronization	F&P SO#14
11	ENR / Monitor Traffic Situation	B10 – Traffic Planning and Synchronization	F&P SO#22
12	TMA / Control Arrival Sequence	B10 – Traffic Planning and Synchronization	F&P SO#23
13	TMA / Apply Delay	B10 – Traffic Planning and Synchronization	F&P SO#24

Table 5: OFA Operational Services & Safety Objectives (success approach).

ID	Description
F&P SO#01	*ATC shall control aircraft arriving in own sector and ensure safe separation from other traffic.*
F&P SO#02	*ATC shall determine the expected STAR/RWY combination for each arriving aircraft*
F&P SO#03	*ATC shall communicated the expected STAR/RWY combination to each arriving aircraft.*
F&P SO#04	*ATC shall update Ground Trajectory with the determined STAR/RWY combination.*
F&P SO#05	*A/C shall update Air Trajectory with the received STAR/RWY combination.*

F&P SO#06	ATC shall build arrival sequence
F&P SO#07	ATC shall insert flight reaching extended horizon into arrival sequence.
F&P SO#08	ATC shall adjust AMAN to operational needs, such as: runway in use, runway closure, landing rate.
F&P SO#10	ATC shall update Arrival Sequence accounting for new information that can impact the sequence
F&P SO#11	ATC shall assess the need for delay on arrival. *Note: Delay can be positive or negative.*
F&P SO#12	ATSU En-route shall deliver traffic sequenced and metered in the order as presented by AMAN, to ATSU Approach. *Note: ATC may introduce additional manual input in the AMAN sequence as required.*
F&P SO#14	ATSU En-route shall apply AMAN advisories (TTL/TTG).
F&P SO#22	ATSU En-route shall continually monitor traffic situation and ensure that the AMAN planned times are met.
F&P SO#23	ATSU Approach shall manage traffic in Arrival Sequence delivered by ATSU En-Route, ensuring that AMAN times and sequence order are maintained.
F&P SO#24	ATSU Approach shall apply AMAN advisories to traffic as delivered by ATSU En Route.

Table 6: List of Safety Objectives (success approach) for Normal Operations.

Note: Services and objectives inherited from baseline AMAN marked in grey italics.

2.6.3 Analysis of the Concept for a Typical Flight

Most of the safety objectives identified by P05.06.04 and P05.06.07 relate to CTA etc., thus only three remain applicable:

ID	Description
F&P SO#26	Airspace design shall be optimized to support the concept.
F&P SO#29	Quality of trajectory prediction used by AMAN to build the sequence shall be sufficient to support concept operation.
F&P SO#33	Rules shall be defined as part of ATC Strategies in AMAN configuration to reflect principles governing overtake scenarios and using input information such as route, aircraft performance, onboard parameters and strategic prioritization.

Table 7: Additional Safety Objectives (success approach)

2.7 Operations under Abnormal Conditions

Non-nominal and abnormal operations are only degrees of unusual situations that fall within the normal duties of the ATCOs and are covered by normal processes (they are not as exceptional as failure cases).

As per SRM, "*the safety assessments need to consider all foreseeable (for foreseen) operating conditions, irrespective of whether they can be defined as "normal" and "abnormal"* ". As such, cases of non-nominal or abnormal conditions are covered jointly in the fault tree and the SR.

2.7.1 Identification of Abnormal Conditions

Abnormal condition ID	**Abnormal condition title**	**Description**	**Associated pre-existing hazards**
AC#1	Aircraft emergency	An aircraft declares emergency or urgency anywhere in the airspace where service is being provided.	Any
AC#2	planned RWY closure	A scheduled closure of runway occurs, negatively impacting airport capacity.	Hp3
AC#3	unplanned RWY closure	An unscheduled closure of runway occurs, negatively impacting airport capacity.	Any
AC#4	planned RWY change	A scheduled change or active runway occurs, impacting tactical traffic management. Runway capacity is impacted marginally at most.	Hp3
AC#5	unplanned RWY change	An unscheduled change or active runway occurs, impacting tactical traffic management. Runway capacity is impacted marginally at most.	Any
AC#6	sudden change in WX	An unexpected severe change of weather conditions impacts tactical traffic management, airspace and/or airport capacity.	Hp3
AC#7	severe WX	An occurrence of severely inclement weather impacts tactical traffic management, airspace and/or airport capacity.	Hp3
AC#8	sudden activation of restricted airspace	An unscheduled activation of restricted airspace impacts flow management and	No explicit hazard[8]

[8] AC#8 is connected to hazard category "airspace infringement" listed in the Guidance; the category was assessed as not relevant to the concept.

		airspace capacity.	
AC#9	low-performance aircraft	A low performance aircraft disrupts provision of service. *A light category aircraft sequenced would run the risk of requiring greater separation in APP. A low speed performance aircraft will have to be kept outside the main flow as there would be constant overtakes.*	Hp2
AC#10	TCAS RA occurs	An instance of TCAS RA is reported by an aircraft.	Hp1

Table 8: Identification of abnormal conditions

2.7.2 Potential Mitigations of Abnormal Conditions

Abnormal condition ID	**Abnormal condition title**	**Mitigation**	**Associated F&P SO or Assumption A-xxx**
AC#1	Aircraft emergency	If ATC determines that the emergency scenario is not compatible with continued sequence implementation, ATC shall provide control service and abort/update the sequence as required.	F&P SO#01 A-006 F&P SO#10
AC#2	planned RWY closure	ATC updates AMAN with the new operational parameter. Sequence building is automatically adjusted to suit the new operational conditions.	F&P SO#08 F&P SO#10
AC#3	unplanned RWY closure	ATC updates AMAN with the new operational parameter. ATC provides control service and updates the sequence as required.	F&P SO#01 F&P SO#08 A-006 F&P SO#10
AC#4	planned RWY change	As AC#2	F&P SO#08 F&P SO#10
AC#5	unplanned RWY change	As AC#3	F&P SO#01 F&P SO#08 F&P SO#10 A-006
AC#6	sudden change in	As AC#3	F&P SO#01

	WX		F&P SO#08 F&P SO#10 A-006
AC#7	severe WX	As AC#3	F&P SO#01 F&P SO#08 F&P SO#10 A-006
AC#8	sudden activation of restricted airspace	As AC#3	F&P SO#01 F&P SO#08 F&P SO#10 A-006
AC#9	low-performance aircraft	As AC#3	F&P SO#01 F&P SO#08 F&P SO#10 A-006
AC#10	TCAS RA occurs	As AC#3	F&P SO#01 F&P SO#10 A-006

Table 9: Safety objectives (F&P) to mitigate abnormal conditions.

2.8 Mitigation of System-generated Risks (failure approach)

2.8.1 Identification and Analysis of System-generated Hazards

System generated hazards were derived using the AIM MAC ENR and TMA Risk model.

Numbering of Operational hazards commences with 06 for simplicity and traceability to the Success Approach Safety objectives.

OH#	**Description**	**Related SO** ***(success approach)***	**Operational Effects**	**Mitigations of Effects**	**Severity** ***(most probable effect)***
OH#06	ATC fails to build arrival sequence	F&P SO#06	Inbound traffic not sequenced, multiple frequent trajectory conflicts at merging points in TMA and En-Route. Traffic reaching runway is not optimized for wake vortex, causing partial loss of runway throughput.	A-006 A-007 F&P SO#30 F&P SO#34M	SC4b

OH#07	ATC fails to insert and sequence an emergent flight at the Eligibility Horizon.	F&P SO#07	Single flight is not sequenced, causing a trajectory conflict in own sector or downstream.	F&P SO#08 F&P SO#10 A-006 A-007	SC4b
OH#08	ATC fails to adjust AMAN to relevant operational needs and parameters.	F&P SO#08	Planned sequence is unsuitable or incompatible with new operating conditions. Operational need is not met, resulting in potential tactical conflicts.	A-006 A-007	SC4b
OH#10	ATC fails to update the sequence to account for new relevant or important information.	F&P SO#10	Sequence is outdated and incompatible with actual operational conditions. Tactical conflicts result in own sector and downstream.	A-006 A-007	SC4b
OH#11	ATC fails to assess need for delay to a newly sequenced flight.	F&P SO#11	Natural sequence is implemented, resulting in tactical conflicts at merging points.	A-006 A-007	SC4b
OH#12	ATSU En-route fails to deliver the implemented sequence to ATSU Approach	F&P SO#12	Multiple and frequent tactical conflicts in ATSU Approach sectors.	A-006 A-007 F&P SO#23	SC4b
OH#14	ATSU En-route fails to apply AMAN advisories	F&P SO#14	Natural sequence is implemented, resulting in tactical conflicts at merging points in Approach sectors.	A-006 A-007 F&P SO#22 F&P SO#23	SC4b
OH#22	ATSU En-route fails to monitor traffic and to ensure that AMAN times are being	F&P SO#22	AMAN times not met at transfer to ATSU Approach, resulting in tactical conflicts in TMA.	A-006 A-007	SC4b

	met.				
OH#23	ATSU Approach fails to manage traffic in Arrival Sequence delivered by ATSU En-Route.	F&P SO#23	AMAN times and sequence order are not maintained, resulting in potential tactical conflicts.	A-006 A-007	SC4b
OH#24	ATSU Approach fails to apply AMAN advisories to traffic as delivered by ATSU En-route	F&P SO#24	Incorrect sequence resulting in tactical conflicts in TMA.	A-006 A-007 F&P SO#23	SC4b
OH#26	Airspace design insufficient to support the concept.	F&P SO#26	Ineffective arrival management, potential conflicts in all sectors.	A-006 A-007 F&P SO#22 F&P SO#23	SC4b

Table 10: Operational Hazards and Analysis

Depending on implementation, it may be possible and desirable for AMAN to provide a measure of verification concerning its operation and the quality of its input data. For instance, the quality of trajectory prediction could be subject to a continuous assessment of confidence or merit; where used, weather data input could be verified against an independent source or against Mode S IAS readout compared to radar speed readout. Operational messages containing flight plan information could be verified against historical records on the basis of the 24 bit ICAO address. Concerning own operation, AMAN could conduct a continuous verification of its timing reference against a trusted source.

As the same holds true for the CMAN, an additional SO has been added. To discern it from the AMAN SOs a “M” has been added as a postfix.

ID	Description
F&P SO#30	AMAN shall continuously monitor and diagnose its operation and the quality of its input data against all applicable criteria and alert the sequence manager by means of a suitable HMI message.
F&P SO#34M	CMAN shall continuously monitor and diagnose its operation and the quality of its input data against all applicable criteria and alert the sequence manager by means of a suitable HMI message.

Table 11: Additional Safety Objectives (functionality and performance) in the case of internal failures

2.8.2 Derivation of Safety Objectives (integrity/reliability)

The method to calculate SO for a given hazard is as follows, see [2]:

$$SO = \frac{MTFoO_{relevant\_severity\_class}}{N \times IM}$$

where:

- $MTFoO_{relevant\_severity\_class}$ stands for the Maximum Tolerable Frequency of Occurrence being the maximum probability of the hazard's effect as defined in Table 6 in Guidance [2].
- N is the overall number of operational hazards for a given severity class at a given barrier as obtained from Table 5, Guidance [2].
- IM is the Impact Modification factor to take account of additional information regarding the operational effect of the hazard, in particular related to the number of aircraft exposed to the operational hazard. The value was determined through expert judgment and in accordance with the Guidance [2] [9].
- We assume that 1 SOH equals 6 flt hr.

The Safety Objectives (integrity/reliability) follow the numbering scheme of the related OH and the SO (success approach). 100 was added to the id-number to discern them.

ID	Safety objective description	Severity Class	Related OH	Safety objective / flt hr	N	IM	Safety Objective / SOH
SO#106	The likelihood that ATC fails to build arrival sequence shall be no more than:	SC4b	OH#06	3.3e-4	30	1	2e-3
SO#107	The likelihood that ATC fails to insert and sequence an emergent flight at the Eligibility Horizon shall be no more than:	SC4b	OH#07	3.3e-4	30	1	2e-3
SO#108	The likelihood that ATC fails to adjust AMAN to relevant operational needs and parameters shall be no more than:	SC4b	OH#08	3.3e-4	30	1	2e-3
SO#110	The likelihood that ATC fails to update the	SC4b	OH#10	3.3e-4	30	1	2e-3

[9] The expert panel chose value 1 for all but one OH, the reasoning being that it is judged as unlikely that more than a few aircraft would be affected at any one time, or that additional aggravating or extenuating circumstances would be present. The exception is OH#126 where value of 10 was chosen as the effect will impact the entirety of arrival traffic.

	sequence to account for new relevant or important information shall be no more than:						
SO#111	The likelihood that ATC fails to assess need for delay to a newly sequenced flight shall be no more than:	SC4b	OH#11	3.3e-4	30	1	2e-3
SO#112	The likelihood that ATSU En-route fails to deliver the implemented sequence to ATSU Approach shall be no more than:	SC4b	OH#12	3.3e-4	30	1	2e-3
SO#114	The likelihood that ATSU En-route fails to apply AMAN advisories shall be no more than:	SC4b	OH#14	3.3e-4	30	1	2e-3
SO#122	The likelihood that ATSU En-route fails to monitor traffic and to ensure that AMAN times are being met shall be no more than:	SC4b	OH#22	3.3e-4	30	1	2e-3
SO#123	The likelihood that ATSU Approach fails to control traffic in Arrival Sequence as delivered by ATSU En-route shall be no more than:	SC4b	OH#23	3.3e-4	30	1	2e-3
SO#124	The likelihood that ATSU Approach fails to apply AMAN advisories to traffic as delivered by ATSU En-route shall be no more than:	SC4b	OH#24	3.3e-4	30	1	2e-3
SO#126	The likelihood that Airspace design insufficient to support the concept shall be no more than:	SC4b	OH#26	3.3e-4	30	10	2e-4

Table 12: Safety Objectives (integrity/reliability)

2.9 Impacts on adjacent airspace or on neighbouring ATM Systems

Airspace adjacent to the ATSU Destination is handled in this SAR under the header of Upstream ATSU, and as such the Upstream ATSU is tasked with the implementation of the sequence, see Table 6. In this capacity, Upstream ATSU is providing a service which benefits the Destination ATSU and traffic. Two preconditions are required to support this delegated service execution; a technical means to exchange information related to sequence build and implementation, and regulatory means to govern the provision of the service.

ID	Description
F&P SO#31	Upstream ATSU ATM system shall receive, process and display arrival management information.
F&P SO#32	Appropriate Letters of Agreement or Service Level Agreements shall be in place stipulating the duties of the Upstream ATSU with respect to sequence implementation.

Table 13: Additional Safety Objectives (functionality and performance) for Compatibility

2.10 Achievability of the Safety Criteria

Achievability of safety criteria was assessed through expert judgment. The experts were operational air traffic controllers who had day to day experience of baseline AMAN operations and participated as operational experts in V2 and V3 validation activities [11], [12] of SESAR AMAN into Multiple Airports.

Safety Criterion	Description	Achieved through	Validation Technique
SAC#4	There will be an 5% reduction in the number of ATC induced conflicts in the **TMA environment**	The criterion is achieved through the extension of the horizon as compared to the baseline AMAN. To quantify the effect in terms of reduction in conflicting trajectories, certain specific assumptions and generalizations of either model are necessary at this step: **Assumptions Baseline AMAN:** Assumed an eligibility horizon of ~20 minutes, baseline AMAN operation allows approximately 70 NM of flight distance to absorb delay. The horizon coincides approximately with the top of descent for the majority of high-level jet traffic. Approximately 75% of the route remaining to the metering point will occur at the descent speed, which optimally is operator selected but more realistically ATC assigned, with the proportion between the two growing in favour of ATC with increasing traffic density. **Assumptions SESAR Extended Horizon AMAN:** See assumption A-108 regarding operation of	Real Time Simulation

		prototype Extended AMAN in validation environment, provided by operational experts familiar with Extended AMAN validation exercises. **Assumptions regarding environment:** It is assumed that other factors such as traffic density, extent of use of vertical separation in inbound flows and airspace structure and flow organization, are the same for baseline AMAN and Extended AMAN. **Argument:** Based on these assumption, with an eligibility horizon of about 200NM, an extra 2-3 minutes delay absorption is possible without the need for holding as compared to the baseline AMAN, which corresponds to 8-12 NM depending on aircraft speed. Minimum inter-aircraft separation in cruise will be 10 but more commonly 5 NM depending on surveillance performance. Controller safety margins and in-trail spacing typically result in additional 3-5 NM, resulting in a spacing interval of around 10 NM in en-route cruise. A fully saturated, horizontally separated inbound flow will then contain around ten aircraft over the 100NM ~ 20 min extension. With additional 8-12 NM to absorb a delay need which otherwise would have to be absorbed by tactical control, this translates to roughly 10% reduction in potential tactical conflicts, including generous safety margins. This is well sufficient to meet the 5% criterion in almost any balanced demand-capacity scenario. This SAC is not directly impacted by CMAN but rather inherited from E-AMAN	
SAC#5	There will be **no increase in the number of ATC Induced conflicts in the en-route environment**	The extension of the arrival horizon with simultaneous accommodation of departures from nearby airports designated as satellites will result in a well organized, sequenced traffic flow in TMA. Expert judgment based on validation results indicates that neither the extension, nor the integration of these satellite departures will have a measurable impact on the conflict rate in en-route, assuming that assumptions A-002 and A-003 are taken into account and properly addressed. *Expert judgment indicates that while residual conflict rate in En-Route will remain approximately comparable between the baseline AMAN and the SESAR Extended AMAN, the implementation of the sequence will come at a lower ATCO workload enabling potential productivity gains at the ATC side (and possible cost reduction to the airspace users*	Real Time Simulation

		in terms of flight duration, delays and fuel burn). *This has been validated by EXE-778 of P05.04.02, [12]*	
SAC#7	There will be an 5% reduction in pre-tactical conflicts in the **TMA environment**	The extension of the arrival horizon (with simultaneous accommodation of departures from nearby airports designated as satellites) will allow for a sequenced flow in TMA. The magnitude of the reduction is dependent on local parameters such as traffic density and proportion of traffic originating from satellite airports as well as local airspace and AMAN configuration. Assumed that in peak or near-peak traffic density, the likelihood that a non-pre-sequenced (a.k.a pop-up) satellite departure will cause an overload and/or disturbance in the arrival sequence, thus increasing risk of potential conflict, approaches one, expert judgment estimates the reduction to between 15 and 25%. Note: A pop-up flight is considered a pre-tactical conflict in TMA as it occurs before En-route or TMA controllers execute any tactical control over the flight. This SAC is not directly impacted by CMAN but rather inherited from E-AMAN	Real Time Simulation

Table 14: Achievability of Safety Criteria

2.11 Validation & Verification of the Safety Specification

Safety objectives were obtained by P05.06.04 and P0.5.06.07 through breakdown of Operational Service definition provided in [6], using expertise of operational and safety personnel. Competences of panel members are indicated below:

Panel chair: Validation expert, ATM Systems engineer of 8 years.

Panel member #1: ATM Safety and Quality assurance expert of 7 years.

Panel member #2: Former ATC En-Route qualification of 20 years followed by Safety expert – accidents investigation of 15 years. Operational expertise in Arrival traffic management.

Panel member #3: Valid ATC En-Route and Approach of 21 years, Operational expertise in Arrival traffic management and ATC systems of 15 years.

Panel associate member #1: Aircraft Safety and Airworthiness expert, P16.06.01 delegate

Panel associate member #2: ATM Systems engineer and SESAR PFP, P05.06.07 delegate

Panel associate member #3: ATM Systems engineer, interoperability expert

This work has been supplemented by P05.04.02 regarding the implications of TS-0303 by licenced TMA and en-route controllers as well as ATM experts of 10+ years experience in Arrival Management applications.

Consolidated lists of Safety Objectives for either approach are provided in Appendix A.

3 Safe Design at SPR Level

3.1 Scope

The scope of this chapter includes standard steps addressed from chiefly an operational perspective:

- Description of SPR level model
- Derivation of Safety Requirements (Functional and Performance) from Safety Objectives.
- Thread analyses of the SPR-level model for normal and abnormal operating conditions and derivation of related additional Safety Requirements (Functional and Performance)
- Analysis of system induced hazards and their causes through the application of H-FTA
- Derivation of Safety Requirements (Integrity and Reliability)
- Assessment of Achievability of Safety Criteria and Requirements.

3.2 The SPR-level Model

3.2.1 Description of SPR-level Model

For the ETMA process model please refer to section 5.1

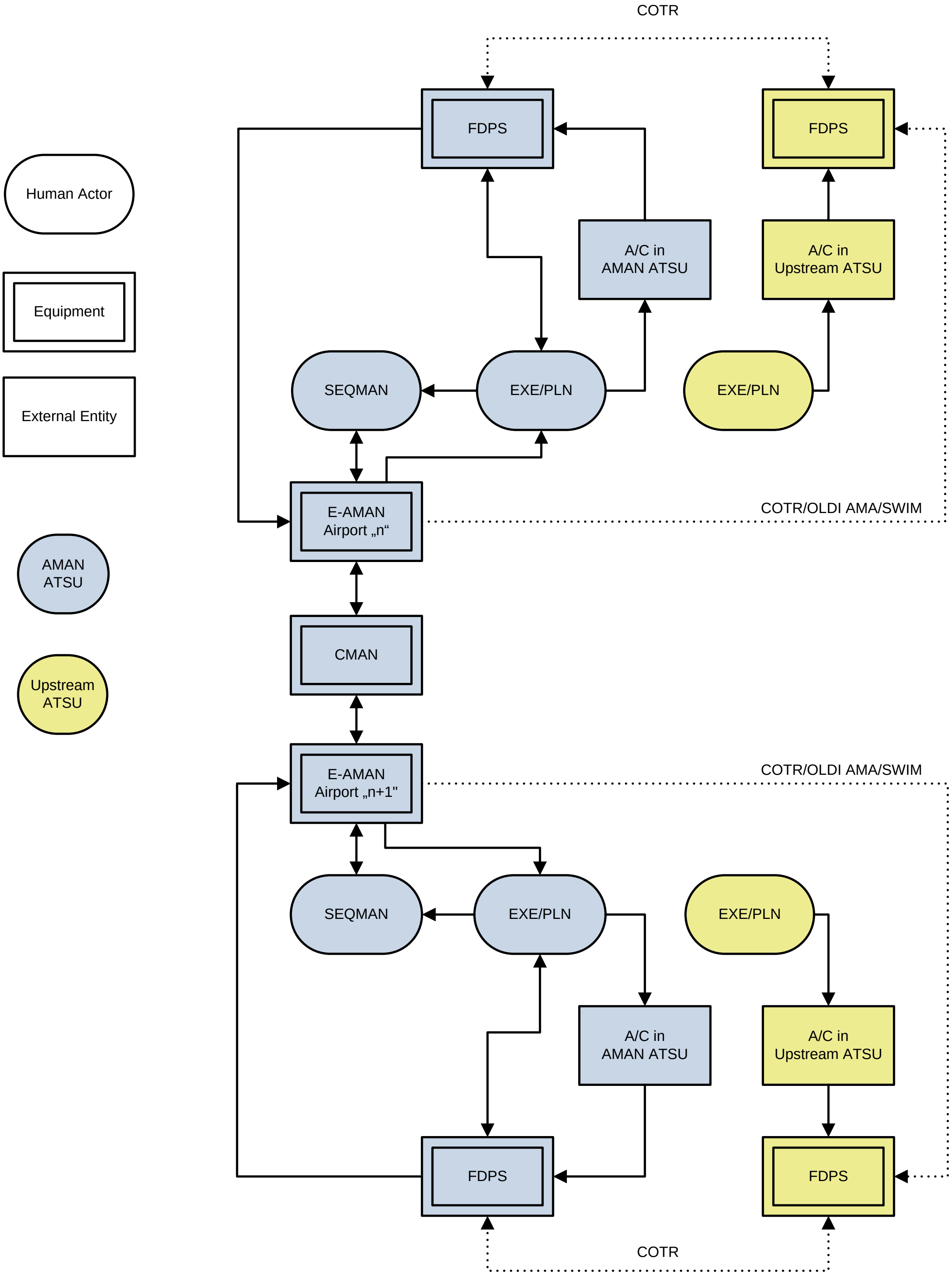

Figure 8 TS-0303 SPR-level Model

Table 15 below gives an exhaustive list of all human roles, equipment, interfaces and external entities pertinent to the SPR level diagrams. See definitions in following chapters.

Element	Class	Domain
SEQ_MAN	Human	Ground
E-AMAN	Equipment	Ground
CMAN	Equipment	Ground
EXE/PLN ATSU DEST	Human	Ground
EXE/PLN ATSU Upstream	Human	Ground
FDPS	Equipment	Ground
COTR	Interface	Ground-Ground

Table 15 Definition of SPR level model elements

3.2.1.1 Aircraft Elements

Not applicable

3.2.1.2 Ground Elements

The functional design defines the ground domain in four separate nodes where distinct services of the operating method are centralized. The nodes are supported by a common infrastructure of equipment and interfaces. The positions are:

- AMAN
- CMAN
- ATSU Upstream
- ATSU Destination

HUMAN:

SEQ_MAN

SEQ_MAN – Sequence Manager – is a role defined in the functional design. The role is responsible for supervision and executive control of the AMAN tool, the setting and execution of the overall Arrival Management strategy and responsibility for the planning of the arrival sequence. Sequence manager operates AMAN through a HMI, and interfaces with other positions using Coordination and Transfer. It is not envisaged for Sequence Manager to interface directly with traffic using voice or datalink.

Note: The Sequence Manager role may be aggregated with other controller roles in one position as determined locally.

Upstream EXE/PLN

Upstream Executive – Planner role is allocated to and provides ATC service in sectors of an ATSU that:

a) is directly involved in the implementation of the sequence

AND

b) does not have responsibility for the destination airport

Upstream EXE/PLN interaction with other ATSU actors is determined by the implementation of the supporting Coordination and Transfer. There will be a two way COTR link to the Destination ATSU and one-way (receive) or two-way interface with AMAN equipment. The role uses voice R/T communicate with traffic.

Destination EXE/PLN

Destination Executive – Planner role is allocated to and provides ATC service in the ATSU that has responsibility for the destination airport. Likewise, the role uses R/T voice for air-ground communication, COTR for coordination with other ATSU's and COTR or direct contact with SEQ_MAN and other controllers in own ATSU. It uses AMAN HMI and interacts two-way with AMAN through functionality in its Controller Working Position (CWP).

EQUIPMENT:

AMAN

Arrival Manager retrieves operational configuration and operational parameters such as active runway configuration, desired throughput rates, service data from other collaborating systems and weather forecasts and/or observations. Flight information is provided to AMAN continuously either via a direct connection or COTR from the ATSU Destination FDPS. Its operational configurations define among other items the horizons in terms of flight time remaining. AMAN interfaces with and is supervised and operated by SEQ_MAN. AMAN also interfaces with all concerned EXE/PLN positions, Destination or Upstream either via COTR, other specific equipment or other means. It receives updated Arrival Management Info from CMAN. AMAN is responsible for a number of key tasks, defined under Procedure.

CMAN

CMAN receives Arrival Management Information from each destination Airport AMAN in the Multi-Airport Environment. It predicts the amount of bunching in E-TMA en-route sectors where inbound streams converge. To prevent bunching, updated Arrival Management Information is sent back to the individual AMANs.

FDPS

Each ATSU is equipped with own instance of Flight Data Processing System, FDPS; its tasks are unchanged from the previous operating method, including providing flight information and other service data to the AMAN. FDPS interfaces with controllers using CWP.

CWP

Each EXE/PLN is working at a Controller Working Position, CWP. The position concentrates all equipment, interfaces and support tools defined for the specific EXE/PLN role. Additionally, the CWP should implement and integrate an intuitive means of interaction with AMAN.

COTR (Equipment enabling Coordination and transfer)

All EXE/PLN positions utilize Coordination and Transfer by any means available including telephony, integrated display functionality, direct contact and other, to communicate with each other and with SEQ_MAN.

PROCEDURE:

This section describes the procedures taking place in the ground domain. For each procedure we state Owner – the role that the procedure is allocated to, and Equipment – the piece of equipment that is most prominently associated with the procedure.

ATC Sequence build and spacing

Owner: SEQ_MAN

Equipment: AMAN

AMAN receives continuous update of the air picture from FDPS and determines for each flight actual flight time remaining to runway threshold. When a flight is determined as approaching the eligibility horizon, AMAN inserts the flight in the sequence in compliance with the applicable rules, strategies and operational parameters. The sequence is updated each time any item of information is received that has an impact on the sequence. Note that AMAN works solely in the time dimension; the geographical position and location of the aircraft has no bearing on the sequence update beyond the application of strategies that depend on position[10] or location[11]. SEQ_MAN supervises the sequence, receives input from EXE/PLN and makes arbitrary updates as deemed necessary. When it is determined that sufficient spacing cannot be guaranteed in the natural sequence, AMAN will, in accordance with applicable rules and strategies, assess the need for delay or gain of individual flights, update the sequence accordingly and if the flight has passed the Active Advisory Horizon, AMAN will publish the arrival management to the respective EXE/PLN role, having regard for engaged delay sharing strategies.

ATC Sequence implementation

Owner: EXE/PLN

Equipment: CWP

EXE/PLN roles receive updated sequence information in their CWP and implement the determined sequence order and spacing based on the provided delay information. In the context of this SAR there is only one format considered, as CTA etc. are not considered.

- *AMAN advisory*

  This format is the default format generally applicable to all flights. It is published to the controller using a suitable notation and the controller implements ("applies") the advisory using any means of traffic control available; typically speed instructions, vectors, use of holding patterns and similar.

EXE/PLN in coordination with SEQ_MAN continue to monitor the sequence, make adjustments to it as necessary and continually deliver the spaced and established sequence to the approach controllers.

[10] Position may be considered in an ATC Strategy where cross border interoperability issues lead to an uneven horizon.

[11] Location may be considered in an ATC Strategy for flights departing out of satellite airports, if e.g. it is determined that such flights require a spacing that is different from that of en-route flights.

INTERFACE:

Two way voice R/T

All EXE positions use voice R/T for air-ground communication.

COORDINATION AND TRANSFER

Coordination and transfer is used between controller roles to coordinate with one another concerning sequence implementation matters.

AMAN-FDPS

This interface is used for communication of traffic information from FDPS to AMAN, and for AMAN advisories from AMAN to FDPS, to be displayed to respective CWP.

This interface is largely implementation dependent. For instance, it is possible for AMAN to use trajectory predictions in part or in full extent as provided by FDPS, or to only use select flight plan data and to produce own predictions. In the other direction, AMAN may communicate directly with CWPs or interoperate with FDPS to have its information present to the controllers integrated in the air situation picture as generated by FDPS. AMAN may even interface with Surveillance Data Processing System (SDPS) directly or via FDPS to receive traffic position updates.

AMAN HMI

AMAN HMI is the interface between controllers on one side, SEQ_MAN and EXE/PLN, and AMAN on the other side. The interface allows exchange of information both ways between AMAN and SEQ_MAN, and one-way or two-way between AMAN and EXE/PLN, as determined by local implementations.

CWP HMI

Controller working position is the aggregation of interfaces between EXE/PLN and all other system elements.

3.2.1.3 External Entities

Classification of external entities is partially dependent on implementation. At the very least, the following entities can be classified as external, under the principle that they do not actively impact the concept under normal operation, yet their failure will have an appreciable safety impact.

Traffic En-route

Traffic En-Route has a passive role in AMAN advisories, the implementation of which is transparent to the traffic.

Surveillance Data Processing System (SDPS)

SDPS generates traffic identity and position information which is used throughout the chain for countless purposes, most notably Trajectory Prediction and Coordination-Transfer. Failure of SDPS will result in a major disturbance to the entire ATC process and in comparison, its impact on the Arrival Management function will be dependent on local assumptions and mitigation means. In the context of this SAR this eventuality is handled through mitigation MM-01 expressed in assumptions A-006 and A-007 which empower ATC to partly or fully suspend arrival management operations in favour of separation provision and safety assurance.

DCB and Network Management (not shown in diagrams, see assumption A-110)

DCB and Network Management are strategic functions with the key objective to ensure that day to day demand for the Arrival Management process does not exceed its capacity, derived from the airport and airspace capacity of the constituents of the process.

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

Safety Objectives ***(Functionality and Performance from success approach)***	**Requirement** ***(forward reference)***	**Maps on to**
SO#06	E-AMAN shall build arrival sequence. [SR-01]	E-AMAN
	AMAN ATSU shall provide E-AMAN with flight information regarding all flights inbound to the destination airport. [SR-02]	FDPS
	AMAN ATSU shall provide E-AMAN with flight information regarding an arriving flight when the flight reaches the defined Eligibility Horizon. [SR-03]	FDPS
	Flight data distribution shall ensure that flight information provided to E-AMAN shall be correct and accurate. [SR-04]	FDPS
	Sequence Manager shall supervise and control E-AMAN [SR-05].	SEQ_MAN
	E-AMAN shall provide CMAN with correct and accurate arrival management information. [SR-54]	E-AMAN
	CMAN shall provide E-AMAN with correct and accurate adjusted arrival management information. [SR-55]	CMAN
SO#07	E-AMAN shall insert a representation of an inbound flight reaching the Eligibility Horizon in the sequence in accordance	E-AMAN

	with applicable rules and strategies. [SR-06]	
SO#08	SEQ_MAN shall adjust control parameters of E-AMAN to reflect actual and planned operational conditions. [SR-07] SEQ_MAN shall have the authority to select and engage ATC strategies. [SR-08]	SEQ_MAN SEQ_MAN
SO#10	E-AMAN shall update the sequence to account for new and relevant information. [SR-11] SEQ_MAN shall introduce changes and adjustments to the sequence as deemed necessary for safe and expedient flow of inbound traffic. [SR-12] SEQ_MAN shall use COTR to coordinate with other controllers regarding sequence build as required. [SR-13]	E-AMAN SEQ_MAN SEQ_MAN
SO#11	For each inserted flight E-AMAN shall assess whether there exists a need to delay or expedite the flight so as to comply with the required traffic flow parameters. [SR-14] For each inserted flight CMAN shall assess whether there exists a need to delay the flight to prevent bunching. [SR-53]	E-AMAN CMAN
SO#12	SEQ_MAN shall introduce changes and adjustments to the sequence as deemed necessary for safe and expedient flow of inbound traffic. [SR-16] SEQ_MAN shall use COTR to coordinate with other controllers regarding sequence build as required. [SR-13] EXE/PLN En-Route sector controllers shall implement the sequence and delay/expedition of flights before flights reach coordination point with Approach sectors. [SR-18]	SEQ_MAN SEQ_MAN EXE/PLN ATSU Upstream/DEST
SO#14	En-Route controllers shall apply AMAN advisories (TTL/TTG) to flights under their control. [SR-20]	EXE/PLN ATSU Upstream/DEST
SO#22	En-Route controllers shall continuously monitor traffic in their sectors and ensure that the AMAN advisories are complied with. [SR-38]	EXE/PLN ATSU Upstream/DEST
SO#23	Following handover of traffic from En-Route sectors, Approach controllers shall continuously monitor traffic in their sectors and ensure that the AMAN advisories are complied with. [SR-39]	EXE/PLN ATSU DEST

SO#24	Controllers shall apply AMAN advisories (TTL/TTG) to flights under their control. [SR-20]	EXE/PLN ATSU DEST
SO#29	Quality of trajectory prediction used by E-AMAN to build the sequence shall be sufficient to support concept operation. [SR-44]	TP
SO#30	E-AMAN shall continuously monitor and diagnose its operation. [SR-45] E-AMAN shall continuously monitor the quality of its input data. [SR-46] E-AMAN shall alert SEQ_MAN by means of a suitable HMI message if it determines that its operation or quality of its input data are suspect. [SR-47]	E-AMAN E-AMAN E-AMAN
SO#31	Upstream ATSU ATM system shall receive, process and display arrival management information. [SR-48]	ATSU Upstream
SO#32	*Assumption A-009*	OUT OF SCOPE
SO#33	E-AMAN configuration shall provide functionality to define rules to govern potential overtake situations, as functions of route, aircraft type and its associated performance characteristics, distance-to-go, downlinked aircraft parameters if available, strategic prioritization, other data sources as available. [SR-49]	E-AMAN
SO#34M	CMAN shall continuously monitor and diagnose its operation. [SR-50] CMAN shall continuously monitor the quality of its input data. [SR-51] CMAN shall alert SEQ_MAN by means of a suitable HMI message if it determines that its operation or quality of its input data are suspect. [SR-52]	CMAN CMAN CMAN

Table 16: Mapping of Safety Objectives to SPR-level Model Elements

Table 17 below gives the reordered list of derived Safety Requirements – Functionality and Performance

Safety Requirement (functionality & performance)	**Requirement**	**Derived from Table 10**
SR-01	E-AMAN shall build arrival sequence.	SO#06
SR-02	AMAN ATSU shall provide E-AMAN with flight information regarding all flights inbound to the destination airport.	SO#06
SR-03	AMAN ATSU shall provide E-AMAN with flight information regarding an arriving flight when the flight reaches the defined	SO#06

	Eligibility Horizon.	
SR-04	Flight data distribution shall ensure that flight information provided to E-AMAN shall be correct and accurate.	SO#06
SR-05	Sequence Manager shall supervise and control E-AMAN.	SO#06
SR-06	E-AMAN shall insert a representation of an inbound flight reaching the Eligibility Horizon in the sequence in accordance with applicable rules and strategies.	SO#07
SR-07	SEQ_MAN shall adjust control parameters of E-AMAN to reflect actual and planned operational conditions.	SO#08
SR-08	SEQ_MAN shall have the authority to select and engage predefined ATC strategies reflecting sets of rules according to which to build the sequence. [SR-08]	SO#08
SR-11	E-AMAN shall update the sequence to account for new and relevant information.	SO#10
SR-12	SEQ_MAN shall introduce changes and adjustments to the sequence as deemed necessary for safe and expedient flow of inbound traffic.	SO#10
SR-13	SEQ_MAN shall use COTR to coordinate with other controllers regarding sequence build as required.	SO#10 SO#12
SR-14	For each inserted flight E-AMAN shall assess whether there exists a need to delay or expedite the flight so as to comply with the required traffic flow parameters.	SO#11
SR-16	SEQ_MAN shall introduce changes and adjustments to the sequence as deemed necessary for safe and expedient flow of inbound traffic.	SO#12
SR-18	EXE/PLN En-Route sector controllers shall implement the sequence and delay/expedition of flights before flights reach coordination point with Approach sectors.	SO#12
SR-20	En-Route controllers shall apply AMAN advisories (TTL/TTG) to flights under their control.	SO#14 SO#24
SR-38	En-Route controllers shall continuously monitor traffic in their sectors and ensure that the AMAN advisories are complied with.	SO#22
SR-39	Following handover of traffic from En-Route sectors, Approach controllers shall continuously monitor traffic in their sectors and ensure that the AMAN advisories are complied with.	SO#23
SR-44	Quality of trajectory prediction used by E-AMAN to build the sequence shall be sufficient to support concept operation.	SO#29

SR-45	E-AMAN shall continuously monitor and diagnose its operation.	SO#30
SR-46	E-AMAN shall continuously monitor the quality of its input data.	SO#30
SR-47	E-AMAN shall alert SEQ_MAN by means of a suitable HMI message if it determines that its operation or quality of its input data are suspect.	SO#30
SR-48	Upstream ATSU ATM system shall receive, process and display arrival management information.	SO#31
SR-49	E-AMAN configuration shall provide functionality to define rules to govern potential overtake situations, as functions of route, aircraft type and its associated performance characteristics, distance-to-go, downlinked aircraft parameters if available, strategic prioritization, other data sources as available.	SO#33
SR-50	CMAN shall continuously monitor and diagnose its operation.	SO#34M
SR-51	CMAN shall continuously monitor the quality of its input data.	SO#34M
SR-52	CMAN shall alert SEQ_MAN by means of a suitable HMI message if it determines that its operation or quality of its input data are suspect.	SO#34M
SR-53	For each inserted flight CMAN shall assess whether there exists a need to delay the flight to prevent bunching.	SO#11
SR-54	E-AMAN shall provide CMAN with correct and accurate arrival management information	SO#06
SR-55	CMAN shall provide E-AMAN with correct and accurate adjusted arrival management information.	SO#06

Table 17: Derivation of Safety Requirements (functionality and performance) from Safety Objectives

The following assumptions were made in deriving the above Safety Requirements (Functionality and Performance):

ID	Assumptions
A-002	Airspace design is optimized to the greatest extent possible to facilitate concept operation. Common key areas of interest exist in the location of merging points, metering points and coordination points.
A-003	Airspace design excludes danger and restricted areas (D, R and other forms of restrictions such as TSA, Prohibited airspace, “No fly zones” etc) to the extent where they would interfere with the provision of the service. Where exclusion of such areas cannot be accomplished, airspace design shall define mitigation means such as alternate arrival routes circumventing the segregated areas.
A-006	At any point if the controller deems the sequence unworkable, tactical control shall

	be established. This assumption is grounded in baseline method: *F&P SO#01 ATC shall control aircraft arriving in his sector and ensure safe separation from other traffic*
A-007	When the controller has determined that the sequence has become unworkable, coordination shall take place to inform impacted controllers including the sequence manager as required.
A-009	Appropriate Letters of Agreement or Service Level Agreements shall be in place stipulating the duties of the Upstream ATSU with respect to sequence implementation.
A-010	Flight crew is advised with respect to the expected STAR/RWY before the provision of the service commences. This assumption is grounded in baseline method: *F&P SO#02 ATC shall provide STAR/RWY to the A/C* *F&P SO#03 A/C shall receive STAR/RWY*
A-011	Ground and air trajectories are updated with the expected STAR/RWY. This assumption is grounded in baseline method: *F&P SO#04 ATC shall update Ground Trajectory with the STAR/RWY* *F&P SO#05 A/C shall update Air Trajectory with the STAR/RWY*
A-013	Independent of the delay situation, ensuring separation and reaching Letters of Agreement exit conditions must always be prioritized over the pre-sequencing task.

Table 18: Assumptions made in deriving the above Safety Requirements

3.3 Analysis of the SPR-level Model – Normal Operational Conditions

The OSED [10] defines Normal operating scenario based on conducted validation exercise design.

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

The table below gives a set of additional safety requirements (functionality and performance) obtained through analysis of the SPR level model.

No impact on the function of safety nets was observed.

ID **[SPR-level Model element]**	**Description**	**Thread Action Number**
SEQ_MAN-N01	Sequence manager shall be able to arbitrarily assign a runway to a flight	generic scenario

SEQ_MAN-N02	Sequence manager shall prompt E-AMAN to recalculate an arbitrary portion of a stabilized sequence.	Generic scenario
E-AMAN-N01	E-AMAN shall make consistent use of best source of information for the following service data: - operational parameters - flight information - trajectory prediction	generic scenario
E-AMAN-N02	E-AMAN shall provide to SEQ_MAN at the minimum the following arrival management information: - value of advisory - sequence number - time ordered sequence - sequence filterable by runway/metering or feeder fix *Note: distance to go is an optional information item as per local implementation.*	Generic scenario
E-AMAN-N03	Configuration of E-AMAN shall be validated and verified prior to operational deployment.	Generic scenario
E-AMAN-N04	E-AMAN shall consider any change introduced in the sequence by SEQ_MAN as permanent unless prompted to recalculate by SEQ_MAN	generic scenario
E-AMAN-N05	E-AMAN shall continuously update estimated landing times for sequenced traffic	generic scenario
E-AMAN-N06	E-AMAN shall not automatically change order in the sequence to traffic having passed SSH.	Generic scenario
E-AMAN-N07	E-AMAN shall not constrain a flight by an advisory when it is determined that there is no need for delay.	Generic scenario
E-AMAN-N08	E-AMAN shall indicate explicitly to SEQ_MAN and ATCO an intentionally unconstrained flight.	generic scenario
E-AMAN-N09	E-AMAN shall determine and assign runway to a flight in accordance with a predefined runway utilization strategy.	Generic scenario
ATCO-N01	Controllers in any involved ATSU (Upstream and Destination) shall coordinate with SEQ_MAN with respect to desired changes in sequence as required.	Generic scenario
CMAN-N01	Configuration of CMAN shall be validated and verified prior to operational deployment.	Generic scenario

Table 19: Additional SR from Thread Analysis – Normal Operational Conditions

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

The abnormal operational conditions identified by P05.06.04 and P05.06.07 were confirmed to be applicable for TS-0303 in several single-day real-time simulations conducted by P05.04.02.

3.4.1 Scenarios for Abnormal Conditions

AC ID	Scenario	Rationale for inclusion
AC#1	Aircraft emergency	6.7.1
AC#2	planned RWY closure	6.7.1
AC#3	unplanned RWY closure	6.7.1
AC#4	planned RWY change	6.7.1
AC#5	unplanned RWY change	6.7.1
AC#6	sudden change in WX	6.7.1
AC#7	severe WX	6.7.1
AC#8	sudden activation of restricted airspace	6.7.1
AC#9	low-performance aircraft	6.7.1
AC#10	TCAS RA occurs	6.7.1

Table 20: Operational Scenarios – Abnormal Conditions

3.4.2 Derivation of Safety Requirements (Functionality and Performance) for Abnormal Conditions

Ref	**Abnormal Conditions / SO** *(Functionality and Performance)*	Mitigations (SR 0xx and/or A 0xx)
AC#1	F&P SO#01 F&P SO#10	A-006, A-007 SR-12
AC#2	F&P SO#08 F&P SO#10	SR-07, SR-08, SR-12
AC#3	F&P SO#01 F&P SO#08 F&P SO#10	A-006, A-007 SR-07, SR-08, SR-12

AC#4	F&P SO#08 F&P SO#10	SR-07, SR-08, SR-12
AC#5	F&P SO#01 F&P SO#08 F&P SO#10	A-006, A-007 SR-07, SR-08, SR-12
AC#6	F&P SO#01 F&P SO#08 F&P SO#10	A-006, A-007 SR-07, SR-08, SR-12
AC#7	F&P SO#01 F&P SO#08 F&P SO#10	A-006, A-007 SR-07, SR-08, SR-12
AC#8	F&P SO#01 F&P SO#08 F&P SO#10	A-002, A-003
AC#9	SO#10	A-006, A-007, SR-12
AC#10	F&P SO#01 F&P SO#10	A-006, A-007

Table 21: Safety Requirements or Assumptions to mitigate abnormal conditions

3.4.3 Thread Analysis of the SPR-level Model - Abnormal Conditions

3.4.3.1 Scenario AC#01

In non-standard specific cases such as a declared emergency scenario but also including lower level of distress categories such as urgency, medical urgency or low fuel urgency, there is an operational need to arbitrarily prioritize the workflow in the impacted sector and its dependents. The impacted flight(s) would be prioritized tactically, with the overarching Separation Assurance task taking full precedence over sequence implementation matters. As a consequence, it is necessary for E-AMAN to relinquish all control or advice concerning the impacted flight(s). E-AMAN shall therefore:

- Allow SEQ_MAN to assign, if required, a special designation to a flight and upon SEQ_MAN doing so, remove the flight from the sequence but retain it in its database in case a re-insertion is desirable at a later stage. [SR-A02], [SR-A03]
- Allow SEQ_MAN to permanently delete a flight from the sequence. [SR-A05]
- Allow SEQ_MAN to reserve a time slot of arbitrary length (buffer) at an arbitrary runway. [SR-A01]

3.4.3.2 Scenario AC#02, AC#04

When a planned runway closure or change occurs for reasons such as snow clearance, debris inspection or external unavailability, it is necessary for the event to be reflected in E-AMAN plan. SEQ_MAN introduces the planned change in operating conditions via SR-07, SR-08, SR-12. The event is considered fully covered by existing SR.

3.4.3.3 Scenario AC#03, AC#05

An unplanned sudden runway change or closure is in effect no different from a planned closure or change except that the event is introduced with immediate effect. SEQ_MAN introduces the new operating conditions by way of SR-07, SR-08, SR-12. Flights to which an update of sequence is still permissible shall have their times updated as per SR-11. Flights to which an update is no longer permissible, i.e. primarily those having already passed the metering fix shall be handled tactically with Separation Assurance service prioritized. Some may be inserted manually as per [SR-A04] triggering a subsequent sequence update as per SR-11, others will receive full tactical control. Removals from sequence shall occur as per [SR-A05] the SEQ_MANs discretion.

3.4.3.4 AC#06 AC#07

Weather related phenomena shall be handled via SR-07, SR-08, SR-12, with tactical control afforded where necessary as per A-006 and A-007. The scenarios are considered fully covered by existing SR.

3.4.3.5 AC#08

As airspace design is almost exclusively out of scope of tactical traffic management, sudden activation of restricted airspace should be avoided as far as possible through airspace design in accordance with A-002 and A-003 and where that cannot be achieved, mitigations should be provided as per A-003. SEQ_MAN shall then handle the changed parameters by way of SR-07, SR-08, SR-12. The scenario is considered fully covered by existing SR and assumptions.

3.4.3.6 AC#09

Low performance aircraft should be handled tactically. It may be necessary for SEQ_MAN to reserve the runway for an arbitrary period of time as per [SR-A01], and for SEQ_MAN and E-AMAN to remove the flight from the sequence as per [SR-A02] and [SR-A03].

3.4.3.7 AC#10

TCAS-RA is typically a short term event associated with the function of a safety net. As such, it receives priority and if any conflict with tactical traffic management matters occurs, the scenario is resolved in full compliance with A-006 and A-007.

3.4.4 Effects on Safety Nets – Abnormal Operational Conditions

No impact found on airborne or ground-borne safety nets.

3.4.5 Dynamic Analysis of the SPR-level Model – Abnormal Operational Conditions

n/a

3.4.6 Additional Safety Requirements – Abnormal Operational Conditions

The abnormal operational conditions identified by P05.06.04 and P05.06.07 were confirmed to be applicable for TS-0303 in several single-day real-time simulations conducted by P05.04.02.

ID **[SPR-level Model element]**	**Description**	**Thread Action Number [Scenario # xx]**
SR-A01	SEQ_MAN shall insert a tactical reservation of arbitrary length in the sequence to account for abnormal cases such as low performance aircraft or short term runway closure.	AC#01 AC#03 AC#09
SR-A02	SEQ_MAN shall designate a flight in case of special treatment is necessary.	AC#01 AC#09
SR-A03	E-AMAN shall exclude from sequencing a flight designated by SEQ_MAN for special treatment.	AC#01 AC#09
SR-A04	SEQ_MAN shall manually define and insert a flight in the sequence.	AC#03 AC#05
SR-A05	SEQ_MAN shall manually remove a flight from the sequence.	AC#01 AC#03 AC#05

Table 22: Additional Safety Requirements from Thread Analysis – Abnormal Operational Conditions

3.5 Design Analysis – Case of Internal System Failures

3.5.1 Causal Analysis

Hybrid Fault Tree Analysis (HFTA) was applied in derivation of quantitative and qualitative safety requirements.

Hybrid Fault Tree Analysis (H-FTA) is considered superior to other methods due to its treatment of human error not as a failure to which a quantitative objective and requirement could be associated, instead as an inherent property of the design of the human factor. A property that can be alleviated or mitigated by suitable design choices in the development of the system or concept.

Identify Matching Point between AIM and Top Event (Step 1)

Applicable AIM: MAC. All top events (see Appendix D) were determined to reside within Barrier 10 “Inadequate Traffic Synchronization of Arrivals”. Individual fault trees for each top event followed the relationship indicated by AIM: MAC between the two children of the matching event: Inadequate Synchronization Information and Inadequate Synchronization Task.

Set Top Event Severity Classification (Step 2)

Using the AIM built-in Severity Classification Scheme as per SRM Guidance E.

MAC-SC4b MTFoO = 1e-2 per flight hour.

Top event in the fault tree correspond to each individual Safety Objective (Integrity and Reliability).

See attribution of Safety Severity Classes to top level events according to HFTA.

Allocate SAFETY SEVERITY Class for lower level event (Step 3)

See attribution of Safety Severity Classes to lower level events according to HFTA.

Allocate Qualitative / Quantitative Safety Requirements (Step 4)

This section provides a list of causes, per SPR-model level element, identified in the HFTA causal analysis, together with the associated operational hazards. The specific list of causes can be found in Appendix D. Associated Safety Requirements are set in 7.5.4.

Cause ID	Cause description	H-FTA SSC	Related OH
	CMAN		
CMAN-001	CMAN is not available or unserviceable. [3.3e-4 SOH]	Minor	OH#06 OH#07 OH#10
CMAN-002	CMAN incorrect assessment of need for delay. [2e-4 SOH]	Minor	OH#11
CMAN-003	CMAN is not available or unserviceable. [2e-4 SOH]	Minor	OH#11
CMAN-004	CMAN incorrect assessment of need for delay. [3.3e-4 SOH]	Minor	OH#14 OH#24
	E-AMAN		
E-AMAN-001	E-AMAN is not available or unserviceable. [3.3e-4 SOH]	Minor	OH#06 OH#07 OH#10
E-AMAN-002	E-AMAN operates on an incorrect time reference. [3.3e-4 SOH]	Minor	OH#07 OH#10 OH#14 OH#24
E-AMAN-003	E-AMAN fails to accept human input. [1e-3 SOH]	Minor	OH#08

E-AMAN-004	E-AMAN is not available or unserviceable. [2e-4 SOH]	Minor	OH#11
E-AMAN-005	E-AMAN operates on an incorrect time reference. [2e-4 SOH]	Minor	OH#11
E-AMAN-006	E-AMAN incorrectly assesses need for delay [2e-4 SOH]	Minor	OH#11
E-AMAN-007	E-AMAN incorrectly assesses need for delay [3.3e-4 SOH]	Minor	OH#14 OH#24
	SEQ_MAN		
SEQ_MAN-001	SEQ_MAN fails to supervise E-AMAN. [HIC: Low]	Minor	OH#06 OH#12 OH#14 OH#24
SEQ_MAN-002	SEQ_MAN makes an incorrect input. [HIC: Medium]	Minor	OH#08 OH#10 OH#12
	ATCO		
ATCO-001	ATCO fails a coordination task. [HIC: Medium]	Minor	OH#08 OH#10 OH#12
ATCO-002	ATCO fails to implement AMAN advisories. [HIC: Low]	Minor	OH#14 OH#24
ATCO-012	ATCO fails to monitor compliance with clearances related to implementation of advisories. [HIC:Low]	Minor	OH#22 OH#23
	FDPS		
FDPS-001	Incorrect flight information is provided by flight data processing system in ATSU Destination. [2.5e-4 SOH]	Minor	OH#06 OH#07 OH#10
FDPS-002	Incorrect flight information is provided by flight data processing system in ATSU Destination. [5e-4 SOH]	Minor	OH#11
	ATSU		
ATSU-001	ATSU Destination provides incorrect STAR/RWY information to SEQ_MAN/E-AMAN. [2.5e-4 SOH]	Minor	OH#08
ATSU-002	ATSU Destination provides incorrect landing rate information to SEQ_MAN/E-AMAN. [2.5e-4 SOH]	Minor	OH#08
ATSU-003	ATSU fails to define a correct ATC strategy. [2.5e-4 SOH]	Minor	OH#08
ATSU-004	ATSU fails to implement agreed delay sharing	Minor	OH#23

	strategy in AMAN configuration [2e-3 SOH]		
	COTR		
COTR-001	Coordination and Transfer equipment inoperative. [2.5e-4 SOH]	Minor	OH#06 OH#07 OH#10
	CWP-HMI		
CWP-HMI-001	CWP HMI fails to present AMAN advisories to the controller. [5e-4 SOH]	Minor	OH#14 OH#24
CWP-HMI-002	CWP HMI presents incorrect AMAN advisories to the controller. [5e-4 SOH]	Minor	OH#14 OH#24
	Trajectory Prediction		
TP-001	Inaccurate Trajectory Prediction information provided to E-AMAN. [2.5e-4 SOH]	Minor	OH#06 OH#07
TP-002	Trajectory Prediction information unavailable. [2.5e-4 SOH]	Minor	OH#06 OH#07
TP-003	Inaccurate Trajectory Prediction information provided to E-AMAN. [5e-4 SOH]	Minor	OH#11

Table 23 Identification of causes of internal failures

3.5.2 Common Cause Analysis

"Not applicable at SPR model level. The Common Cause Analysis should be considered as part of the physical level safety assurance activities to be handled by the technical project".

3.5.3 Formalization of Mitigations

Table below provides a list of mitigations identified in the course of derivation of system internal hazards, including the stage of safety objective definition. Mitigation means associated with a particular human operator task are provided by reference.

MM-ID	MM Definition	Related A-xxx/ Cause ID	Related OH	Related SR (forward ref)
MM-01	Controllers shall have the full discretion over the application and provision of the service. If at any point the controller deems the service inadequate or potentially compromising safe operation, the provision of separation assurance shall take utmost precedence over the provision of the traffic synchronization	A-006 A-007	OH#06 OH#07 OH#08 OH#10 OH#11	

	service. Controllers shall be trained to exercise this discretion.		OH#12 OH#14 OH#22 OH#23 OH#24 OH#26	
MM-02	E-AMAN shall be designed to facilitate coordination of sequence build and implementation related information between SEQ_MAN and EXE/PLN controllers active in or contributing to the implementation of the sequence.	ATCO-001	OH#08 OH#10 OH#12	SR-116
MM-08	Airspace design shall be optimized to the greatest extent possible to facilitate concept operation. Common key areas of interest exist in the location of merging points, metering points and coordination points. Airspace design excludes danger and restricted areas (D, R and other forms of restrictions such as TSA, Prohibited airspace, “No fly zones” etc) to the extent where they would interfere with the provision of the service	A-002 A-003		

3.5.4 Safety Requirements (integrity/reliability)

The table below gives an exhaustive listing of Safety Requirements – Integrity and Reliability. According to H-FTA guidance [3], definition of qualitative requirements addressing Human Factor is to be done by HP specialist in 16.6.5. The SAR team, on coordination with Safety Expert provided by P16.06.01 and in conjunction with the guidelines published in the above referred to guidance, elected to follow the following principles in addressing the human performance requirements

HIC	Interpretation	Requirement focus area
Low	The assessment found evidence of a highly effective concept present in the design.	Adequate training of the human operator in the specified task is sufficient to achieve the safety objective.
Medium	The assessment found evidence of an effective design or request for change in concept.	Adequate training of the human operator in the specified task coupled with associated adequate mitigation means is sufficient to achieve the safety objective.
High	The assessment found no evidence concerning design effectiveness. Open Issues and/or	Further validation is required to address Open Issues and Assumptions to achieve the safety objective.

	Assumptions requiring further attention and validation.	

Table 24 Principles for the formulation of qualitative requirements addressing human performance

Conversion to colloquial values is provided in the requirement definition for better readability, assuming continuous 24/7 E-AMAN operation.

SR	Safety Requirement	HP 16.6.5	Related Cause ID
	E-AMAN		
SR-101	The likelihood of E-AMAN being not available or unserviceable shall be no more than 2e-4 SOH, approximately once every 7 months.	N/A	E-AMAN-001 E-AMAN-004
SR-102	The likelihood of E-AMAN operating on an incorrect time reference shall be no more than 2e-4 SOH, approximately once every 7 months.	N/A	E-AMAN-002 E-AMAN-005
SR-103	The likelihood of E-AMAN failing to accept human input shall be no more than 1e-3 SOH, approximately once every 6 weeks.	N/A	E-AMAN-003
SR-104	The likelihood of E-AMAN incorrectly assessing need for delay shall be no more than 2e-4 SOH, approximately once every 7 months.	N/A	E-AMAN-006 E-AMAN-007
	SEQ_MAN		
SR-112	SEQ_MAN shall be trained to supervise E-AMAN.	Low	SEQ_MAN-001
SR-113	SEQ_MAN shall be trained with respect to correct input and operation of AMAN.	Medium	SEQ_MAN-002
	ATCO		
SR-115	Controllers shall be trained with respect to coordination tasks related to sequence implementation. *Mitigation provided by MM-02 –> SR-116.*	Medium	ATCO-001
SR-116	E-AMAN shall be designed to facilitate coordination of sequence build and implementation related information between SEQ_MAN and EXE/PLN controllers active in or contributing to the implementation of the sequence. *This is MM-02 providing mitigation of SR-115*	N/A	ATCO-001

SR-117	Controllers shall be trained with respect to implementation of AMAN advisories.	Low	ATCO-002
SR-127	Controllers shall be trained with respect to continuous monitoring and assessment of compliance with clearances related to implementation of AMAN advisories.	Low	ATCO-012
	FDPS		
SR-128	The likelihood that incorrect flight information is provided by flight data processing system in ATSU Destination shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.	N/A	FDPS-001 FDPS-002
	ATSU		
SR-131	The likelihood that ATSU Destination provides incorrect STAR/RWY information to SEQ_MAN/E-AMAN shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.	N/A	ATSU-001
SR-132	The likelihood that ATSU Destination provides incorrect landing rate information to SEQ_MAN/E-AMAN shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.	N/A	ATSU-002
SR-133	The likelihood that ATSU fails to define a correct ATC strategy shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.	N/A	ATSU-003
SR-134	The likelihood that ATSU fails to implement agreed delay sharing strategy in AMAN configuration shall be no more than 2e-3 SOH, approximately once every three weeks.	N/A	ATSU-004
	COTR		
SR-135	The likelihood that coordination and transfer equipment is inoperative shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.	N/A	COTR-001
	CWP-HMI		
SR-136	The likelihood that CWP HMI fails to present AMAN advisories to the controller shall be no more than 5e-4 SOH, approximately once every 12 weeks.	N/A	CWP-HMI-001
SR-137	The likelihood that CWP HMI presents incorrect AMAN advisories to the controller shall be no more than 5e-4 SOH, approximately once every 12 weeks.	N/A	CWP-HMI-002
	Trajectory Prediction		
SR-151	The likelihood that inaccurate Trajectory Prediction information is provided to E-AMAN shall be no more than	N/A	TP-001 TP-003

	2.5e-4 SOH, approximately once every 5.5 months.		
SR-152	The likelihood that Trajectory Prediction information is unavailable to E-AMAN shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.	N/A	TP-002
	CMAN		
SR-153	The likelihood of CMAN being not available or unserviceable shall be no more than 2e-4 SOH, approximately once every 7 months.	N/A	CMAN-001 CMAN-003
SR-154	The likelihood of CMAN incorrectly assessing need for delay shall be no more than 2e-4 SOH, approximately once every 7 months.	N/A	CMAN-002 CMAN-004

Table 25 Safety Requirements – Integrity and Reliability

3.6 Achievability of the SAfety Criteria

Following section 6.10, Safety Criteria are considered achievable if the mechanisms described therein can be demonstrated on the SPR level model underlying the Safety Requirements. The SPR level model was developed and validated iteratively in close cooperation with operational, safety and quality experts, as were all Safety Objectives and Operational Hazards and the derived Safety Requirements. This continuity is considered a sufficient guarantee that the Safety criteria will be achieved.

3.7 Realism of the SPR-level Design

3.7.1 Achievability of Safety Requirements / Assumptions

Safety requirements derived in this assessment target chiefly two domains; equipment and human factor.

Equipment related Safety Requirements are explicit (success approach) or quantified (failure approach). The lowest quantified failure rate corresponds to the order of 1e-4, therefore well within the range of typical reliability requirement imposed on equipment in civil aviation.

Human factor related Safety Requirements are explicit and qualitative in either approach, therefore considered fully achievable.

Thus, all requirements defined in this SAR are considered achievable.

3.7.2 “Testability” of Safety Requirements

As per Appendix C.1, Assumption A-105, physical level modelling is expected to take place in 10.01.07. Thus, it falls within the purview of said project to assess and report on the testability of the determined safety requirements.

3.8 Validation & Verification of the Safe Design at SPR Level

V2 and a V3 exercises [11] [12] were performed on TS-0303 within the scope of P05.04.02. Together with previous work within WP5 on TS-0305-A they form the basis for this report.

Of special note are real-time simulation exercises EXE-187,188 and 189 which contributed in a major share to the definition of the P05.06.07 OSED, EXE-485 and EXE-358 which evaluated an industrial prototype of E-AMAN, produced in 10.09.02, and most recently the ongoing EXE-695. In addition please refer to Section 6.11.

4 Detailed Safe Design at Physical Level

As per Appendix C.1, Assumption A-105, it was agreed at OFA to conduct the technical level, including physical modelling, in technical project 10.01.07. Consequently, this chapter is out of scope of this assessment.

Appendix A Consolidated List of Safety Objectives

A.1 Safety Objectives (Functionality and Performance)

ID	Description
F&P SO#01	*ATC shall control aircraft arriving in own sector and ensure safe separation from other traffic.*
F&P SO#02	*ATC shall determine the expected STAR/RWY combination for each arriving aircraft*
F&P SO#03	*ATC shall communicated the expected STAR/RWY combination to each arriving aircraft.*
F&P SO#04	*ATC shall update Ground Trajectory with the determined STAR/RWY combination.*
F&P SO#05	*A/C shall update Air Trajectory with the received STAR/RWY combination.*
F&P SO#06	ATC shall build arrival sequence
F&P SO#07	ATC shall insert flight reaching extended horizon into arrival sequence.
F&P SO#08	ATC shall adjust AMAN to operational needs, such as: runway in use, runway closure, landing rate.
F&P SO#10	ATC shall update Arrival Sequence accounting for new information that can impact the sequence
F&P SO#11	ATC shall assess the need for delay on arrival. *Note: Delay can be positive or negative.*
F&P SO#12	ATSU En-route shall deliver traffic sequenced and metered in the order as presented by AMAN, to ATSU Approach. *Note: ATC may introduce additional manual input in the AMAN sequence as required.*
F&P SO#14	ATSU En-route shall apply AMAN advisories (TTL/TTG).
F&P SO#22	ATSU En-route shall continually monitor traffic situation and ensure that the AMAN planned times are met.
F&P SO#23	ATSU Approach shall manage traffic in Arrival Sequence delivered by ATSU En-Route, ensuring that AMAN times and sequence order are maintained.
F&P SO#24	ATSU Approach shall apply AMAN advisories to traffic as delivered by ATSU En Route.
F&P SO#26	Airspace design shall be optimized to support the concept.

F&P SO#29	Quality of trajectory prediction used by AMAN to build the sequence shall be sufficient to support concept operation.
F&P SO#30	AMAN shall continuously monitor and diagnose its operation and the quality of its input data against all applicable criteria and alert the sequence manager by means of a suitable HMI message.
F&P SO#31	Upstream ATSU ATM system shall receive, process and display arrival management information.
F&P SO#32	Appropriate Letters of Agreement or Service Level Agreements shall be in place stipulating the duties of the Upstream ATSU with respect to sequence implementation.
F&P SO#33	Rules shall be defined as part of ATC Strategies in AMAN configuration to reflect principles governing overtake scenarios and using input information such as route, aircraft performance, onboard parameters and strategic prioritization.
F&P SO#34M	CMAN shall continuously monitor and diagnose its operation and the quality of its input data against all applicable criteria and alert the sequence manager by means of a suitable HMI message.

Table 26: Consolidated list of Safety Objectives (Functionality and Performance).

A.2 Safety Objectives (Integrity)

ID	Safety objective description	Safety Objective / SOH
SO#106	The likelihood that ATC fails to build arrival sequence shall be no more than:	2e-3
SO#107	The likelihood that ATC fails to insert and sequence an emergent flight at the Eligibility Horizon shall be no more than:	2e-3
SO#108	The likelihood that ATC fails to adjust AMAN to relevant operational needs and parameters shall be no more than:	2e-3
SO#110	The likelihood that ATC fails to update the sequence to account for new relevant or important information shall be no more than:	2e-3
SO#111	The likelihood that ATC fails to assess need for delay to a newly sequenced flight shall be no more than:	2e-3
SO#112	The likelihood that ATSU En-route fails to deliver the implemented sequence to ATSU Approach shall be no more than:	2e-3

SO#114	The likelihood that ATSU En-route fails to apply AMAN advisories shall be no more than:	2e-3
SO#122	The likelihood that ATSU En-route fails to monitor traffic and to ensure that AMAN times are being met shall be no more than:	2e-3
SO#123	The likelihood that ATSU Approach fails to control traffic in Arrival Sequence as delivered by ATSU En-route shall be no more than:	2e-3
SO#124	The likelihood that ATSU Approach fails to apply AMAN advisories to traffic as delivered by ATSU En-route shall be no more than:	2e-3
SO#126	The likelihood that Airspace design insufficient to support the concept shall be no more than:	2e-4

Table 27: Consolidated list of Safety Objectives (Integrity and Reliability).

Appendix B Consolidated List of Safety Requirements

B.1 Safety Requirements (Functionality and Performance)

Safety Requirement (functionality & performance)	Requirement	Derived from Table 10
SR-01	E-AMAN shall build arrival sequence.	SO#06
SR-02	AMAN ATSU shall provide E-AMAN with flight information regarding all flights inbound to the destination airport.	SO#06
SR-03	AMAN ATSU shall provide E-AMAN with flight information regarding an arriving flight when the flight reaches the defined Eligibility Horizon.	SO#06
SR-04	Flight data distribution shall ensure that flight information provided to E-AMAN shall be correct and accurate.	SO#06
SR-05	Sequence Manager shall supervise and control E-AMAN.	SO#06
SR-06	E-AMAN shall insert a representation of an inbound flight reaching the Eligibility Horizon in the sequence in accordance with applicable rules and strategies.	SO#07
SR-07	SEQ_MAN shall adjust control parameters of E-AMAN to reflect actual and planned operational conditions.	SO#08
SR-08	SEQ_MAN shall have the authority to select and engage predefined ATC strategies reflecting sets of rules according to which to build the sequence. [SR-08]	SO#08
SR-11	E-AMAN shall update the sequence to account for new and relevant information.	SO#10
SR-12	SEQ_MAN shall introduce changes and adjustments to the sequence as deemed necessary for safe and expedient flow of inbound traffic.	SO#10
SR-13	SEQ_MAN shall use COTR to coordinate with other controllers regarding sequence build as required.	SO#10 SO#12
SR-14	For each inserted flight E-AMAN shall assess whether there exists a need to delay or expedite the flight so as to comply with the required traffic flow parameters.	SO#11
SR-16	SEQ_MAN shall introduce changes and adjustments to the sequence as deemed necessary for safe and expedient flow of inbound traffic.	SO#12

SR-18	EXE/PLN En-Route sector controllers shall implement the sequence and delay/expedition of flights before flights reach coordination point with Approach sectors.	SO#12
SR-20	En-Route controllers shall apply AMAN advisories (TTL/TTG) to flights under their control.	SO#14 SO#24
SR-38	En-Route controllers shall continuously monitor traffic in their sectors and ensure that the AMAN advisories are complied with.	SO#22
SR-39	Following handover of traffic from En-Route sectors, Approach controllers shall continuously monitor traffic in their sectors and ensure that the AMAN advisories are complied with.	SO#23
SR-44	Quality of trajectory prediction used by E-AMAN to build the sequence shall be sufficient to support concept operation.	SO#29
SR-45	E-AMAN shall continuously monitor and diagnose its operation.	SO#30
SR-46	E-AMAN shall continuously monitor the quality of its input data.	SO#30
SR-47	E-AMAN shall alert SEQ_MAN by means of a suitable HMI message if it determines that its operation or quality of its input data are suspect.	SO#30
SR-48	Upstream ATSU ATM system shall receive, process and display arrival management information.	SO#31
SR-49	E-AMAN configuration shall provide functionality to define rules to govern potential overtake situations, as functions of route, aircraft type and its associated performance characteristics, distance-to-go, downlinked aircraft parameters if available, strategic prioritization, other data sources as available.	SO#33
SR-50	CMAN shall continuously monitor and diagnose its operation.	SO#34M
SR-51	CMAN shall continuously monitor the quality of its input data.	SO#34M
SR-52	CMAN shall alert SEQ_MAN by means of a suitable HMI message if it determines that its operation or quality of its input data are suspect.	SO#34M
SR-53	For each inserted flight CMAN shall assess whether there exists a need to delay the flight to prevent bunching.	SO#11
SR-54	E-AMAN shall provide CMAN with correct and accurate arrival management information	SO#06
SR-55	CMAN shall provide E-AMAN with correct and accurate adjusted arrival management information.	SO#06
Requirements determined from thread analysis of Normal Operating Conditions		

SEQ_MAN-N01	Sequence manager shall be able to arbitrarily assign a runway to a flight	generic scenario
SEQ_MAN-N02	Sequence manager shall prompt E-AMAN to recalculate an arbitrary portion of a stabilized sequence.	Generic scenario
E-AMAN-N01	E-AMAN shall make consistent use of best source of information for the following service data: - operational parameters - flight information - trajectory prediction	generic scenario
E-AMAN-N02	E-AMAN shall provide to SEQ_MAN at the minimum the following arrival management information: - value of advisory - sequence number - time ordered sequence - sequence filterable by runway/metering or feeder fix *Note: distance to go is an optional information item as per local implementation.*	Generic scenario
E-AMAN-N03	Configuration of E-AMAN shall be validated and verified prior to operational deployment.	Generic scenario
E-AMAN-N04	E-AMAN shall consider any change introduced in the sequence by SEQ_MAN as permanent unless prompted to recalculate by SEQ_MAN	generic scenario
E-AMAN-N05	E-AMAN shall continuously update estimated landing times for sequenced traffic	generic scenario
E-AMAN-N06	E-AMAN shall not automatically change order in the sequence to traffic having passed SSH.	Generic scenario
E-AMAN-N07	E-AMAN shall not constrain a flight by an advisory when it is determined that there is no need for delay.	Generic scenario
E-AMAN-N08	E-AMAN shall indicate explicitly to SEQ_MAN and ATCO an intentionally unconstrained flight.	generic scenario
E-AMAN-N09	E-AMAN shall determine and assign runway to a flight in accordance with a predefined runway utilization strategy.	Generic scenario
ATCO-N01	Controllers in any involved ATSU (Upstream and Destination) shall coordinate with SEQ_MAN with respect to desired changes in sequence as required.	Generic scenario
CMAN-N01	Configuration of CMAN shall be validated and verified prior to operational deployment.	Generic scenario

Requirements determined from thread analysis of Abnormal Operating Conditions		
SR-A01	SEQ_MAN shall insert a tactical reservation of arbitrary length in the sequence to account for abnormal cases such as low performance aircraft or short term runway closure.	AC#01 AC#03 AC#09
SR-A02	SEQ_MAN shall designate a flight in case of special treatment is necessary.	AC#01 AC#09
SR-A03	E-AMAN shall exclude from sequencing a flight designated by SEQ_MAN for special treatment.	AC#01 AC#09
SR-A04	SEQ_MAN shall manually define and insert a flight in the sequence.	AC#03 AC#05
SR-A05	SEQ_MAN shall manually remove a flight from the sequence.	AC#01 AC#03 AC#05

Table 28: Consolidated list of Safety Requirements (functionality and performance)

B.2 Safety Requirements (Integrity)

SR	Safety Requirement	HP 16.6.5	Related Cause ID
	E-AMAN		
SR-101	The likelihood of E-AMAN being not available or unserviceable shall be no more than 2e-4 SOH, approximately once every 7 months.	N/A	E-AMAN-001 E-AMAN-004
SR-102	The likelihood of E-AMAN operating on an incorrect time reference shall be no more than 2e-4 SOH, approximately once every 7 months.	N/A	E-AMAN-002 E-AMAN-005
SR-103	The likelihood of E-AMAN failing to accept human input shall be no more than 1e-3 SOH, approximately once every 6 weeks.	N/A	E-AMAN-003
SR-104	The likelihood of E-AMAN incorrectly assessing need for delay shall be no more than 2e-4 SOH, approximately once every 7 months.	N/A	E-AMAN-006 E-AMAN-007
	SEQ_MAN		

SR-112	SEQ_MAN shall be trained to supervise E-AMAN.	Low	SEQ_MAN-001
SR-113	SEQ_MAN shall be trained with respect to correct input and operation of AMAN.	Medium	SEQ_MAN-002
	ATCO		
SR-115	Controllers shall be trained with respect to coordination tasks related to sequence implementation. *Mitigation provided by MM-02 –> SR-116.*	Medium	ATCO-001
SR-116	E-AMAN shall be designed to facilitate coordination of sequence build and implementation related information between SEQ_MAN and EXE/PLN controllers active in or contributing to the implementation of the sequence. *This is MM-02 providing mitigation of SR-115*	N/A	ATCO-001
SR-117	Controllers shall be trained with respect to implementation of AMAN advisories.	Low	ATCO-002
SR-127	Controllers shall be trained with respect to continuous monitoring and assessment of compliance with clearances related to implementation of AMAN advisories.	Low	ATCO-012
	FDPS		
SR-128	The likelihood that incorrect flight information is provided by flight data processing system in ATSU Destination shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.	N/A	FDPS-001 FDPS-002
	ATSU		
SR-131	The likelihood that ATSU Destination provides incorrect STAR/RWY information to SEQ_MAN/E-AMAN shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.	N/A	ATSU-001
SR-132	The likelihood that ATSU Destination provides incorrect landing rate information to SEQ_MAN/E-AMAN shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.	N/A	ATSU-002
SR-133	The likelihood that ATSU fails to define a correct ATC strategy shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.	N/A	ATSU-003
SR-134	The likelihood that ATSU fails to implement agreed delay sharing strategy in AMAN configuration shall be no more than 2e-3 SOH, approximately once every three weeks.	N/A	ATSU-004
	COTR		

SR-135	The likelihood that coordination and transfer equipment is inoperative shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.	N/A	COTR-001
	CWP-HMI		
SR-136	The likelihood that CWP HMI fails to present AMAN advisories to the controller shall be no more than 5e-4 SOH, approximately once every 12 weeks.	N/A	CWP-HMI-001
SR-137	The likelihood that CWP HMI presents incorrect AMAN advisories to the controller shall be no more than 5e-4 SOH, approximately once every 12 weeks.	N/A	CWP-HMI-002
	Trajectory Prediction		
SR-151	The likelihood that inaccurate Trajectory Prediction information is provided to E-AMAN shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.	N/A	TP-001 TP-003
SR-152	The likelihood that Trajectory Prediction information is unavailable to E-AMAN shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.	N/A	TP-002
	CMAN		
SR-153	The likelihood of CMAN being not available or unserviceable shall be no more than 2e-4 SOH, approximately once every 7 months.	N/A	CMAN-001 CMAN-003
SR-154	The likelihood of CMAN incorrectly assessing need for delay shall be no more than 2e-4 SOH, approximately once every 7 months.	N/A	CMAN-002 CMAN-004

Table 29 Safety Requirements – Integrity and Reliability

Appendix C Assumptions, Safety Issues & Limitations

C.1 Assumptions log

The following Assumptions were necessarily raised in the course of the Safety Assessment.

Ref	Assumption
A-002	Airspace design is optimized to the greatest extent possible to facilitate concept operation. Common key areas of interest exist in the location of merging points, metering points and coordination points.
A-003	Airspace design excludes danger and restricted areas (D, R and other forms of restrictions such as TSA, Prohibited airspace, “No fly zones” etc) to the extent where they would interfere with the provision of the service. Where exclusion of such areas cannot be accomplished, airspace design shall define mitigation means such as alternate arrival routes circumventing the segregated areas.
A-006	At any point if the controller deems the sequence unworkable, tactical control shall be established.
A-007	When the controller has determined that the sequence has become unworkable, coordination shall take place to inform impacted controllers including the sequence manager as required.
A-009	Appropriate Letters of Agreement or Service Level Agreements shall be in place stipulating the duties of the Upstream ATSU with respect to sequence implementation.
A-010	Flight crew is advised with respect to the expected STAR/RWY before the provision of the service commences. This assumption is grounded in baseline method: *F&P SO#02 ATC shall provide STAR/RWY to the A/C* *F&P SO#03 A/C shall receive STAR/RWY*
A-011	Ground and air trajectories are updated with the expected STAR/RWY. This assumption is grounded in baseline method: *F&P SO#04 ATC shall update Ground Trajectory with the STAR/RWY* *F&P SO#05 A/C shall update Air Trajectory with the STAR/RWY*
A-013	Independent of the delay situation, ensuring separation and reaching Letters of Agreement exit conditions must always be prioritized over the pre-sequencing task.
A-103	VFR flights are considered out of scope of this SAR.
A-104	Derivation of relationship between Flight hour (FH) and Sector Operating Hour (SOH) SOH (ENR) = 6 FH (36 acft/hr w/ 10 min dwell time) SOH (TMA) = 6 FH (45 acft/hr w/ 8 min dwell time)
A-105	Safe design at the physical level will be performed by 10.01.07 as agreed in OFA level coordination.

A-108	Assumptions relating to the calculation of criteria achievability, see 2.10 Typical descent speed in near-peak traffic for baseline AMAN: There is no “typical” speed in contemporary operations according to operational experts. An example typical fuel savvy flight will descend at 240-260 KIAS from cruise. A flight with a tight connection or behind schedule: 280-310 KIAS: Typical speed reduction and increase range in contemporary operations: 250 – 300 KIAS. Typical speed range for cruise portion of Extended AMAN: +/- M0.03, translates to range: M0.75 – M0.81 Central Limit Theorem in distribution of descent speeds and ranges: Does not apply due to CFMU; verify from EXE-485. Distribution of advisories is heavily skewed towards TTL, ca 9:1 and otherwise randomized and dependent on airspace and AMAN configuration.
A-109	SAR scope defined according to EATMA v4.
A-110	A strategic planning mechanism is in place to ensure that traffic demand does not exceed the available capacity of each ATSU.

C.2 Safety Issues log

N/A

C.3 Operational Limitations log

N/A

Appendix D Causal Analysis

This chapter presents the causal analysis on Safety Objectives – integrity, which was used in 7.5.1. The analysis was conducted using the Hybrid FTA method proposed by WP16.

D.1 SO#106

The likelihood of ATC failing to build the arrival sequence shall be no more than 2e-3 / SOH.

Hybrid FTA Safety Severity Class: Minor.

E-AMAN-001	E-AMAN unserviceable. [3.3e-4 SOH]	SSC:Minor	E-AMAN
CMAN-001	CMAN unserviceable [3.3e-4 SOH]	SSC:Minor	CMAN
SEQ_MAN-001	SEQ_MAN fails to supervise E-AMAN. [minor impact] [HIC:L]	SSC:Minor	SEQ_MAN
TP-001	Inaccurate Trajectory Prediction information provided to E-AMAN. [2.5e-4 SOH]	SSC:Minor	TP
TP-002	Trajectory Prediction information unavailable. [2.5e-4 SOH]	SSC:Minor	TP
COTR-001	Coordination and Transfer equipment inoperative. [2.5e-4 SOH]	SSC:Minor	COTR
FDPS-001	Incorrect flight information is provided by flight data processing system in ATSU Destination. [2.5e-4 SOH]	SSC:Minor	FDPS

D.2 SO#107

The likelihood of ATC failing to insert and sequence an emergent flight at Eligibility Horizon shall be no more than 2e-3 / SOH.

Hybrid FTA Safety Severity Class: Minor.

E-AMAN-001	E-AMAN unserviceable. [3.3e-4 SOH]	SSC:Minor	E-AMAN
CMAN-001	CMAN unserviceable [3.3e-4 SOH]	SSC:Minor	CMAN
E-AMAN-002	E-AMAN incorrect time reference. [3.3e-4 SOH]	SSC:Minor	E-AMAN
TP-001	Inaccurate Trajectory Prediction information provided to E-AMAN. [2.5e-4 SOH]	SSC:Minor	TP
TP-002	Trajectory Prediction information unavailable. [2.5e-4 SOH]	SSC:Minor	TP
COTR-001	Coordination and Transfer equipment inoperative. [2.5e-4 SOH]	SSC:Minor	COTR

FDPS-001	Incorrect flight information is provided by flight data processing system in ATSU Destination. [2.5e-4 SOH]	SSC:Minor	FDPS

D.3 SO#108

The likelihood of ATC failing to adjust E-AMAN to relevant operational parameters shall be no more than 2e-3 / SOH.

Hybrid FTA Safety Severity Class: Minor.

E-AMAN-003	E-AMAN fails to accept human input [1e-3 SOH]	SSC:Minor	E-AMAN
SEQ_MAN-002	SEQ_MAN makes an incorrect input [minor impact] [HIC:M].	SSC:Minor	SEQ_MAN
ATCO-001	ATCO fails a coordination task. [minor impact] [HIC:M].	SSC:Minor	ATCO
ATSU-001	ATSU Destination provides incorrect STAR/RWY information to SEQ_MAN/E-AMAN. [2.5e-4 SOH]	SSC:Minor	ATSU DEST
ATSU-002	ATSU Destination provides incorrect landing rate information to SEQ_MAN/E-AMAN. [2.5e-4 SOH]	SSC:Minor	ATSU DEST
ATSU-003	ATSU fails to define a correct ATC strategy. [2.5e-4 SOH]	SSC:Minor	ATSU (any)

D.4 SO#110

The likelihood that the ATC fails to update the sequence to account for new relevant or important information shall be no more than 2e-3 / SOH.

Hybrid FTA Safety Severity Class: Minor.

E-AMAN-001	E-AMAN unserviceable. [3.3e-4 SOH]	SSC:Minor	E-AMAN
CMAN-001	CMAN unserviceable [3.3e-4 SOH]	SSC:Minor	CMAN
E-AMAN-002	E-AMAN incorrect time reference. [3.3e-4 SOH]	SSC:Minor	E-AMAN
SEQ_MAN-002	SEQ_MAN makes an incorrect input. [minor impact] [HIC:M].	SSC:Minor	SEQ_MAN
ATCO-001	ATCO fails coordination task [minor impact] [HIC:M].	SSC:Minor	ATCO
COTR-001	Coordination and Transfer equipment inoperative. [2.5e-4 SOH]	SSC:Minor	COTR
FDPS-001	Incorrect flight information is provided by flight data processing system in ATSU Destination. [2.5e-4 SOH]	SSC:Minor	FDPS

D.5 SO#111

The likelihood that ATC fails to assess need for delay to a newly sequenced flight shall be no more than 2e-3 / SOH.

Hybrid FTA Safety Severity Class: Minor.

E-AMAN-004	E-AMAN unserviceable. [2e-4 SOH]	SSC:Minor	E-AMAN
CMAN-003	CMAN unserviceable [2e-4 SOH]	SSC:Minor	CMAN
E-AMAN-005	E-AMAN incorrect time reference. [2e-4 SOH]	SSC:Minor	E-AMAN
E-AMAN-006	E-AMAN incorrect assessment of need for delay [2e-4 SOH]	SSC:Minor	E-AMAN
CMAN-002	CMAN incorrect assessment of need for delay [2e-4 SOH]	SSC:Minor	CMAN
TP-003	Inaccurate Trajectory Prediction information provided to E-AMAN. [5e-4 SOH]	SSC:Minor	TP
FDPS-002	Incorrect flight information is provided by flight data processing system in ATSU Destination. [5e-4 SOH]	SSC:Minor	FDPS

D.6 SO#112

The likelihood that ATSU En Route fails to deliver the implemented sequence to ATSU Approach shall be no more than 2e-3 / SOH.

Hybrid FTA Safety Severity Class: Minor.

SEQ_MAN-001	SEQ_MAN fails to supervise E-AMAN. [minor impact] [HIC:L].	SSC:Minor	SEQ_MAN
SEQ_MAN-002	SEQ_MAN makes an incorrect input. [minor impact] [HIC:M].	SSC:Minor	SEQ_MAN
ATCO-001	ATCO fails coordination task [minor impact]. [HIC:L].	SSC:Minor	ATCO

D.7 SO#114

The likelihood that ATSU En Route fails to apply AMAN advisories shall be no more than 2e-3 / SOH.

Hybrid FTA Safety Severity Class: Minor.

ATCO-002	ATCO fail to implement AMAN advisories. [minor impact] [HIC:L].	SSC:Minor	ATCO
SEQ_MAN-001	SEQ_MAN fails to supervise E-AMAN. [minor impact] [HIC:L].	SSC:Minor	SEQ_MAN
E-AMAN-002	E-AMAN incorrect time reference. [3.3e-4 SOH]	SSC:Minor	E-AMAN
E-AMAN-007	E-AMAN incorrect assessment of need for delay [3.3e-4	SSC:Minor	E-AMAN

	SOH]		
CMAN-002	CMAN incorrect assessment of need for delay [3.3e-4 SOH]	SSC:Minor	CMAN
CWP-HMI-001	CWP HMI fails to present AMAN advisories to the controller. [5e-4 SOH]	SSC:Minor	CWP-HMI
CWP-HMI-002	CWP HMI presents incorrect AMAN advisories to the controller. [5e-4 SOH]	SSC:Minor	CWP-HMI

D.8 SO#122

The likelihood that ATSU En Route fails to monitor traffic and ensure that AMAN times are being met shall be no more than 2e-3 / SOH.

Hybrid FTA Safety Severity Class: Minor.

ATCO-012	ATCO fails to monitor compliance with clearances related to implementation of advisories [minor impact] [HIC:L].	SSC:Minor	ATCO

D.9 SO#123

The likelihood that ATSU Approach fails to manage traffic in arrival sequence shall be no more than 2e-3 / SOH.

Hybrid FTA Safety Severity Class: Minor.

ATCO-012	ATCO fails to monitor compliance with clearances related to implementation of advisories [minor impact] [HIC:L].	SSC:Minor	ATCO
ATSU-004	ATSU fails to implement agreed delay sharing strategy in AMAN configuration [2e-3 SOH]	SSC:Minor	ATSU (any)

D.10 SO#124

The likelihood that ATSU approach fails to apply AMAN advisories to traffic as delivered by ATSU En Route shall be no more than 2e-3 / SOH.

Hybrid FTA Safety Severity Class: Minor.

ATCO-002	ATCO fail to implement AMAN advisories. [minor impact] [HIC:L].	SSC:Minor	ATCO
SEQ_MAN-001	SEQ_MAN fails to supervise E-AMAN. [minor impact] [HIC:L].	SSC:Minor	SEQ_MAN
E-AMAN-002	E-AMAN incorrect time reference. [3.3e-4 SOH]	SSC:Minor	E-AMAN
E-AMAN-007	E-AMAN incorrect assessment of need for delay [3.3e-4 SOH]	SSC:Minor	E-AMAN

CMAN-002	CMAN incorrect assessment of need for delay [3.3e-4 SOH]	SSC:Minor	CMAN
CWP-HMI-001	CWP HMI fails to present AMAN advisories to the controller. [5e-4 SOH]	SSC:Minor	CWP-HMI
CWP-HMI-002	CWP HMI presents incorrect AMAN advisories to the controller. [5e-4 SOH]	SSC:Minor	CWP-HMI

D.11 SO#126

The likelihood that airspace design is insufficient to support the concept shall be no more than 2e-4 / SOH.

Hybrid FTA Safety Severity Class: Minor.

A-002	Airspace design is optimized to the greatest extent possible to facilitate concept operation. Common key areas of interest exist in the location of merging points, metering points and coordination points.	Assumption
A-003	Airspace design excludes danger and restricted areas (D, R and other forms of restrictions such as TSA, Prohibited airspace, “No fly zones” etc) to the extent where they would interfere with the provision of the service	Assumption

A.1.2 Security risk assessment

A Security Risk Assessment has been performed under the lead of 16.06.02 on OFA level embedded hereafter:

Security Risk Assessment of OFA 04.01.02 Enhanced Arrival & Departure Management in TMA and En Route

Document information	
Project Title	Security Risk Assessment of OFA 04.01.02 Enhanced Arrival & Departure Management in TMA and En Route
Project Number	16.06.02
Project Manager	EUROCONTROL
Deliverable Name	Security Risk Assessment of OFA 04.01.02 Enhanced Arrival & Departure Management in TMA and En Route
Deliverable ID	
Edition	00.00.05
Template Version	03.00.00
Task contributors	
EUROCONTROL	

Abstract

This document contains a security risk assessment of OFA 04.01.02 Enhanced Arrival & Departure Management in TMA and En Route.

Authoring & Approval

Prepared By - *Authors of the document.*		
Name & Company	Position & Title	Date
[redacted] EUROCONTROL (Winsland)	[redacted]	<03/08/2015>
[redacted] EUROCONTROL (Winsland)	[redacted]	<03/08/2015>
[redacted] EUROCONTROL (Winsland)	[redacted]	<03/08/2015>

Reviewed By - *Reviewers internal to the project.*		
Name & Company	Position & Title	Date
[redacted] EUROCONTROL	[redacted]	31/08/2015
[redacted] EUROCONTROL	[redacted]	31/08/2015

Reviewed By - *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date
<Name / Company>	<Position / Title>	<DD/MM/YYYY>

Approved for submission to the SJU By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
<Name / Company>	<Position / Title>	<DD/MM/YYYY>

Rejected By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
<Name / Company>	<Position / Title>	<DD/MM/YYYY>

Rational for rejection
None.

Document History

Edition	Date	Status	Author	Justification
00.00.01	03/08/2015		[redacted]	New Document
00.00.02	31/08/2015		[redacted]	Addressing OFA 4.1.2 review comments
00.00.03	24/09/2015		[redacted]	Addressing P. Conroy comments arising from previous version changes.
00.00.04	25/09/2015		[redacted]	Proof read edits.
00.00.05	18/04/2016		[redacted]	Update to include CMAN in respect of multiple airport coordination.

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

List of tables

List of figures

No table of figures entries found.

1 Introduction

This document describes a risk assessment of 04.01.02 ‘Enhanced Arrival & Departure Management in TMA and En Route’. The work is provided as an annex as it is intended to form an annex of the OFA SPR documentation.

Appendix A Security Risk Assessment

A.1 Introduction

A.1.1 Purpose of the annex

This annex describes a risk assessment of 04.01.02 ‘Enhanced Arrival & Departure Management in TMA and En Route’. The work updates previous (2013) security risk assessment on AMAN and i4D+CTA in order to support the latest versions of the concept and in particular SESAR Solutions 05 (Extended-AMAN Horizon) and 06 (CTA in medium density / complexity environment).

The risk assessment has been carried out by WP16.06.02, specifically the following people: Martin Hawley / EUROCONTROL (Winsland); Karol Gőtz / EUROCONTROL (Winsland); and Paul Thomas / EUROCONTROL (Winsland).

The risk assessment is necessarily high level and has worked from a variety of OFA documentation. This also means that it is not specific to SESAR Solutions 05, 06 and 08. As these solutions are developed further and detailed system descriptions are available it is recommended that the risk assessment is iterated.

A.1.2 Intended readership

The annex is intended to support on-going security analysis and design of the OFA/SESAR Solutions as the SESAR Solutions are developed towards operational deployment. The intended readership is therefore all of those involved in this development, particularly in developing security requirements and solutions for operational deployment.

A.1.3 Inputs from other projects

A significant input to this work is the Security Risk Assessment of OFA 04.01.05 i4D+CTA Security Risk Assessment (2013) and the Extended AMAN Security Case (2013), both carried out by 16.06.02. A number of documents have been reviewed in the course of this risk assessment and are listed in section A.9. In particular we have drawn upon:

- 04.03-D012-i4D and CTA OSED Requirement - Part 1, 5/11/2014. Particular reference has been made to the following sections: 2.2 ‘Operational Concept Description’; 2.2.2 ‘Traffic synchronisation between ATSUs’; and 3.1.2 ‘Aircraft equipage and Ground capabilities’. The latter section comments that whilst the “IOP service does not require special aircrafts equipment beyond today operations….the ground systems have to be equipped with Flight Object Server (FOS) to exchange Flight Objects (FO).”

- 04.03-D07-IOP OSED and Requirements - Part 1 OSED, 5/11/2014. Particular reference has been made to the following sections: 2.2 ‘Operational Concept Description’ (noting reference to the OLDI Arrival Management (AMA) message ‘Time at COP’ - inter-centre Co-ordination Point; 4.2.2 ‘i4D Concept Description’, which provides a good description of the steps involved in trajectory negotiation; 2.3 ‘Processes and Services’, which describes the set of services to synchronise airborne and ground held trajectory data (send and receive), send data to other parties, calculate a time window for a fix, negotiate and agree a CTA, manage aircrew accept/reject, monitor compliance, terminate CTA management etc.

- 05.06.01-D67, Step 1 OSED - second iteration, 27/11/2012. Particular reference has been made to the Required Airborne and Ground Capabilities for i4D. We note that “Project 5.6.1 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, it is not a pre-requisite for CTA operations”.

- 05.06.01 D74 Step 1 OSED - Iteration 3, 01.00.00, 11/09/2013, particularly concerning required I4D equipage for non-equipped, basic CTA and i4D aircraft. We note the following point about the airborne architecture: "it is considered to be of benefit to have an integrated Communication and Flight Management Systems (link between comm. and navigation to support the automatic upload of agreed 3D trajectories and time/speed constraints). This document also addresses Required Ground Capabilities for CTA Operations and refers to technical constraints that might impact the concept or the solution that are identified within P9.1, referencing:
    - SESAR P9.1 Overall Technical Verification & Validation Report – Mainline Aircraft – Step 1 (VALR), D05, 01.00.00, 06-12-2012.
    - SESAR P9.1, Aircraft & System Performance and Functional Requirements – Step 1, Edition 1.3, 13-04-2010.
- 04.03.00 D07-IOP OSED and Requirements - Part 3, 21/06/2011.
- 05.06.04 D34-002 INTEROP5.6.4 Interoperability Requirements (INTEROP) for TS-0305-A, 00.00.01, 31/03/2015, which provides an overview of the information exchanges. Points of note are: the interactions with the Network Manager are out of scope of the Step 1 OSED; departure information may be provided from a variety of source systems, such as DMAN or an integration of AMAN and DMAN, both outside the scope of this SPR-INTEROP. Also referred to is the arrival management functional block model in section 3.1.4 and taken from 10.01.07 Functional Decomposition.

A.1.4 Glossary

Term	Definition
Asset	Elements in the system that have value for the achievement of business objectives
Availability	The property of being accessible and usable upon demand by an authorized entity
Compromised	The loss, corruption or reduction in the performance of a primary or supporting asset (e.g. loss of confidentially, reduced availably, increased latency, corruption of data)
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature
Impact	The extent to which compromising confidentiality, availability or integrity of an asset affects the achievement of business objectives
Impact Scenario	A sequence of operational steps describing the impact done over a primary asset (see fig 2)
Integrity	The property of safeguarding the accuracy and completeness of assets
Likelihood	Evaluation of the chance of a threat scenario successfully occurring
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

Term	Definition
Risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby have an impact on the identified assets.
Risk assessment	The overall process of risk identification and risk evaluation
Risk evaluation	The process of assigning values to the likelihood and impacts of a risk
Risk identification	The process of finding, listing and characterizing elements of risk
Risk treatment	The process of selecting and implementing measures to modify risk
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.
Threat	The potential cause of an unwanted incident which may result in an impact on the OFA
Threat Scenario	A threat scenario is a combination of a threat over a supporting asset within the considered environment (see fig 2)
Vulnerability	A security weakness of an asset that can be exploited by an attacker via a threat

A.1.5 Acronyms

Term	Definition
AMAN	Arrival Manager (Equipment)
ATIS	Automatic Terminal Information Service
ATM	Air Traffic Management
CIA	Confidentiality, Integrity, Availability
CMAN	Centre Manager
CTA	Controlled Time of Arrival
CWP	Controller Working Position
E-AMAN	Extended AMAN
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
ICAO	International Civil Aviation Organization
MSSC	Minimum Set of Security Controls
NA	Not Applicable

Term	Definition
OFA	Operational Focus Area
OLDI	On-Line data Interchange
OSED	Operational Services and Environmental Description
PA	Primary Asset
RTF	Radio Telephony
SecRAM	Security Risk Assessment Methodology
SESAR	Single European Sky ATM Research
SESAR Programme	The programme which defines the Research and Development activities and Projects for the SJU.
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SJU Work Programme	The programme which addresses all activities of the SESAR Joint Undertaking Agency.
SO	Security Objective(s)
SPR	Safety and Performance Requirements
SRA	Security Risk Assessment
TTA	Target Time of Arrival
TTG	Time to Gain
TTL	Time to Lose
TTO	Target Time Over
Tx/Rx	Transmit/Receive
WP	Work Package

A.2 Scope

A.2.1 OFA details

OFA 04.01.02 contributes to three SESAR Solutions:

- SESAR Solution #05 E-AMAN horizon
- SESAR Solution #06 CTA in medium density / complexity environment
- SESAR Solution #08 AMAN into Multiple Airports

The OFA supports arrivals management into a TMA through arrivals sequencing support, facilitating the use of fixed routes (e.g. PRNAV), CDAs and agreeing a Controlled Time of Arrival (at a defined point) with a particular flight. The arrival managers are intended to help to smooth throughput through an earlier metering of the inbound traffic. By extending the arrivals management to surrounding sectors, holding can be reduced by absorbing some of the queuing time in sectors adjacent to the TMA.

The CTA is issued by the AMAN at destination, but the communication of the CTA to the aircraft (using either voice or CPDLC) usually takes place upstream, which might involve it taking place in an ATSU different from the one issuing it. This requires coordination mechanisms and messaging related to CTA to be in place between the two ATSUs.

Where several proximate arrival traffic streams are being handled these streams may require additional coordination between individual AMANs. To avoid bunching and potential bottlenecks in a multi-airport TMA, and thereby keep up the arrivals rate, an additional arrival planning component ‘Centre Manager’ (CMAN) is defined to ensure that the preferred time over is optimised according to the wider-TMA operations within from a Centre Management point of view.

The OFA provides a number of operational advantages for terminal operations, including complexity management and queue management.

A.2.2 Security objective

The general security objective is for the risk to CIA criteria on Primary Assets to be the lowest possible (of low or medium) in accordance with the risk matrix of the SESAR Security Risk Assessment Methodology.

	Reviewed Impact				
Likelihood	1	2	3	4	5
5	Low	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

The risk matrix shown here is used to determine risk combining impact assessment of supporting assets with the likelihood of an attack. The impact on supporting assets is derived from the primary assets that they support. The risk matrix is constructed so that risks defined from high impact (4-5) and low likelihood (1-2) can only be reduced to Medium risks. The objective on individual primary assets is therefore to reach either Low or Medium for impacts of level 1-3 and 4-5 respectively.

A.2.3 Scope

The scope of this risk assessment is based on an Extended AMAN operation covering:

- Two ATC areas of responsibility (AoR), with an upstream ATSU and a downstream ATSU. The upstream ATSU serves the destination TMA for the flight.
- AMAN sequencing support of multiple flights into the downstream ATSU TMA.
- Consideration of the upstream ATSU coordinating a CTA with a particular flight.

- The flight may be an aircraft with either Basic CTA or i4D[12], with non-CTA flights included with respect to sequencing but not CTA coordination. A key difference is the accuracy of i4D equipped aircraft and the use of ADS-C for airborne system - ground system RTA interval communication:
    - o “Basic CTA aircraft: 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).
    - o 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).”
- Impact considerations on the OFA/SESAR Solutions only. E.g. use of Extended Projected Profile (EPP) for tools other than AMAN is not covered.

A.2.4 Assumptions

Many of the main components that support Extended AMAN are already in operation and will be covered by existing security controls. As these differ between locations it has been assumed that the MSSCs (Minimum Set of Security Controls) will be implemented.

A.2.5 Limitations

This risk assessment is at a high level, commensurate with the level of detail available at this stage of Extended AMAN development.

[12] From P5.6. 1 ‘Ground & Airborne Capabilities to Implement Sequence’, D74 Step 1 OSED - Iteration 3, 01.00.00, 11/09/2013.

A.3 Impact Assessment

A.3.1 Primary Asset Identification

The first stage of impact assessment is to identify primary assets. The following list has been developed in consultation with OFA4.1.2.

	AMAN Extended Horizon Primary Assets (*indicates new PA)		
	Description	**Type (information/ service)**	**Rationale for considering PA**
1	Trajectory exchange and synchronization (air-ground)	Service	Key component of service[13].
2	EPP (ADS-C Extended Projected profile)	Information	Format for downlink of FMS held data on trajectory.
3	RTF Aeronautical mobile service	Service	Air-ground communication service that will also support trajectory exchange.
4	CPDLC Aeronautical mobile service	Service	Enables exchange of messages between pilot and controller
5	Arrival Management Information Service	Service	Ground-ground exchange of sequence and supporting information. Also implies cross border exchange.
6	Aeronautical fixed service	Service	Ground-ground communication service to support liaison between ATSUs and air mobile service.
7	Flight Plan Data	Information	Used to build sequence information and determine reference points in calculating TTL/G in combination with surveillance data.
8	Surveillance position	Information	Used in conjunction with flight plan data to determine reference points / trajectory prediction.
9	AMAN processing function	Service	Receives, processes and outputs data to enable the arrival management. E.g. sequence generator, CTA.

[13] It has been commented that these may alternatively split into two primary assets and this should be taken into consideration in a future iteration of the risk assessment. Trajectory exchange may provide data to several other functions/activities, only one of which may be to a synchronisation check on the air/ground trajectories. For example, the full EPP received via the trajectory exchange mechanism might be going to the synchronisation check area, whereas an individual element of that data, the aircraft mass, might be going separately to the tool trajectory prediction area.

	AMAN Extended Horizon Primary Assets (*indicates new PA)		
	Description	Type (information/ service)	Rationale for considering PA
10	Trajectory prediction	Service	May be within AMAN or derived from other ground system such as ETFMS if no better alternative. Used to calculate the arrival sequence using trajectory data (Reliable ETA Min/Max) provided by the aircraft itself (i4D equipped) or by using modelled and/or historic aircraft performance data within its sequencing algorithms (non-i4D equipped).
11	Flight Object	Information	Standardised model for sharing up-to-date flight information.
12	Monitor and provide alerts	Service	Reassures ATCOs that the operation is according to plan.
13	P-RNAV capability	Service	Aircraft capability requirement.
14	Meteorological information	Information	Used generally in trajectory prediction but within i4D aircraft, used to increase the accuracy of trajectory prediction to achieve CTA +/- 10s.
15	CMAN Processing Function	Service	Processes information from n+1 AMAN processors and outputs preferred time over information to AMANs in order to optimise arrivals from a centre management perspective.

A.3.2 Impact assessment

The impact assessment considers the impact on the OFA's operations according to the compromising (e.g. total or partial loss) of Confidentiality, Integrity or Availability (CIA) if no controls are in place to protect the asset. Because the OFA requires the majority of the listed primary assets to function at all, the results following show very similar impacts for the loss of CIA on each primary asset. The impact is classified against the following table

	5	4	3	2	1
IMPACT AREAS	Catastrophic	Critical	Severe	Minor	No impact / NA
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

The tables following shows the results of this assessment and the rationale.

Primary Asset PA#1						
Name:	Trajectory exchange and synchronization (air-ground)					
Type:	Service					
Description:	Trajectory exchange and synchronization (air-ground)					
Compromise of Confidentiality						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	1	1	1	3	2	1
Overall impact: 3						
Rationale:	Loss of confidentiality should have no operational impact but may raise concerns of regulators and impact branding. NB it has been commented that precise trajectory information may assist in direct physical attacks on aircraft. This issue will be taken forward into 16.6.2 work on RPAS.					
Compromise of Integrity						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	This may lead to false assumptions about the trajectory and incorrect operational decision making. This may impact capacity as controllers resolve issues with pilots, taking up workload and will reduce predictability (small capacity impact; 2 implies <10%). The effect on branding ('4' implies 'National Attention') may be large even if the operational impact is small. Regulatory issues may arise around security and safety management systems. When a problem is detected, this will lead to a loss of availability as operators will stop using the system until the problem is resolved.					
Compromise of Availability						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Loss of availability will lead to loss of benefit of the OFA/SESAR Solutions supported. These relate to complexity management (workload) and queuing (workload and flight efficiency). These are: some loss of capacity through increased controller workload (2 implies <10%); reduced flight efficiency (as AMAN provides for more efficient profiles / better opportunity for aircrew to manage profiles); reduced predictability; corresponding reduction in environmental benefits as flight efficiency reduces.					

Primary Asset PA#2						
Name:	EPP (ADS-C Extended Projected profile)					
Type:	Information					
Description:	FMS held data on trajectory in a specific format.					
Compromise of Confidentiality						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	1	1	1	3	2	1
Overall impact: 3						
Rationale:	Impact similar to loss of trajectory exchange but note that EPP also supports other controller tools so a loss of CIA of EPP may have more impact than the loss of trajectory exchange at the system level.					
Compromise of Integrity						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Rationale as for Confidentiality.					
Compromise of Availability						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Rationale as for Confidentiality.					

Primary Asset PA#3	
Name:	RTF Aeronautical mobile service
Type:	Service
Description:	Air-ground voice communication service that will also support trajectory exchange.

Compromise of Confidentiality

Personnel	Capacity	Performance	Economic	Branding	Regulation	Environment
1	1	1	1	2	2	1

Overall impact: 2

Rationale:	Aeronautical comms are required for communication between pilot and controller. RTF is currently an open channel and loss of confidentiality is therefore seen to have no impact for RTF.

Compromise of Integrity

Personnel	Capacity	Performance	Economic	Branding	Regulation	Environment
1	2	2	1	4	2	1

Overall impact: 4

Rationale:	Loss of integrity of data AMS could imply discrete modification of data as for Trajectory Sync and EPP.

Compromise of Availability

Personnel	Capacity	Performance	Economic	Branding	Regulation	Environment
1	2	2	1	4	2	2

Overall impact: 4

Rationale:	Loss of availability could lead to a reversion to RTF but allow the operation to continue.

Primary Asset PA#4

Name:	CPDLC Aeronautical mobile service
Type:	Service
Description:	Controller Pilot Datalink Communication

Compromise of Confidentiality

Personnel	Capacity	Performance	Economic	Branding	Regulation	Environment
1	1	1	1	2	2	1

Overall impact: 2

Rationale: Loss of confidentiality of CPDLC could cause regulatory or branding problems but should not impact operations. Loss of confidentiality is therefore seen to have a minor impact for data. Note that without assured confidentiality attackers can learn how to spoof systems, leading to an integrity concern.

Compromise of Integrity

Personnel	Capacity	Performance	Economic	Branding	Regulation	Environment
1	2	2	1	4	2	2

Overall impact: 4

Rationale: Loss of integrity of data could imply discrete modification of data as for Trajectory Sync and EPP. E.g. loss of integrity of CPDLC could lead to an incorrectly agreed CTA, which may not be noticed until the CTA agreement is breached.

Compromise of Availability

Personnel	Capacity	Performance	Economic	Branding	Regulation	Environment
1	2	2	1	4	2	2

Overall impact: 4

Rationale: Loss of availability of data AMS would require reversion to non-AMAN operating procedures.

Primary Asset PA#5						
Name:	Arrival Management Information Service					
Type:	Service					
Description:	Ground-ground exchange of sequence and supporting information. Also implies cross border exchange.					
Compromise of Confidentiality						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	1	1	1	2	2	1
Overall impact: 2						
Rationale:	Loss of confidentiality of service could cause regulatory or branding problems but should not impact operations.					
Compromise of Integrity						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Loss of integrity could mean downstream ATSU coordinates an incorrect CTA with aircraft in its AoR, e.g. based on incorrect TTO, TTL, TTG. Alternatively an incorrect sequence could be built, increasing controller workload to correct it once recognised.					
Compromise of Availability						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Loss of availability requires a reversion to non-E AMAN operations.					

Primary Asset PA#6						
Name:	Aeronautical fixed service (voice)					
Type:	Service					
Description:	Ground-ground communication service to support voice communication between ATSUs.					
Compromise of Confidentiality						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	1	1	1	2	2	1
Overall impact: 2						
Rationale:	Loss of confidentiality of service could cause regulatory or branding problems but should not impact operations.					
Compromise of Integrity						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Loss of integrity could mean downstream ATSU coordinates an incorrect CTA with aircraft.					
Compromise of Availability						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						

Primary Asset PA#7						
Name:	Flight Plan Data					
Type:	Information					
Description:	Used to build sequence information determine reference points in calculating TTL/G in combination with surveillance data.					
Compromise of Confidentiality						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	1	1	1	2	2	1
Overall impact: 2						
Rationale:	Loss of confidentiality of service could cause regulatory or branding problems but should not impact operations.					
Compromise of Integrity						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Loss of integrity of the flight plan will cause difficulties in resolving the discrepancy via EPP and may be readily identified, causing reversion to non-E AMAN operations. This would have system wide implications that are not addressed in this assessment.					
Compromise of Availability						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Loss of availability of the flight plan will cause reversion to non-E AMAN operations. This would have system wide implications that are not addressed in this assessment.					

Primary Asset PA#8						
Name:	Surveillance position					
Type:	Information					
Description:	Used in conjunction with flight plan data to determine reference points / trajectory prediction.					
Compromise of Confidentiality						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	1	1	1	1	1	1
Overall impact: 1						
Rationale:	Loss of confidentiality of service should not impact operations. Impact would be less than other E-AMAN information as similar positon data is available via ADS-B.					
Compromise of Integrity						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Loss of integrity of position will cause difficulties in determining CTA intervals and resolving the discrepancy may lead to reversion to non-E AMAN operations. This would have system wide implications that are not addressed in this assessment.					
Compromise of Availability						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Loss of availability of position will cause reversion to non-E AMAN operations. This would have system wide implications that are not addressed in this assessment.					

Primary Asset PA#9						
Name:	AMAN processing function					
Type:	Service					
Description:	Receives, processes and outputs data to enable the arrival management. E.g. sequence generator, CTA.					
Compromise of Confidentiality						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	1	1	1	2	2	1
Overall impact: 2						
Rationale:	Loss of confidentiality should not impact operations but would cause concerns about other impacts.					
Compromise of Integrity						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Loss of integrity of the processing function could result in sequences, including CTAs, being unreliable. These conditions may not be immediately obvious to controllers and may result in aircraft sequences not being 'built' correctly, or CTAs being erroneous given/complied with. However, the loss would soon become obvious. The consequence could be increased workload in resolving problems leading to reversion to non-E-AMAN operations.					
Compromise of Availability						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Loss of availability leads to reversion to non-E-AMAN operations.					

<table>
<tr><th colspan="7">Primary Asset PA#10</th></tr>
<tr><td><b>Name:</b></td><td colspan="6">Trajectory prediction</td></tr>
<tr><td><b>Type:</b></td><td colspan="6">Service</td></tr>
<tr><td><b>Description:</b></td><td colspan="6">May be within AMAN or derived from other ground system such as ETFMS if no better alternative. Used to calculate the arrival sequence using trajectory data (Reliable ETA Min/Max) provided by the aircraft itself (i4D equipped) or by using modelled and/or historic aircraft performance data within its sequencing algorithms (non-i4D equipped).</td></tr>
<tr><td colspan="7"><b>Compromise of Confidentiality</b></td></tr>
<tr><td><b>Personnel</b></td><td><b>Capacity</b></td><td><b>Performance</b></td><td><b>Economic</b></td><td><b>Branding</b></td><td><b>Regulation</b></td><td><b>Environment</b></td></tr>
<tr><td>1</td><td>1</td><td>1</td><td>1</td><td>2</td><td>2</td><td>1</td></tr>
<tr><td colspan="7"><b>Overall impact:</b> 2</td></tr>
<tr><td><b>Rationale:</b></td><td colspan="6">Loss of confidentiality should not impact operations but would cause concerns about other impacts.</td></tr>
<tr><td colspan="7"><b>Compromise of Integrity</b></td></tr>
<tr><td><b>Personnel</b></td><td><b>Capacity</b></td><td><b>Performance</b></td><td><b>Economic</b></td><td><b>Branding</b></td><td><b>Regulation</b></td><td><b>Environment</b></td></tr>
<tr><td>1</td><td>2</td><td>2</td><td>1</td><td>4</td><td>2</td><td>2</td></tr>
<tr><td colspan="7"><b>Overall impact:</b> 4</td></tr>
<tr><td><b>Rationale:</b></td><td colspan="6">Loss of integrity could result in sequences being unreliable and in incorrect prediction of CTA windows, and when detected this may lead to temporary increased workload, then reversion to non-E-AMAN operations. There may be wider system impacts outside of this OFA/SESAR Solution.</td></tr>
<tr><td colspan="7"><b>Compromise of Availability</b></td></tr>
<tr><td><b>Personnel</b></td><td><b>Capacity</b></td><td><b>Performance</b></td><td><b>Economic</b></td><td><b>Branding</b></td><td><b>Regulation</b></td><td><b>Environment</b></td></tr>
<tr><td>1</td><td>2</td><td>2</td><td>1</td><td>4</td><td>2</td><td>2</td></tr>
<tr><td colspan="7"><b>Overall impact:</b> 4</td></tr>
<tr><td><b>Rationale:</b></td><td colspan="6">Loss of availability leads to reversion to non-E-AMAN operations. There may be wider system impacts outside of this OFA/SESAR Solution.</td></tr>
</table>

Primary Asset PA#11						
Name:	Flight Object					
Type:	Information					
Description:	Standardised model for sharing up-to-date flight information. This may not be needed for Step 1 where it could be considered as the equivalent of the EPP Primary Asset.					
Compromise of Confidentiality						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	1	1	1	2	2	1
Overall impact: 2						
Rationale:	As for EPP.					
Compromise of Integrity						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	As for EPP, with wider system concerns outside of E-AMAN.					
Compromise of Availability						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	0
Overall impact: 4						
Rationale:	As for EPP, with wider system concerns outside of E-AMAN.					

Primary Asset PA#12						
Name:	Monitor and provide alerts					
Type:	Service					
Description:	Reassures ATCOs that the operation is according to plan.					
Compromise of Confidentiality						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	1	1	1	2	2	1
Overall impact: 2						
Rationale:	Loss of confidentiality should not impact operations but would cause concerns about other impacts.					
Compromise of Integrity						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Loss of integrity could result in incorrect alerts and temporary increased workload then reversion to non-E-AMAN operations.					
Compromise of Availability						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Loss of availability could result in a state of no alerts with lack of awareness. This may lead to increased workload in resolving issues late-on then reversion to non-E-AMAN operations.					

Primary Asset PA#13						
Name:	P-RNAV capability					
Type:	Service					
Description:	Aircraft capability requirement.					
Compromise of Confidentiality						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	1	1	1	1	1	1
Overall impact: 1						
Rationale:	NA					
Compromise of Integrity						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	4	2
Overall impact: 4						
Rationale:	Loss of integrity of P-RNAV could potentially lead to CTA not being met but could have wider impacts than E-AMAN.					
Compromise of Availability						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	1	1	1	4	4	1
Overall impact: 4						
Rationale:	Loss of availability of PRNAV could may make meeting a CTA with accuracy not possible, but could have wider impacts than E-AMAN.					

Primary Asset PA#14						
Name:	Meteorological information					
Type:	Information					
Description:	Within i4D aircraft, used to increase the accuracy of trajectory prediction to achieve CTA +/- 10s.					
Compromise of Confidentiality						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	1	1	1	1	1	1
Overall impact: 1						
Rationale:	NA, MET data generally non-confidential					
Compromise of Integrity						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Loss of integrity could result in incorrect prediction of CTA windows / sequencing and lead to temporary increased workload, then reversion to non-E-AMAN operations (depending on how Trajectory Prediction is provided). There may be wider system impacts outside of this OFA/SESAR Solution.					
Compromise of Availability						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	2	2	1	4	2	2
Overall impact: 4						
Rationale:	Loss of availability could lead to reversion to non-E-AMAN operations (depending on how Trajectory Prediction is provided). There may be wider system impacts outside of this OFA/SESAR Solution.					

Primary Asset PA#15						
Name:	CMAN processing function					
Type:	Service					
Description:	Processes information from n+1 AMAN processors and outputs preferred time over information to AMANs in order to optimise arrivals from a centre management perspective.					
Compromise of Confidentiality						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	1	1	1	2	2	1
Overall impact: 2						
Rationale:	Loss of confidentiality should not impact operations but would cause concerns about other impacts.					
Compromise of Integrity						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	3	3	1	4	2	2

Overall impact: 4						
Rationale:	Similar to AMAN, loss of integrity of the processing function could result in sequences, including CTAs. For CMAN this would have impacts over multiple airports. Also as for AMAN these conditions may not be immediately obvious to controllers and may result in aircraft sequences not being 'built' correctly, or CTAs being erroneous given/complied with. Such conditions would become apparent as there could be bottlenecks developing, with a consequential increase in workload to resolve problems leading to reversion to non-E-AMAN operations for multiple airports.					
Compromise of Availability						
Personnel	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulation**	**Environment**
1	3	3	1	4	2	2
Overall impact: 4						
Rationale:	Loss of availability leads to reversion to non-E-AMAN operations for multiple airports.					

A.3.3 Overall impacts and security objectives

The risk assessment methodology takes the overall impact of loss of CIA to that of the maximum impact across each impact area. The following table summarises these overall impacts against the security objective for each primary asset:

Table 30: Security objectives on primary assets

Primary Asset	Overall Impact	Security objective for risk
Trajectory exchange and synchronization (air-ground)	4	Medium
EPP (Extended Projected profile)	4	Medium
Aeronautical mobile service	4	Medium
CPDLC	4	Medium
Arrival Management Service	4	Medium
Aeronautical fixed service	4	Medium
Flight Plan Data	4	Medium
Correlated position report	4	Medium
AMAN processing function	4	Medium
Trajectory prediction	4	Medium
Flight Object	4	Medium
Flight Object Server	4	Medium
Monitor and provide alerts	4	Medium
P-RNAV capability	4	Medium
Meteorological information	4	Medium
CMAN processing function	4	Medium

It should be noted that the overall impact of 4 primarily results from the 'Branding' Impact Area. The rationale is that loss of CIA may not strongly impact operations as the fall-back will be to current operating methods; with a period without the benefits of Extended AMAN. The public consequences of a successful attack will however attract widespread media interest and analysis that have a high impact on the reputation of the organisations involved. Whilst this may be the case in the initial years of operation, over time normal operations may become reliant on AMAN. For ATSUs that are at or near system capacity, this reliance will mean that the impact of loss of CIA may become more operationally critical and other impact areas than branding may dominate (e.g. capacity or performance).

A.4 Supporting Assets

From a review of OFA 4.1.2 documentation a list of supporting assets has been created and reviewed with OFA 4.1.2 participants. The supporting assets are defined at the level of major system components. Not all of the supporting assets are carried through to the risk assessment so the table below shows whether they have been included and the rationale for inclusion or exclusion.

From the table, the following assets only have been chosen for further assessment: **AMAN Processor**, **ADS-C datalink**, **ADS-C Processor**. The rationale for excluding the remaining supporting assets is largely based on: (a) whether the systems are already operational; and (b) whether the security requirements will be driven by a different primary capability. A high level risk assessment of CPDLC/ADS-C has been covered in the security risk assessment of OFA 04.01.05 i4D+CTA and the results of this have been integrated into this risk assessment.

Table 31: Supporting assets

Name	Location	Description	Include?	Rationale for inclusion/exclusion
AMAN processor	ATSU	AMAN processor	Include	New or extended capability of existing SA.
CMAN processor	ATSU	CMAN processor	Include	New or extended capability of existing SA.
CWP	ATSU	CWP	Include	Extended usage/capability of existing SA.
ATCO	ATSU	ATCO	Exclude	Controls will be in place in support of core service of this SA.
Air Crew	A/C	Air Crew	Exclude	Controls will be in place in support of core service of this SA.
OLDI	GND	OLDI	Exclude	Controls will be in place in support of core service of this SA.
SWIM	GND	SWIM	Exclude	New capability but has existing Security Risk Assessment (SRA).
RTF System	A/C + GND	RTF System to support voice communications between ground and aircraft. Excludes Tx/Rx antennae which are defined as a separate Supporting Asset.	Exclude	Controls will be in place in support of core service of this SA.
Flight Object Server	ATSU	Flight Object Server	Exclude	Discussion with OFA 4.1.2 but wider issue for SESAR to be carried forward.
Meteorological database	ATSU	Meteorological database	Exclude	Controls will be in place in support of core service of this SA.

Name	Location	Description	Include?	Rationale for inclusion/exclusion
ADS-C datalink(s)	A/C + GND	ADS-C datalink(s)	Include	Extended usage/capability of existing SA.
ADS-C processor	A/C + GND	ADS-C processor	Include	Extended usage/capability of existing SA.
FMS	A/C	FMS (inc FMS required time of arrival (RTA) in i4D a/c)	Exclude	Controls will be in place in support of core service of this SA.
ATIS	A/C	ATIS, which provides up-to-date meteorological information to aircrew.	Exclude	Extended usage of existing SA.
SDP	ATSU	Surveillance Data Processing (Radar / ADS-B) and associated tools and comms/distribution.	Exclude	Controls will be in place in support of core service of this SA.
P-RNAV capability	A/C	P-RNAV capability	Exclude	Controls will be in place in support of core service of this SA.
Mode S radar	A/C + GND	Mode S radar	Exclude	Controls will be in place in support of core service of this SA.
Primary radar	GND	Primary radar	Exclude	Controls will be in place in support of core service of this SA.
Electronic Flight Bag	A/C	Electronic Flight Bag	Exclude	Discussion with OFA 4.1.2 on the basis that this could be used by aircrew for 'what-if' flight planning but no provision for this in Step 1.
DMAN	GND	DMAN	Exclude	Considered independent operationally from AMAN.
FDPS	ACC	Flight Data Processing system. Provides flight plan data to AMAN.	Exclude	Controls will be in place in support of core service of this SA.
A/G Transmit/Receive aerial stations		A/G Transmit/Receive aerial stations	Exclude	Controls will be in place in support of core service of this SA.

A.5 Vulnerability and threat assessment

A.5.1 Vulnerabilities

The key vulnerability concerns are as follows:

- **AMAN Processor.** The AMAN processor is a software system which is assumed to be hosted on equipment similar to existing ATM systems. Vulnerabilities will occur from the specific host equipment and its operating system. Without appropriate built in controls the

AMAN software may be vulnerable to a range of threats from external or internal sources that are not controlled by e.g. firewalls, malware/virus protection etc.

- **CMAN Processor.** As for AMAN processor.
- **ADS-C datalink.** The concern about ADS-C datalink is the vulnerability concerns are jamming and spoofing. Jamming can be a localised threat and may not be a major issue for the OFA at the regional level. Spoofing or similar threats to integrity may present more of a problem.
- **ADS-C processor(s).** The ADS-C processing functions have the same vulnerabilities as any software system and the issues will be as for the AMAN Processor within ground facilities and other avionics systems on-board aircraft.

A.5.2 Threats

Based on the assumption that MSSCs will be implemented, the vulnerabilities of the supporting assets will be reduced. We have therefore included the following threats only:

- **Abuse of rights and privilege escalation**. Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions, assumed as abuse of rights.
- **Corruption of data**. Deterioration of computer data as a result of some external agent. Most of the time, corruption of data will lead to produce unexpected results when accessed by the system or the related application. Nevertheless, in case of coherent corruption, this may lead to deception and unwanted behaviour of the personnel, systems and application.
- **Cyber intrusion**. Illegal access to devices, networks and systems using computer or related networks or systems. The attacker may use vulnerabilities or back doors on systems at the boundaries to commit his intrusion.
- **Malware**. Contraction of "malicious software" that corresponds to any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware, programming that gathers information about a computer user without permission.
- **Jamming**. Transmission of a noise signal across one or more of the wireless frequencies to raise the noise level or overload the receiver circuitry and cause a loss of communication. Jamming of wired signals may require physical access and is considered out of scope.
- **Spoofing**. Situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. For instance, it could be used in ground message spoofing to send wrong information to pilots as if it was coming from a legitimate ATCO. Replay attack can also been considered in this threat, and consists in interception of valid data transmission which will be maliciously or fraudulently repeated or delayed.
- **Denial of service**. Denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. One common method of attack, called 'flooding', involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable.

Combining these threats and supporting assets leads to a number of ‘threat scenarios’. A threat scenario is a combination of a threat acting on a supporting asset with identified vulnerabilities which has an impact (derived from the primary asset it supports). The identified threat scenarios are shown in the following table.

A.6 Risk evaluation

Risk has been estimated by applying a level of likelihood to the threat scenarios. The level of likelihood has been estimated by the authors using the following scale:

Likelihood	Qualitative interpretation
5. Certain	There is a high chance that the scenario successfully occurs in the short term.
4. Very likely	There is a high chance that the scenario successfully occurs in the medium term.
3. Likely	There is a high chance that the scenario successfully occurs during the lifetime of the project.
2. Unlikely	There is a low chance that the scenario successfully occurs during the lifetime of the project.
1. Very Unlikely	There is very little or no chance that the scenario successfully occurs during the lifetime of the project.

As can be seen in the table, the assessment of likelihood, over the life-time of the system is between 2 and 3 for the different threats:

Table 32: Threat scenarios and corresponding risk

Threat	Supporting Asset	Effect on CIA	Summary impact	Likelihood	Risk
Spoofing	ADS-C datalink(s)	I	4	3	High
Denial of service	ADS-C datalink(s)	A	4	3	High
Cyber intrusion	ADS-C processor	C I A	4	3	High
Malware	ADS-C processor	C I A	4	3	High
Cyber intrusion	AMAN processor	C I A	4	3	High
Malware	AMAN processor	C I A	4	3	High
Jamming	ADS-C datalink(s)	A	4	2	Medium
Abuse of rights and privilege escalation	ADS-C processor	C I A	4	2	Medium
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	Medium

A.7 Risk treatment

A.7.1 Overview

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.

As discussed earlier, a number of supporting assets were excluded from the assessment as they are already operational systems or the security requirements will be 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.7.2 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.

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 / CMAN 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.7.3 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
Jamming	ADS-C datalink(s)	A	4	1	Medium
Cyber intrusion	ADS-C processor	C I A	4	1	Medium
Malware	ADS-C processor	C I A	4	2	Medium
Abuse of rights and privilege escalation	ADS-C processor	C I A	4	1	Medium
Corruption of data	ADS-C processor	I A	4	2	Medium
Cyber intrusion	AMAN processor	C I A	4	1	Medium
Malware	AMAN processor	C I A	4	1	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
Cyber intrusion	CMAN processor	C I A	4	1	Medium
Malware	CMAN processor	C I A	4	1	Medium
Abuse of rights and privilege escalation	CMAN processor	C I A	4	2	Medium
Corruption of data	CMAN processor	I A	4	2	Low

A.7.4 Comparison with safety requirements

The security risk assessment has been cross-checked the recommendations of the safety risk assessment (05.06.04 D34-001 Safety Assessment Report for Tactical TMA and En-route Queue Management) and the SPR [13] and the following requirements will also have a mitigating impact on security risk:

REQ-05.04.02-SPR-0005.0037	E-AMAN shall continuously monitor and diagnose its operation and alert Sequence manager if its operational status has exceeded applicable operational parameters.
REQ-05.04.02-SPR-0005.0038	E-AMAN shall continuously monitor the quality of its input data and alert Sequence manager if input data quality is suspect.

REQ-05.04.02-SPR-0005.0401	CMAN shall continuously monitor and diagnose its operation and alert Sequence manager if its operational status has exceeded applicable operational parameters.
REQ-05.04.02-SPR-0005.0401	CMAN shall continuously monitor the quality of its input data and alert Sequence manager if input data quality is suspect.

A.7.5 Further security requirements development

A large part of the rationale for developing security controls during the development phase is to build controls into the detailed specification and design work. The preceding list of recommended controls should therefore be considered as an envelope for refinement and detailed specification by the system designers. A further point of reference is the SWIM security work [12]. The following are also important to note:

- Some of the above controls may be costly to implement and this should be taken into account in specifying. As an example, the control ‘Standby / Alternate Facilities’ for AMAN/CMAN Processor should be assessed in the context of an ANSPs’ overall contingency/fall-back strategy.
- The risk assessment has assumed that other controls will be in place for some of the systems shown in the supporting assets list in Table 2.

A.8 Conclusions

The security risk assessment of OFA 4.1.2 has highlighted a number of key risks to the following Supporting Assets: AMAN Processor, CMAN 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.

A.9 References

[1] 16.06.02 OFA 04.01.05 i4D+CTA Security Risk Assessment (2013).

[2] 16.06.02 Extended AMAN Security Case (2013).

[3] 04.03-D012-i4D and CTA OSED Requirement - Part 1, 5/11/2014.

[4] 04.03-D07-IOP OSED and Requirements - Part 1 OSED, 5/11/2014.

[5] 05.06.01-D67, Step 1 OSED - second iteration, 27/11/2012.

[6] 05.06.01 D74 Step 1 OSED - Iteration 3, 01.00.00, 11/09/2013.

[7] 04.03.00 D07-IOP OSED and Requirements - Part 3, 21/06/2011.

[8] 05.06.04 D34-002 INTEROP5.6.4 Interoperability Requirements (INTEROP) for TS-0305-A, 00.00.01, 31/03/2015.

[9] 16.06.02, SESAR ATM Security Reference Material - Level 2 - 2014, D101, 00.04.02.

[10] D131 16.6.2 Security Database Application 00.03.01.

[11] 05.06.04 D34-001 Safety Assessment Report for Tactical TMA and En-route Queue Management.

[12] 14.02.0.2 D23 ‘SWIM Security Risk Assessment’, 00.01.01 21/11/2014.

[13] 05.04.02-DEL05-Step 1 Final SPR-00.00.20.

A.10 Annex - Summary of MSSCs

The following table lists the MSSCs:

Ref	Name	Description
C1	Security policy compliance	The OFA shall produce, approve, and adopt a security policy which complies with the SESAR security policy; the policy shall be communicated to all relevant parties.
C2	Security policy compliance	The OFA shall review the information and ATM services security policy and ensure that it remains effective.
C3	Security Management	The OFA shall provide the resources needed for information and ATM services security and assign roles and responsibilities for all security management functions.
C4	Security Control Management	The OFA shall ensure that the implementation of information and ATM services security controls is co-ordinated across the OFA.
C5	External relationships	The OFA shall have procedures in place that specify when and by whom external authorities (e.g. law enforcement, fire department, supervisory authorities) shall be contacted in the event of a security incident.
C6	External relationships	The OFA shall review the security requirements and risks of every external access to information or ATM Services before granting access.
C7	Asset identification	All assets shall be clearly identified and an inventory of all important assets drawn up and maintained
C8	Asset ownership	All information and ATM services associated with information processing facilities shall be 'owned' by a designated responsible individual or OFA role.
C9	Asset use rules	Rules for the acceptable use of assets shall be identified, documented, and implemented.
C10	Information labelling and handling, Classification guidelines	All Information and ATM services shall be classified in terms of its value, legal requirements, sensitivity and criticality to OFAs.
C11	Information labelling and handling, Classification guidelines	An appropriate set of procedures for information and ATM service labelling and handling shall be developed and implemented in accordance with the classification scheme adopted
C12	Personnel verification	Background verification checks on all staff shall be carried out in accordance with relevant laws, regulation, and ethics. The checks shall be proportional to the roles and responsibilities, in particular in respect to the business requirements (e.g. safety-critical function, developments), the classification of information to be accessed, and the perceived risks.
C13	Personnel compliance with security policy and procedures	Staff shall apply security in accordance with the established policies and procedures.
C14	Security Management	Staff shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function.

Ref	Name	Description
C15	Review of user access rights	Staff shall undergo a formal rotation, change, and close-out procedure.
C16	Security perimeter	Security perimeters shall be used to protect ATM sensitive areas and ATM processing facilities.
C17	Review of user access rights	ATM secure areas shall be protected by appropriate entry controls which allow access only to authorized personnel and which detect unauthorized access.
C18	Backup facilities	ATM equipment shall be provided with auxiliary means to compensate for deliberate compromising of power supply, overheating and fire.
C19	Cabling security	ATM cabling shall be protected from deliberate damage, eavesdropping or interference.
C20	Equipment maintenance	ATM equipment shall be maintained and serviced to ensure their availability and integrity.
C21	Equipment maintenance	Operating ATM procedures shall be documented, maintained, and made available to all users who need them.
C22	System/equipment control	Changes to ATM information processing facilities, ATM services and systems shall be controlled.
C23	System/equipment control	Acceptance criteria for new ATM information systems or services, upgrades, and new versions shall be established, and suitable security tests of the ATM system(s) carried out during development and prior to acceptance.
C24	Viruses & Malware Installation and Patches	Detection, prevention, and recovery controls to protect ATM software against malicious code and appropriate user awareness procedures shall be implemented.
C25	Information/Software Backup	Back-up copies of ATM information and software shall be taken and tested regularly in accordance with an agreed backup policy.
C26	Network routing control, Network connection control	ATM Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the ATM systems and applications using the network, including information in transit.
C27	Information/Media management	There shall be procedures in place for the management of removable media.
C28	Information/Media management	Media shall be disposed of securely and safely when no longer required, using formal procedures.
C29	Information/Media management	Procedures for the handling and storage of ATM information shall be established to protect ATM services and information from unauthorized disclosure or misuse.
C30	Information/Media management	ATM system documentation shall be protected against unauthorized access.
C31	Information exchange management	Formal exchange policies, procedures, and controls shall be in place to protect the exchange of ATM services and information through the use of all types of communication facilities. Agreements shall be established for the exchange of ATM services and information and software between the OFA and external parties.

Ref	Name	Description
C32	Information exchange management	Information conveyed by electronic messaging shall be appropriately protected.
C33	Information flow monitoring	Procedures for monitoring the use of ATM services and information processing facilities shall be established and the results of the monitoring activities reviewed regularly.
C34	Access information management	ATM logging facilities and log information shall be protected against tampering and unauthorized access.
C35	Access information management	Faults shall be logged, analysed, and appropriate action taken.
C36	Access management	An access control policy shall be established, documented, and reviewed based on business and security requirements for access
C37	Access management	There shall be an access control procedure in place for granting and revoking access to all information systems and services.
C38	Access management	The allocation of access privileges shall be restricted to users who have been specifically authorized to use ATM facilities, and such privileges should be controlled by a formal management process.
C39	Segregation in networks	For shared ATM networks, especially those extending across the OFA's boundaries, the capability of users to connect to the network shall be restricted, in accordance with the access control policy and requirements of the operational applications"
C40	Software installation control	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
C41	Hardware management/control	Sensitive systems shall have a dedicated (protected) computing environment.
C42	Data Input Credibility Checking AND Authentication	User shall be required to follow good security practices in the protection of authentication information or devices.
C43	Equipment management/control	Users shall ensure that unattended equipment has appropriate protection.
C44	Information/Media management	A security policy for papers and removable storage media and information processing facilities shall be adopted.
C45	Equipment management/control	Every specification for new or updated facilities includes security requirements.
C46	Equipment management/control	An operational process which controls how system changes are approved and implemented, and how security considerations are incorporated in the change process shall be enacted.
C47	System management/testing	Security testing shall be performed whenever a system is updated
C48	Security reporting	ATM service and Information security events shall be reported through appropriate management channels as quickly as possible.

Ref	Name	Description
C49	Security reporting	All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses or malfunctions in ATM systems or services.
C50	Contingency management	Management responsibilities and procedures shall be established to ensure an effective and orderly response to ATM service and information security incidents.
C51	Evidence management	Where a follow-up action against a person or organization after an ATM service or information security incident involves legal action (either civil or criminal), pieces of evidence shall be collected, retained, and presented to the relevant jurisdiction(s).
C52	Security requirements management	A managed process shall be developed and maintained that addresses the ATM service and information security requirements needed for ATM business continuity.
C53	Horizon scanning	Events that can cause interruptions to ATM business processes shall be identified, along with the probability and impact of such interruptions and their consequences for ATM information security.
C54	Contingency management	Plans shall be developed and implemented to maintain or restore operations and to ensure the availability, integrity and confidentiality of information at the required level and in the required time scales following interruption to critical ATM business processes.
C55	Contingency management	ATM business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.
C56	Security requirements compliance	Compliance to statutory, regulatory and contractual requirements shall be checked, and the correct and authorized use of facilities and assets shall be defined.
C57	Regulatory requirements compliance	Any personal or protectively classified information shall be protected in accordance with National and European requirements.

-END OF DOCUMENT-

The security risk assessment of OFA 4.1.2 has highlighted a number of key risks to the following Supporting Assets: AMAN Processor, CMAN 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. A question that arose is on whether live trials will be the best validation method for all controls. This will depend on whether the next stage of system development is still pre-operational. If this is the case then a mix of live-trial and other means may be needed. Therefore, there are two requirements MSSC and non-MSSC as below:

[REQ]

Identifier	REQ-05.04.02-SEC-0010.0020
Requirement	CMAN with Extended AMAN shall implement the following security controls to complement the MSSCs: AMAN and ADS-C processor · 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).
Title	Additional Security Controls to MSSCs
Status	<In Progress >
Rationale	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 and CMAN Processor • Data Input Credibility Checking AND Authentication (MSSC C42) • Viruses & Malware Installation and Patches (MSSC C24)
Category	<Security>
Validation Method	<Live Trial>
Verification Method	<Inspection>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.02-DOD-OPR1.0011	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A
<ALLOCATED_TO>	<Functional block>	Arrival Mgt (AMAN)	N/A
<APPLIES_TO>	<Service>	ArrivalManagementInformation	N/A

[REQ]

Identifier	REQ-05.04.02-SEC-0010.0010
Requirement	CMAN with Extended AMAN shall implement the applicable minimum set of security controls, with particular focus on: • Data Input Credibility Checking AND Authentication (MSSC C42) • Viruses & Malware Installation and Patches (MSSC C24)

Title	SESAR Minimum Set of Security Controls (MSSCs)
Status	<In Progress>
Rationale	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 and CMAN Processor • Data Input Credibility Checking AND Authentication (MSSC C42) • Viruses & Malware Installation and Patches (MSSC C24)
Category	<Security>
Validation Method	<Live Trial>
Verification Method	<Inspection>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	REQ-05.02-DOD-OPR1.0011	<Full>
<APPLIES_TO>	<Operational Focus Area>	OFA04.01.02	N/A
<ALLOCATED_TO>	<Functional block>	Arrival Mgt (AMAN)	N/A
<APPLIES_TO>	<Service>	ArrivalManagementInformation	N/A

Additionally, and independently of the above mentioned assessment, security attributes in the form of performance attribute “Confidentiality” to Information Exchange Requirements was determined through expert judgment.

A.10.1 Environment impact assessment

While the project supported several exercises fully targeting TS-0303, and many of the activities performed assessments from the perspective of fuel burn and CO2 emissions, no requirements were identified for inclusion in the SPR.

Appendix B Reference to relevant E-AMAN Requirements

B

B.1 Safety Requirements

Identifier	REQ-05.06.04-SPR-0005.0001
Requirement	E-AMAN shall build arrival sequence
Title	Build arrival sequence
Status	<Validated>
Rationale	D05-001-SAR-SR-01; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0002
Requirement	AMAN ATSU shall provide E-AMAN with flight information regarding all flights inbound to the destination airport.
Title	Provide flight information to E-AMAN
Status	<Validated>
Rationale	D05-001-SAR-SR-02; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0003
Requirement	AMAN ATSU shall provide E-AMAN with flight information regarding an arriving flight when the flight reaches the defined Eligibility Horizon.
Title	Provide flight information at EH
Status	<Validated>
Rationale	D05-001-SAR-SR-03; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0004
Requirement	Flight data distribution shall ensure that flight information provided to E-AMAN is correct and accurate to the standard as required for the provision of the ATC separation service.
Title	Provide correct and accurate flight information
Status	<Validated>
Rationale	D05-001-SAR-SR-04; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0005
Requirement	Sequence Manager shall supervise and control E-AMAN.
Title	Supervise and control E-AMAN
Status	<Validated>
Rationale	D05-001-SAR-SR-05; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0006
Requirement	E-AMAN shall insert a representation of an inbound flight reaching the Eligibility Horizon in the sequence in accordance with applicable rules and strategies.
Title	Sequence new flight
Status	<Validated>
Rationale	D05-001-SAR-SR-06; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0007

Requirement	Sequence manager shall adjust control parameters of E-AMAN to reflect actual and planned operational conditions. In all cases this refers to downstream constraints such as desired landing runway throughput or holding stack entry rate/delay. In specific cases, other constraints may be considered as required by local implementation.
Title	Adjust E-AMAN parameters
Status	<Validated>
Rationale	D05-001-SAR-SR-07; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0008
Requirement	Sequence manager shall have the authority to select and engage ATC strategies.
Title	Select and engage ATC Strategies
Status	<Validated>
Rationale	D05-001-SAR-SR-08 Appendix A 485.R2; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0011
Requirement	E-AMAN shall update the sequence to account for new and relevant information.
Title	Update sequence
Status	<Validated>
Rationale	D05-001-SAR-SR-11; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0012
Requirement	Sequence manager shall introduce changes and adjustments to the sequence as deemed necessary for safe and expedient flow of inbound traffic.
Title	Adjust sequence
Status	<Validated>
Rationale	D05-001-SAR-SR-12 D05-001-SAR-SR-16; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0013
Requirement	Sequence manager shall use COTR to coordinate with other controllers regarding sequence build as required.
Title	Coordinate with EXE/PLN controllers
Status	<Validated>
Rationale	D05-001-SAR-SR-13; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0014
Requirement	For each inserted flight E-AMAN shall plan the flight so as to comply with the required traffic flow parameters and subsequently determine whether there exists a need to delay or expedite the flight and issue an advisory to associated controllers.
Title	Assess need for delay
Status	<Validated>
Rationale	D05-001-SAR-SR-14; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0016
Requirement	EXE/PLN En-Route sector controllers shall implement the sequence and delay/expedition of flights under their control before flights reach coordination point with Approach sectors.
Title	Implement sequence in Upstream ATSU
Status	<Validated>
Rationale	D05-001-SAR-SR-18 D05-001-SAR-SR-20; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0031
Requirement	Controllers shall continuously monitor traffic in their sectors and ensure that the AMAN advisories are complied with.
Title	Manage arrival traffic
Status	<Validated>
Rationale	D05-001-SAR-SR-38 D05-001-SAR-SR-39; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0036
Requirement	Quality of trajectory prediction used by E-AMAN to build the sequence shall be sufficient to support concept operation.
Title	Quality of TP
Status	<Validated>
Rationale	D05-001-SAR-SR-44 Appendix A 485.04; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0037
Requirement	E-AMAN shall continuously monitor and diagnose its operation and alert Sequence manager if its operational status has exceeded applicable operational parameters. *Note: Operational service parameters will result from SPR-INTEROP, technical design and local implementation*s.
Title	E-AMAN self monitor and diagnose
Status	<Validated>
Rationale	D05-001-SAR-SR-45 D05-001-SAR-SR-47; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0038
Requirement	E-AMAN shall continuously monitor the quality of its input data and alert Sequence manager if input data quality is suspect.
Title	E-AMAN input data check
Status	<Validated>
Rationale	D05-001-SAR-SR-46 D05-001-SAR-SR-47 Appendix A 485.05; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0039
Requirement	Upstream ATSU ATM system shall receive, process and display arrival management information.

Title	Receive arrival management information Upstream
Status	<Validated>
Rationale	D05-001-SAR-SR-48; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0040
Requirement	E-AMAN configuration shall provide functionality to define rules to govern potential overtake situations, as functions of route, aircraft type and its associated performance characteristics, distance-to-go, downlinked aircraft parameters if available, strategic prioritization, other data sources and other operational parameters as available.
Title	Define overtake rules as ATC strategy
Status	<Validated>
Rationale	D05-001-SAR-SR-49 Appendix A 485.R2 Appendix A 244.02 Appendix A 244.04; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0041
Requirement	Sequence manager shall be able to arbitrarily assign a runway to a flight
Title	Assign runway to flight
Status	<Validated>
Rationale	D05-001-SAR-Sequence manager-N01; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0042
Requirement	Sequence manager shall be able to prompt E-AMAN to recalculate an arbitrary portion of a stabilized sequence.
Title	Manual recalculate sequence
Status	<Validated>
Rationale	D05-001-SAR-Sequence manager-N02; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0043
Requirement	E-AMAN shall make consistent use of best source of information for the following service data: - operational parameters - flight information - trajectory prediction
Title	Consistent use of best data source
Status	<Validated>
Rationale	D05-001-SAR-E-AMAN-N01; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0044
Requirement	E-AMAN shall provide to Sequence manager at the minimum the following arrival management information: - value of advisory

	- sequence number - time ordered sequence - sequence filterable by runway/metering or feeder fix - *Note: distance to go is an optional information item as per local implementation.*
Title	Arrival management information provided to Sequence manager
Status	<Validated>
Rationale	D05-001-SAR-E-AMAN-N02; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0045
Requirement	Configuration of E-AMAN shall be validated and verified prior to operational deployment.
Title	Validate configuration
Status	<Validated>
Rationale	D05-001-SAR-E-AMAN-N03; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0046
Requirement	E-AMAN shall consider any change introduced in the sequence by Sequence manager as permanent unless prompted to recalculate by Sequence manager
Title	Consider change introduced by Sequence manager
Status	<Validated>
Rationale	D05-001-SAR-E-AMAN-N04; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0347
Requirement	E-AMAN shall, either through a parameter setting or through internal logic, define a horizon with respect to the landing time. In the time range defined by the point where flight information is received, and the horizon, E-AMAN shall freely change ordering of flights in the sequence unless prohibited from doing so by input from Sequence manager. The horizon is referred to as Stable Sequence Horizon (SSH) in this SPR and its related OSED.
Title	Define SSH
Status	<Validated>
Rationale	D05-001-SAR-E-AMAN-N06; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.6.04-SPR-0005.0048
Requirement	E-AMAN shall not automatically change order in the sequence of traffic that has passed SSH..
Title	Inhibit reordering past SSH
Status	<Validated>
Rationale	D05-001-SAR-E-AMAN-N06 Appendix A 485.02; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0049

Requirement	E-AMAN shall not constrain a flight by an advisory when it is determined that there is no need for delay.
Title	Judicious use of constraints
Status	<Validated>
Rationale	D05-001-SAR-E-AMAN-N07; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0050
Requirement	E-AMAN shall be configurable to indicate explicitly to Sequence manager and ATCO an intentionally unconstrained flight.
Title	Indicate unconstrained flight
Status	<Validated>
Rationale	D05-001-SAR-E-AMAN-N08; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0051
Requirement	E-AMAN shall determine and assign runway to a flight in accordance with a predefined runway utilization strategy.
Title	Assign runway to flight
Status	<Validated>
Rationale	D05-001-SAR-E-AMAN-N09; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0052
Requirement	Controllers in any involved ATSU (Upstream and Destination) shall coordinate with Sequence manager with respect to desired changes in sequence as required.
Title	Coordinate sequence actions with Sequence Manager
Status	<Validated>
Rationale	D05-001-SAR-ATCO-N01; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0054
Requirement	Sequence manager shall be able to insert a tactical reservation of arbitrary length in the sequence to account for abnormal cases such as low performance aircraft or short term runway closure.
Title	Manually reserve block in sequence
Status	<Validated>
Rationale	D05-001-SAR-SR-A01; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0055
Requirement	Sequence manager shall be able to designate a flight for special treatment where deemed necessary
Title	Special status of flight in sequence
Status	<Validated>
Rationale	D05-001-SAR-SR-A02; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0056
Requirement	E-AMAN shall exclude from sequencing a flight designated by Sequence manager for special treatment.
Title	Special flight excluded from sequencing
Status	<Validated>
Rationale	D05-001-SAR-SR-A03; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0057
Requirement	Sequence manager shall be able to manually define and insert a flight in the sequence.
Title	Manually sequence flight
Status	<Validated>
Rationale	D05-001-SAR-SR-A04; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0058
Requirement	Sequence manager shall be able to manually remove a flight from the sequence.
Title	Manually desequence flight
Status	<Validated>
Rationale	D05-001-SAR-SR-A05; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0059
Requirement	E-AMAN shall monitor communication of Arrival Management information in Upstream ATSU and alert Sequence Manager if reception of said information cannot be verified.
Title	Alert on no-receipt from Upstream.
Status	<Validated>
Rationale	D05-001-SAR-SR-48; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Note: Following requirements contain likelihood figures that may require further consolidation during implementation. Validation results do not refine the expressed needs further. Figures have been achieved by expert assessment.

Identifier	REQ-05.06.04-SPR-0005.0103
Requirement	The likelihood of E-AMAN failing to accept and correctly process human input shall be no more than 1e-3 SOH, approximately once every 6 weeks.
Title	E-AMAN failure to accept input
Status	<Validated>
Rationale	D05-001-SAR-SR-103; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0112
Requirement	Sequence manager shall be trained in control, supervision, operation and HMI input/output functions of E-AMAN.
Title	Sequence manager training
Status	<Validated>
Rationale	D05-001-SAR-SR-112 D05-001-SAR-SR-113 Appendix A 485.R1 Appendix A 244.05; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0115
Requirement	Controllers shall be trained with respect to the following actions : • Coordination of tasks related to sequence implementation • Implementation of advisories • Continuous monitoring and assessment of compliance with clearances related to implementation of AMAN advisories
Title	Controller training
Status	<Validated>
Rationale	D05-001-SAR-SR-115 D05-001-SAR-SR-117 D05-001-SAR-SR-127 Appendix A 485.R1 Appendix A 695.02 Appendix A 695.22 Appendix A 244.05; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0116
Requirement	E-AMAN shall be designed to facilitate coordination of sequence build and implementation related information between Sequence manager and EXE/PLN controllers active in or contributing to the implementation of the sequence.
Title	Coordination function facilitated by E-AMAN
Status	<Validated>
Rationale	D05-001-SAR-SR-116 Appendix A 695.19; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0128
Requirement	The likelihood that incorrect flight information is provided by flight data processing system shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.
Title	Incorrect flight data provided in ATSU Destination
Status	<Validated>
Rationale	D05-001-SAR-SR-128; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0131

Requirement	The likelihood that ATSU Destination provides incorrect STAR/RWY information to Sequence Manager/E-AMAN shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.
Title	Incorrect STAR/RWY provided
Status	<Validated>
Rationale	D05-001-SAR-SR-131; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0132
Requirement	The likelihood that [destination] provides to Sequence Manager /E-AMAN landing rate information that is incompatible with required operating parameters of the destination airport shall be no more than 2.5e-4 SOH, approximately once every 5.5 months. *Note: Under [destination] consider the constituent function that supplies the respective runway usage parameters to E-AMAN or Sequence Manager, as per local implementation.*
Title	Incorrect runway usage constraint provided
Status	<Validated>
Rationale	D05-001-SAR-SR-132; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0133
Requirement	The likelihood that ATSU fails to define a correct ATC strategy shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.
Title	Incorrect ATC Strategy defined
Status	<Validated>
Rationale	D05-001-SAR-SR-133 Appendix A 485.R2 Appendix A 244.02 Appendix A 244.04; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0134
Requirement	The likelihood that ATSU fails to implement agreed delay sharing strategy in AMAN configuration shall be no more than 2e-3 SOH, approximately once every three weeks.
Title	Delay sharing strategy not implemented in AMAN
Status	<Validated>
Rationale	D05-001-SAR-SR-134 Appendix A 695.01 Appendix A 695.03 Appendix A 244.04; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0135
Requirement	[Local implementation] The likelihood that coordination and transfer equipment is inoperative in support of arrival management shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.
Title	Coordination and Transfer inoperative

Status	<Validated>
Rationale	D05-001-SAR-SR-135; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0136
Requirement	The likelihood that CWP HMI fails to present AMAN advisories to the controller shall be no more than 5e-4 SOH, approximately once every 12 weeks.
Title	CWP failure to present advisories
Status	<Validated>
Rationale	D05-001-SAR-SR-136; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0137
Requirement	The likelihood that CWP HMI presents incorrect AMAN advisories to the controller shall be no more than 5e-4 SOH, approximately once every 12 weeks.
Title	CWP presents incorrect advisories
Status	<Validated>
Rationale	D05-001-SAR-SR-137; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0151
Requirement	The likelihood that inaccurate Trajectory Prediction information is provided to E-AMAN shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.
Title	Inaccurate trajectory prediction
Status	<Validated>
Rationale	D05-001-SAR-SR-151 Appendix A 485.04; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0152
Requirement	The likelihood that Trajectory Prediction information is unavailable to E-AMAN shall be no more than 2.5e-4 SOH, approximately once every 5.5 months.
Title	Trajectory prediction not available
Status	<Validated>
Rationale	D05-001-SAR-SR-152; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Note: For the following group of requirements a tolerable level of risk cannot be prescribed nor demonstrated in the form of failure rates or conditions per unit of time or operation as would be the case in functional elements of mechanical or electrical character. Instead, the tolerable level of risk must be designed into the software by ensuring that proper design validation, verification and assurance procedures are followed. A Software Assurance Level (SWAL) implicitly recognizes that in software design, defined in ESARR. The level is indicated in each relevant requirement.

Identifier	REQ-05.06.04-SPR-0005.0154

Requirement	Software functions associated with Trajectory prediction and its provision to the arrival management process shall comply with SWAL4 or other design assurance criteria as applicable to effect severity class 4, “serious incident”.
Title	TP SWAL
Status	<Validated>
Rationale	Software functions cannot be allocated safety targets in terms of failure probabilities. ; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0155
Requirement	Software functions associated with E-AMAN or otherwise the arrival management process shall comply with SWAL4 or other design assurance criteria as applicable to effect severity class 4, “serious incident”.
Title	E-AMAN SWAL
Status	<Validated>
Rationale	Software functions cannot be allocated safety targets in terms of failure probabilities. ; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0156
Requirement	Software functions associated with Flight data production and distribution for the purposes of the arrival management process shall comply with SWAL4 or other design assurance criteria as applicable to effect severity class 4, “serious incident”.
Title	Flight data SWAL
Status	<Validated>
Rationale	Software functions cannot be allocated safety targets in terms of failure probabilities. ; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

B.2 Performance Requirements

Identifier	REQ-05.06.04-SPR-0005.0217
Requirement	Arrival Management Information (shared IE) shall be consistently and simultaneously distributed to all concerned actors.
Title	Updated arrival management information distributed to users
Status	<Validated>
Rationale	Appendix A 485.17; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

Identifier	REQ-05.06.04-SPR-0005.0226
Requirement	To aid controller decision support, constraints imposed on a flight by the transferring sector with respect to sequence implementation should be provided to the receiving controller.
Title	Provide to the controller information about constraints imposed by transferring sector
Status	<Validated>
Rationale	Appendix A 695.19; E-AMAN Requirement from 5.6.4 / 5.6.7 SPR

-END OF DOCUMENT-