Surveillance

Safety case

Porto Santo radar replacement

Prepared by:

Navegação Aérea de Portugal – NAV Portugal, E.P.E.
Rua C, Edifício 118, Aeroporto de Lisboa
1700-007 Lisboa
PORTUGAL

Ref.: 9090.SC.703
Version: 1.00
Date: 19-03-01 (aa-mm-dd)

INTENTIONALLY LEFT BLANK

0 Document Data

0.1 Copyright Note

0.2 Document Parts List

Component Name	Version	Format
SC_RAPOSA	1.00	Word for Windows

0.3 Document Revision History

Version	Date	Change Reference or Comment	Author	Changed Sections / Pages
0.01	18-04-11	Document creation.	Paula Santos	All
0.02	18-09-28	Add safety argument. Describe assessment process.	Paula Santos	All
0.03	18-11-05	Consolidate process and safety case Complete compliance matrixes.	Paula Santos	All
0.04	18-11-09	Consolidate document for review by TF.	Paula Santos	2.5, 3.2. 3.3, Appendix A & B
0.05	18-12-28	Integrate received comments	Paula Santos	Section 2 & 3
0.06	19-02-18	Consolidate document	Paula Santos	Section 2 & 3
1.00	19-03-01	Approved version.	Paula Santos	Minor changes.

0.4 Document Build Instructions

This document makes extensive use of word automations for cross referencing and traceability. The electronic version of this document is available in the following CVS repository:

- ...\9090_Surveillance\Projectos\Safety\Raposa

0.5 Document Approval

Organization	Representative Name	Signature and Date
DSS	Abel Paraiba	Abel Paraiba 2019.03.12 15:00:34 Z
DOPLIS	Carlos Reis	carlos.reis@nav.pt 2019.03.11 12:14:57 Z
DEP	Carlos Alves	carlos.alves@nav.pt 2019.03.03 12:26:55 Z
NASO	Paulo Encarnação	Digitally signed by Paulo Encarnacao Date: 2019.03.03 08:27:45 Z

0.6 Table of Contents

0.7 Table of Figures

0.8 Table of Tables

1 Introduction

The aim of this safety case is to demonstrate that the upgrade of the Porto Santo radar is a safe change. The upgrade of the Porto Santo radar to Mode S is performed in two phases, the first of which was already successfully completed. The second phase requires a long period of unavailability of this radar.

Chapter 1 – this one – introduces the document, presents the scope of the work, the assumptions and constraints.
Chapter 2 – details the change scope, its impact and associated hazards.
Chapter 3 – contains the argument and sub-arguments in a structured way used to demonstrate that the defined safety criteria are met.
Appendix A - is a compliance matrix between the requirements in regulation 1035/2011, Annex II paragraph 3.2 – "*Safety requirements for risk assessment and mitigation with regard to changes*", and the approach followed in the development of this safety case.
Appendix B - is a compliance matrix between the requirements in regulation 2017/373 requirements, its Accepted Means of Compliance and Guidance Material and the approach followed in the development of this safety case.

The document contains boxes of different colours, the blue ones describe the process followed, the yellow ones refer safety requirements and the green ones include de actions that have already been performed.

1.1 Goals

This safety case presents a structured argument that the upgrade of the Porto Santo radar will be free from unacceptable risk and that actions have been taken to minimize risk as much as possible.
It will cover the safety assessment requirements as defined in regulation (EU) 1035/2011 (ref. [7]) and regulation (EU) 2017/373 (ref. [8]), except for the definition of safety objectives and safety criteria (ATS.OR.210).

The compliance matrixes can be found in Appendix A - Traceability to regulation EU 1035/2011 and Appendix B - Traceability to regulation 2017/373 AMC & GM.

1.2 Scope

This safety assessment shall cover:

- The change associated with the RAPOSA project, i.e. the upgrade of Porto Santo radar including the transition phases and the operational usage;
- The interfaces and interactions between the Porto Santo radar and the remainder of the functional system and its operating context, including airspace procedures.
- The planned degraded modes of operation of the functional system, i.e. the unavailability of the radar during the upgrade works and the evaluation;
- Hazard identification
- The safety criteria (*initial approach*)
- Risk analysis, evaluation and mitigation
- Specification of monitoring criteria

1.3 Assumptions

No changes will be made to the data displayed to ATCO, i.e. no specific mode S information will be provided.

1.4 Constraints

Porto Santo radar is the only surveillance means covering the whole Madeira sector.
Adjacent centres rely on Porto Santo data for their surveillance services.

1.5 Glossary

1.5.1 Acronyms

a/c	Aircraft
ACC	Area Control Centre
ADS-B	Automatic Dependent Surveillance - Broadcast
APP	Approach Control
ASTERIX	All Purpose Structured EUROCONTROL Surveillance Information Exchange A standard data format used for the exchange of surveillance data.
ASO	Avaliação de Segurança Operacional
ATCO	Air Traffic Controller
OSED	Operational Services and Environment Description
SSR	Secondary Surveillance Radar
WAM	Wide Area Multilateration

1.5.2 Definitions

From regulation 1035/2011:

safety assurance	*all planned and systematic actions necessary to provide adequate confidence that a product, a service, an organisation or a functional system achieves acceptable or tolerable safety;*
safety objective	*a qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be expected to occur;*
safety requirement	*a risk-mitigation means, defined from the risk-mitigation strategy that achieves a particular safety objective, including organisational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics;*

From regulation 2017/373:

hazard	*any condition, event, or circumstance which could induce a harmful effect;*
functional system	*a combination of procedures, human resources and equipment, including hardware and software, organised to perform a function within the context of ATM/ANS and other ATM network functions;*

For hazards:

Not provided	Missing or too late.
Incorrect	Data received at destination is wrong. Might be used by destination as correct. It is also incorrect when read back is not detected as wrong.
Corrupted	Data received at destination is: • Not readable, • Not understandable or • Immediately detected as wrong
Misdirected	Is received as an incorrect message by the unintended receiver and is also not provided to the intended destination.

1.6 References

Ref.	Document
[1]	Santos, P. L. C. T., Monteiro, P. A. A., Studic, M., & Majumdar, A. (2017). A methodology used for the development of an Air Traffic Management functional system architecture. (https://doi.org/10.1016/j.ress.2017.05.022)
[2]	2000.R007.482 - ACC Lisboa OSED Version 1.00 from 2013-06-28
[3]	2000.OSED.800 OSED Madeira Tower Version 1.00, 2017-04-03
[4]	9090.R029.030 - ARTAS comparative evaluation without Porto Santo radar Version 1.00 from 2017-07-03
[5]	ASO Operação degradada no sector Madeira (WAM Madeira) Versão 2.0 de 2018-04-05
[6]	ASO - FPL Track - Lisboa FIR Versão 4.0 de 2018-06-07
[7]	COMMISSION IMPLEMENTING REGULATION (EU) 1035/2011 “common requirements for the provision of air navigation services”
[8]	COMMISSION IMPLEMENTING REGULATION (EU) 2017/373 “common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight”
[9]	Safety Case Development Manual (Available at EUROCONTROL)
[10]	IS 079/18/CONLIS de 18-04-18 Reciclagem: ATC-TPC1-LIS e ATC-TPC2-LIS Treino em Procedimentos de Contingência. Prestação de Serviço de Controlo de Tráfego Aéreo em Ambiente de Contingência no Sector Madeira da RIV de Lisboa
[11]	INFO 084/CONLIS/18 AIP AMDT: AIRAC 003-18 e AIP SUP: 032/2018 (ATS Contingency Routes For Madeira Sector Due to Radar Inoperative)

2 Change analysis

Define change steps:
1 – Identify the change scope
2 – Identify change impact
3 – Describe planned degraded modes

This change includes the upgrade of the Porto Santo radar to Mode S and all the adaptations required in the functional system to integrate this source of surveillance data.

Safety assessment steps:
The following steps will be performed for both nominal and planned degraded modes
1 – Determine impact on borders of the functional system
2 – Identify new hazards and assess impact on existing hazards
3 – Identify possible causes; e.g. enabler problem (wrong implementation)
4 – Define mitigations for the identified causes

The change analysis process can be seen as a sequence of activities as depicted in the following image:

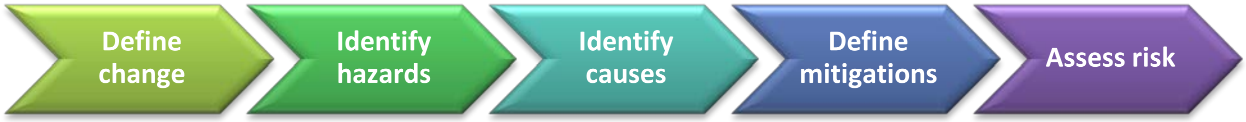

Figure 1: Change assessment process

The analysis is supported by the use of the ATM model MARIA. The model is used as a checklist to help the analyst identify the change scope and its impact in the ATM functional system. The development of this model started in 2012 and has already involved over 100 people in its development and validation. Every time it is used conveys an additional validation activity and an opportunity for improvement. Its hierarchical structure allows experts to focus on their area of expertise, ignoring the global view which is already captured in the model.
Below is a brief description of the model used in this analysis, using information from [1], which should be consulted for more in depth information on this ATM model.

The Air Traffic Management (ATM) system provides a safe, economical, efficient, dynamic and integrated management of air traffic and airspace through the collaborative integration of humans, infrastructure (technology and facilities) and organisations. At present, it is widely accepted that the ATM system is one of the leading complex socio-technical systems in terms safety performance. The Model of ATM used was developed with the aim of providing a sound base for system analysis, including safety, namely by describing the whole system and the interdependencies between its functions. It was developed using a hybrid methodology that integrates two well-known methods for qualitative data analysis – Template Analysis, and for functional modelling – Structured Analysis and Design Technique (SADT). Template Analysis was used to analyse the collected qualitative data that was further organised using the SADT, into the ATM functional system architecture.
The scope of MARIA, defined prior to the study, was to comprise all the ATM functions under the responsibility of the ANSP as illustrated in Figure 2: ATM Model scope. These include all the functions necessary to ensure a continuous, safe, efficient and cost-effective ATM services, by all the airspace sectors, to all the aircraft. Therefore, all of the services that are not within the responsibility of NAV Portugal (i.e. inputs and outputs originating from an aircraft or an external organisation such as the International Civil Aviation Organisation (ICAO), EUROCONTROL or other ANSPs) are out of the scope and belong to the model's exterior.

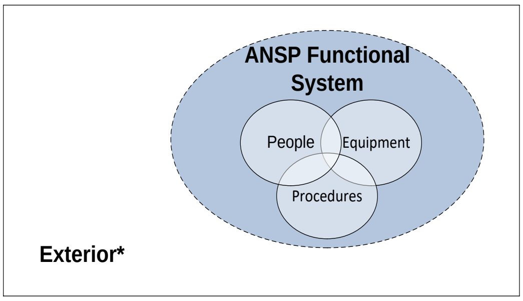

Figure 2: ATM Model scope

The high level view of the ATM model is depicted in Figure 3: ATM Model high-level functions . It comprises 9 functions supported by a 10th function which covers all that is needed to maintain the service provision infrastructure including, among others, the management of human resources, defining procedures, maintaining and replacing equipment.

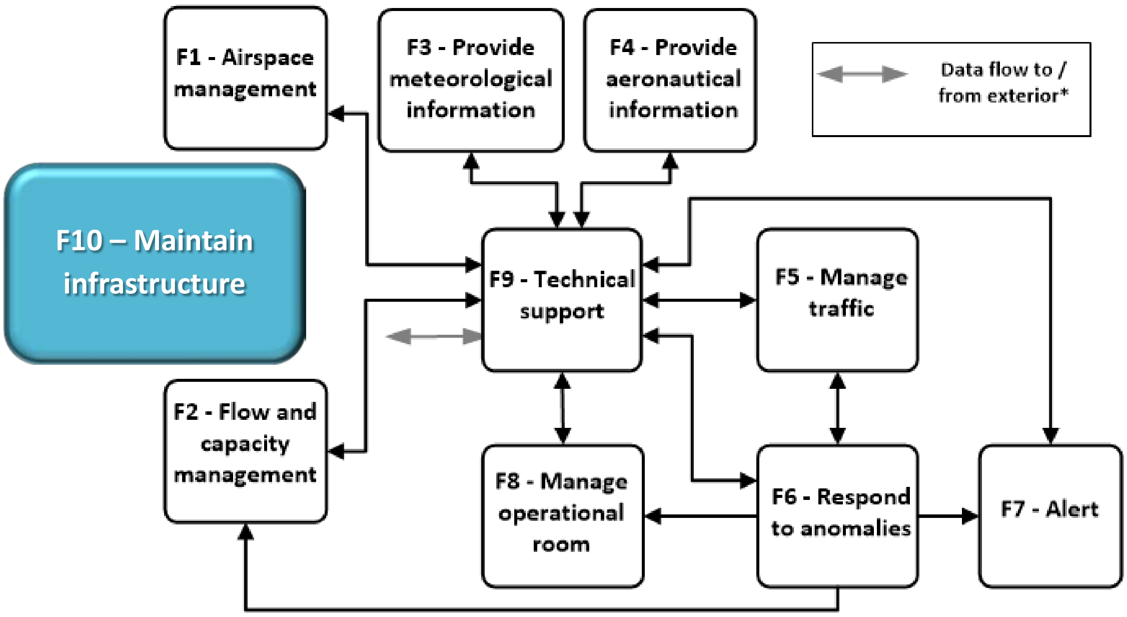
F1 - Airspace management
F3 - Provide meteorological information
F4 - Provide aeronautical information
Data flow to / from exterior*
F10 – Maintain infrastructure
F9 - Technical support
F5 - Manage traffic
F2 - Flow and capacity management
F8 - Manage operational room
F6 - Respond to anomalies
F7 - Alert

Figure 3: ATM Model high-level functions

MARIA attempts to provide a system description, covering people, procedures, equipment, regulation and the external environment. It describes both the system functions and the architecture with all its mechanisms of the Lisbon Flight Information Region (FIR). However, following the processes of internal and external validation it can be stated that this functional model can be extended to a generic ATM system with small adaptations, requiring the system architecture to be adapted to local systems, human tasks and their organization.

Due to the complexity of the system, both top-down and bottom-up coding was carried out with the aim of developing a comprehensive ATM system architecture. Initially, a top-down approach was used to derive a functional system description. During the interviews, the details were captured and added to the top-level structure using a bottom-up approach.

In light of the information flows gathered through the interviews, functions and their couplings were further combined, divided, modified, refined and amended. Hierarchical relationships that explain functional substructures and couplings between the functions were established. For instance, during this process, an additional top-level function was created, function F-10 Maintain Infrastructure. The new function was deemed necessary to account for the support of the remaining nine functions (belonging to the top-level of the MARIA model hierarchy) in the provision and maintenance of required infrastructural resources (e.g. to keep all the internal documentation up to date).

Due to the complexity of the MARIA model in the SADT format, it was deemed necessary to code it into an electronic readable language for the purpose of assuring its consistency and completeness. The MARIA framework offers the following automated functionalities: loading, checking, filtering, and documentation production. The automatic generation of documentation creates graphics, web pages in html format, and open document format. The figures used in this document to represent the functions are extracted from the html model's representation.

2.1 Change scope

Identify the change scope:

The MARIA model covers the whole scope of NAV Portugal ANS and ATM services and can be considered complete at each level of detail. Each NAV Portugal unit has its own model instance.
To ensure that the scope of the change is completely and correctly identified, it is described by pin-pointing the elements of the MARIA model for NAV Portugal that are changed.

The next step is to identify all the units that are affected by the change. This is done by checking the presence of the changed elements in the different unit model instances. In addition expert judgement is used to complement and validate the results.
The impact on the specific units is made explicit and covered in the global assessment.

2.1.1 Changed components

Conventions:

- Orange arrows identify impacted elements
- Orange boxes mark affected functions
- Purple boxes identify impacts to elements outside the functional system
- Red arrows identify potential degraded modes

The scope of this change is F-9.4.2.1: Sensor & Local Tracking, enabler Radar Porto Santo.

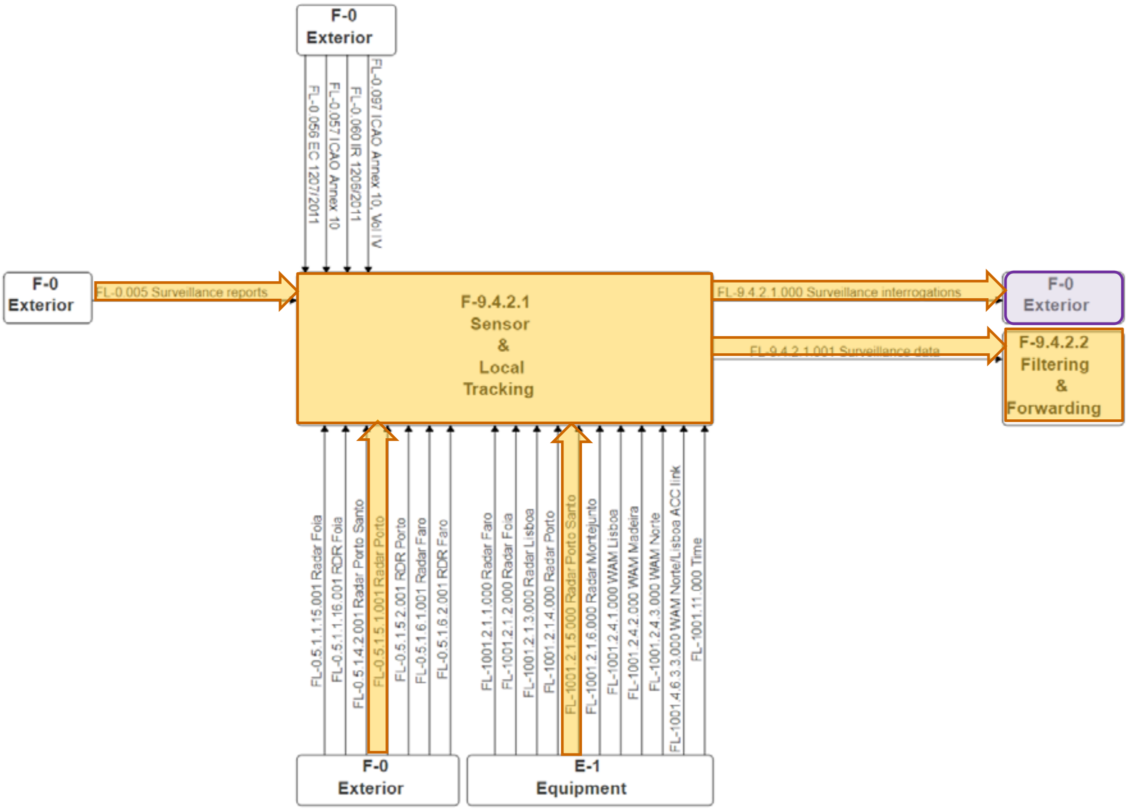
F-0
Exterior
FL-0.056 EC 1207/2011
FL-0.057 ICAO Annex 10
FL-0.060 IR 1206/2011
FL-0.097 ICAO Annex 10, Vol IV
F-0
Exterior
FL-0.005 Surveillance reports
F-9.4.2.1
Sensor
&
Local
Tracking
FL-9.4.2.1.000 Surveillance interrogations
F-0
Exterior
FL-9.4.2.1.001 Surveillance data
F-9.4.2.2
Filtering
&
Forwarding
FL-0.5.1.1.15.001 Radar Foia
FL-0.5.1.1.16.001 RDR Foia
FL-0.5.1.4.2.001 Radar Porto Santo
FL-0.5.1.5.1.001 Radar Porto
FL-0.5.1.5.2.001 RDR Porto
FL-0.5.1.6.1.001 Radar Faro
FL-0.5.1.6.2.001 RDR Faro
FL-1001.2.1.1.000 Radar Faro
FL-1001.2.1.2.000 Radar Foia
FL-1001.2.1.3.000 Radar Lisboa
FL-1001.2.1.4.000 Radar Porto
FL-1001.2.1.5.000 Radar Porto Santo
FL-1001.2.1.6.000 Radar Montejunto
FL-1001.2.4.1.000 WAM Lisboa
FL-1001.2.4.2.000 WAM Madeira
FL-1001.2.4.3.000 WAM Norte
FL-1001.4.6.3.3.000 WAM Norte/Lisboa ACC link
FL-1001.11.000 Time
F-0
Exterior
E-1
Equipment

Figure 4: Scope of the change

The use of Mode S interrogations will affect the outputs of this function to Exterior – the aircraft and the inputs from the aircraft which will now respond with Mode S replies, if capable.

Note: The changes to the ATM systems, although addressed in this safety case, are outside the scope of the RAPOSA project.

2.1.2 Affected units

The Porto Santo radar is an enabler of the function F-9.4.2: Ensure Air Surveillance in the following units:

- Lisboa ACC
- Madeira Tower
- Santa Maria ACC

It is also used by the following adjacent ANSPs: ENAIRE and ONDA.

Except for the Madeira Tower, where it is used for approach control, the information from Porto Santo radar is used to provide surveillance service for en-route control. The separation minima applied is 8NM in the Madeira sector and TMA.
In the areas under the responsibility of NAV Portugal the traffic density is low.

The geographical area affected is represented in the following picture:

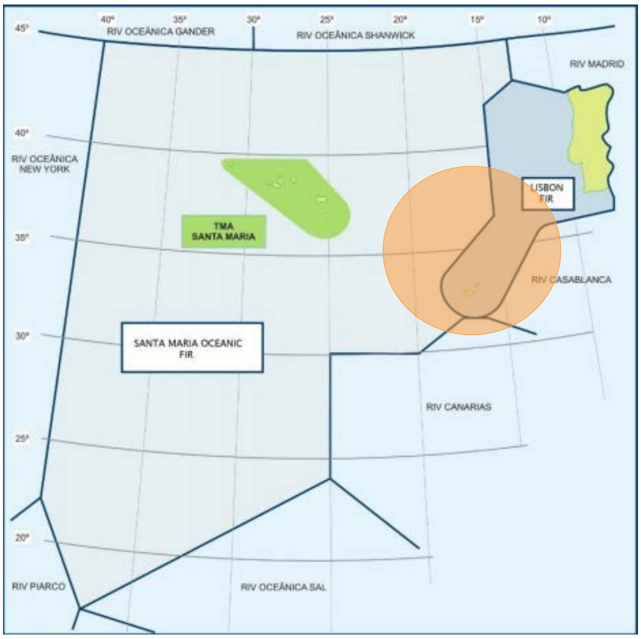

Figure 5: Affected areas

As the maintenance of Porto Santo radar is ensured by the team from Porto Santo tower, this unit will also be impacted. Training on the new radar is required for the Porto Santo maintenance team.

R1. The new Porto Santo maintenance team shall be trained to maintain the new radar.

2.1.3 Affected interfaces and interactions

Identify change impact:
The change impact is assessed using the MARIA model as a representation of the existing functional system. The following approach is followed:
1. One by one, select each output marked as affected in the scope identification;
2. If the output is to exterior assess the impact on the external elements, e.g. aircraft or adjacent units.

3. Iteratively follow the flow of information through the impacted functions until it can be demonstrated or assumed that the output of the function under analysis is not changed;
4. Continue until all flows have been traced to the end, either inside the NAV Portugal or to the exterior.
5. Assess the change impact on all the traversed, i.e. impacted, functions.
6. If the output of the function under analysis is not changed, assess the possible degraded modes.

2.1.3.1 F-9.4.2.1: Sensor & Local Tracking

The change to F-9.4.2.1: Sensor & Local Tracking consists of:

- Replacement of the radar antenna and its processing units

The change to F-9.4.2.1: Sensor & Local Tracking will directly impact:

- Exterior - Aircraft
- F-9.4.2.2: Filtering & Forwarding

Interface: F-9.4.2.1: Sensor & Local Tracking to exterior

The use of Mode S interrogations will affect the outputs of this function to Exterior – the aircraft, and the inputs from the aircraft which will now respond with Mode S replies, if capable.

R2. The new Porto Santo radar shall detect cooperative non Mode S equipped aircraft.

The Mode S ground interrogator provides surveillance of both Mode A/C and Mode S equipped aircraft, with minimal mutual interference. The 1030 MHz interrogation channel is divided into distinct and non-overlapping periods of Mode A/C and Mode S activity, known as the 'all-call' period and Mode S selective interrogation activity, known as the 'roll-call' period.
Interrogations during the all-call period elicit replies from Mode A/C aircraft and acquire Mode S aircraft via acquisition of the 24-bit ICAO aircraft address.

2.1.3.2 F-9.4.2.2: Filtering & Forwarding

The change to F-9.4.2.2: Filtering & Forwarding implies:

- Configuration of the enabler SDDS-NG as the system is already capable of processing mode S data.

Note: ARTAS and SDDS-NG are already processing ASTERIX cat 34/48 from other radars.

The change to F-9.4.2.2: Filtering & Forwarding will directly impact:

- F-9.1 : Ensure Communications
  - F-9.1.2: Ensure Ground/Ground Communications
  - F-9.1.2.4: Ensure Surveillance Messages
  - ➢ F-9.1.2.4.3: Distribution Surveillance Messages -> Adjacent centres
- ➢ F-9.4.2.3: Tracking
- F-9.5: Automatic Traffic Monitoring
  - ➢ F-9.5.2: Automatic Air Traffic Monitoring
- F-9.9: Data Integration
  - ➢ F-9.9.2: Air Coupler
- F-9.10: Presentation Support
  - F-9.10.1: Surveillance Presentation
  - ➢ F-9.10.1.1: Air Surveillance Presentation

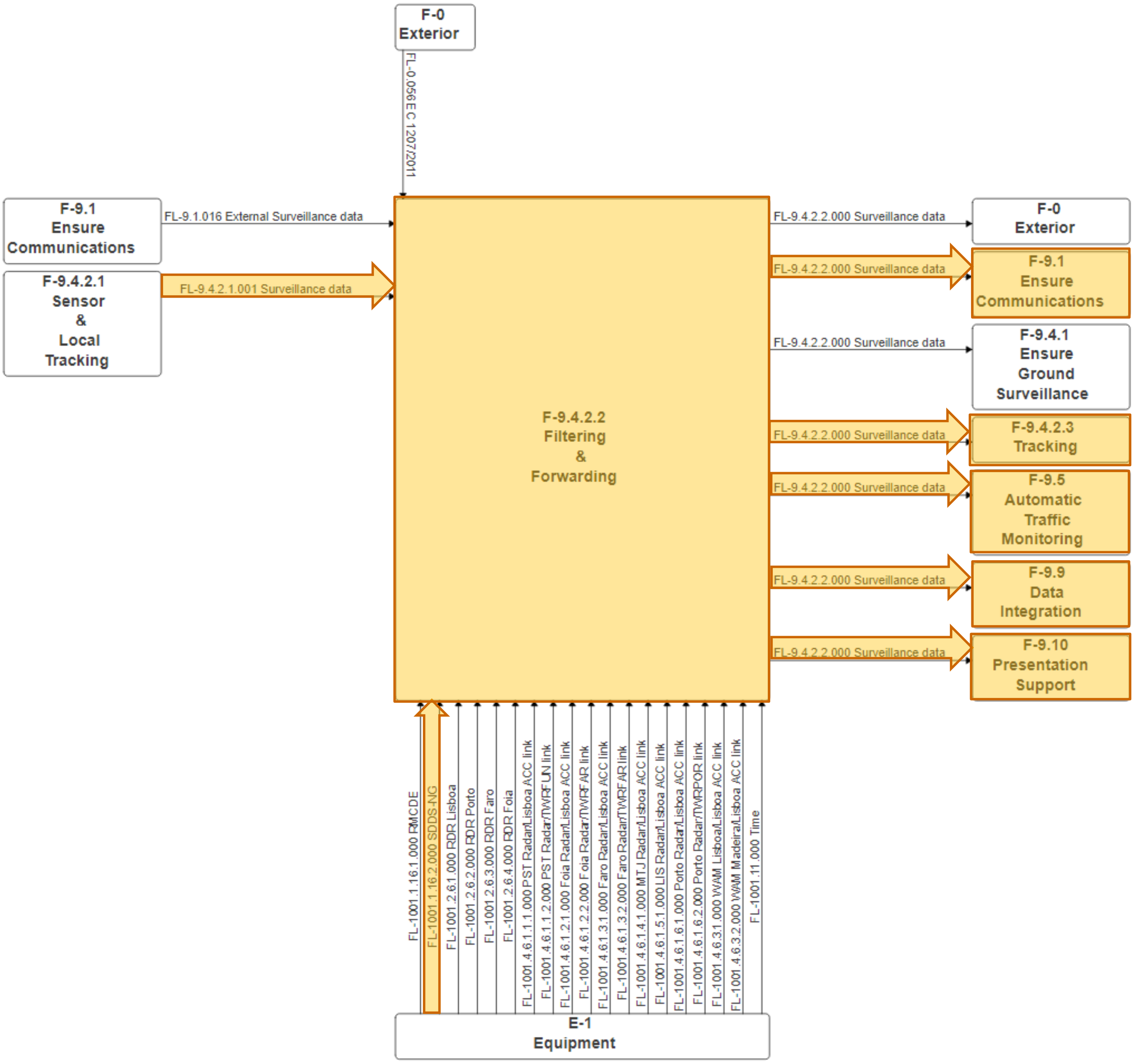
F-0
Exterior
FL-0.056 EC 1207/2011
F-9.1
Ensure
Communications
FL-9.1.016 External Surveillance data
F-9.4.2.1
Sensor
&
Local
Tracking
FL-9.4.2.1.001 Surveillance data
F-9.4.2.2
Filtering
&
Forwarding
FL-9.4.2.2.000 Surveillance data
F-0
Exterior
FL-9.4.2.2.000 Surveillance data
F-9.1
Ensure
Communications
FL-9.4.2.2.000 Surveillance data
F-9.4.1
Ensure
Ground
Surveillance
FL-9.4.2.2.000 Surveillance data
F-9.4.2.3
Tracking
FL-9.4.2.2.000 Surveillance data
F-9.5
Automatic
Traffic
Monitoring
FL-9.4.2.2.000 Surveillance data
F-9.9
Data
Integration
FL-9.4.2.2.000 Surveillance data
F-9.10
Presentation
Support
FL-1001.1.16.1.000 RMCDE
FL-1001.1.16.2.000 SDDS-NG
FL-1001.2.6.1.000 RDR Lisboa
FL-1001.2.6.2.000 RDR Porto
FL-1001.2.6.3.000 RDR Faro
FL-1001.2.6.4.000 RDR Foia
FL-1001.4.6.1.1.1.000 PST Radar/Lisboa ACC link
FL-1001.4.6.1.1.2.000 PST Radar/TWRFUN link
FL-1001.4.6.1.2.1.000 Foia Radar/Lisboa ACC link
FL-1001.4.6.1.2.2.000 Foia Radar/TWRFAR link
FL-1001.4.6.1.3.1.000 Faro Radar/Lisboa ACC link
FL-1001.4.6.1.3.2.000 Faro Radar/TWRFAR link
FL-1001.4.6.1.4.1.000 MTJ Radar/Lisboa ACC link
FL-1001.4.6.1.5.1.000 LIS Radar/Lisboa ACC link
FL-1001.4.6.1.6.1.000 Porto Radar/Lisboa ACC link
FL-1001.4.6.1.6.2.000 Porto Radar/TWRPOR link
FL-1001.4.6.3.1.000 WAM Lisboa/Lisboa ACC link
FL-1001.4.6.3.2.000 WAM Madeira/Lisboa ACC link
FL-1001.11.000 Time
E-1
Equipment

Figure 6: Impact on F-9.4.2.2: Filtering & Forwarding

2.1.3.3 F-9.1.2.4.3: Distribution Surveillance Messages

Adjacent centres will receive Porto Santo radar data in a new format. The format used is standard (ASTERIX category 34/48) and the client systems are able to process it.

As mitigation, the new Porto Santo radar can provide data in ASTERIX category 01/02, similar to the previous radar. Using this data flow will avoid the need to adapt systems in the adjacent centres for the transition.

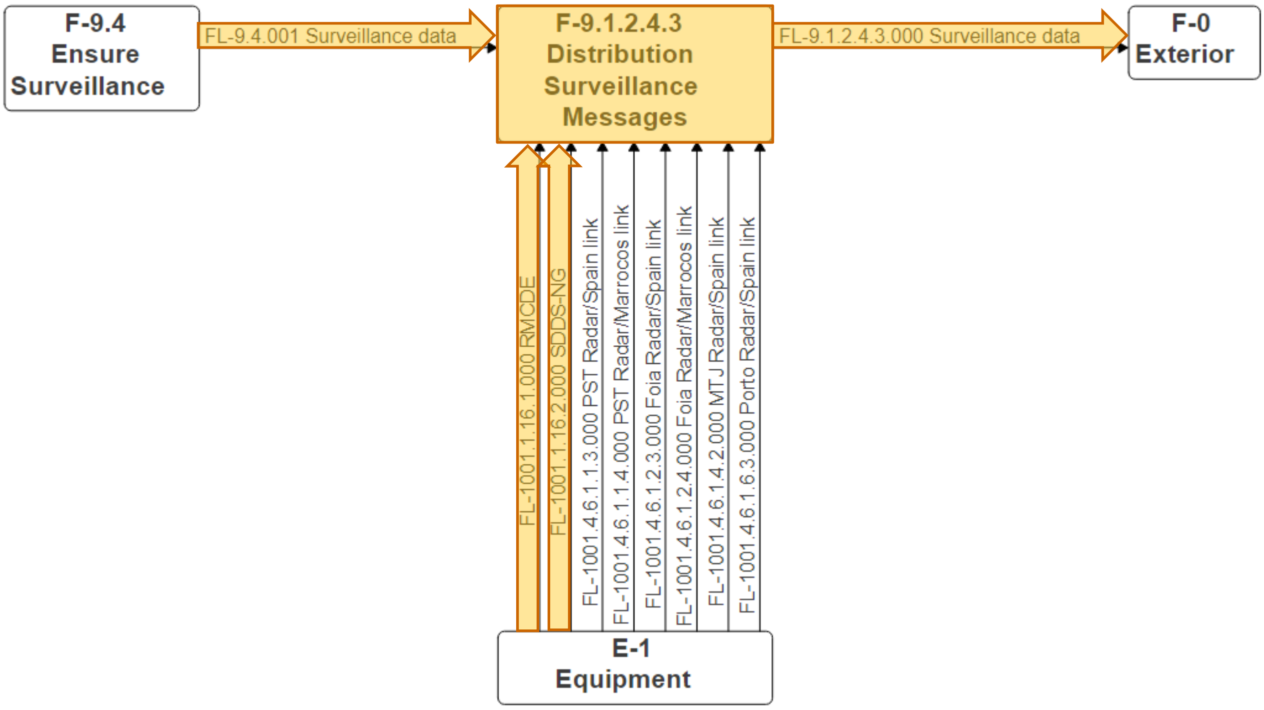
F-9.4
Ensure
Surveillance
FL-9.4.001 Surveillance data
F-9.1.2.4.3
Distribution
Surveillance
Messages
FL-9.1.2.4.3.000 Surveillance data
F-0
Exterior
FL-1001.1.16.1.000 RMCDE
FL-1001.1.16.2.000 SDDS-NG
FL-1001.4.6.1.1.3.000 PST Radar/Spain link
FL-1001.4.6.1.1.4.000 PST Radar/Marrocos link
FL-1001.4.6.1.2.3.000 Foia Radar/Spain link
FL-1001.4.6.1.2.4.000 Foia Radar/Marrocos link
FL-1001.4.6.1.4.2.000 MTJ Radar/Spain link
FL-1001.4.6.1.6.3.000 Porto Radar/Spain link
E-1
Equipment

Figure 7: Impact on F-9.1.2.4.3: Distribution Surveillance Messages

R3. External partners (ONDA & ENAIRE) shall be informed of the change in the data format.

The RADAR will use ASTERIX Category 34/48, to be able to output the Mode-S information extracted from the transponder. However it is still able to output ASTERIX category 1, 2 in case the “client” is unable to process category 34/48.
Morocco and Spain were informed via the AEFMP.

2.1.3.4 F-9.4.2.3: Tracking

The change to F-9.4.2.3: Tracking implies the configuration of the enabler ARTAS main and ARTAS fallback to correctly process the new Porto Santo radar data. As these systems are already capable of processing ASTERIX category 34/48, mode S data, no additional changes are required.

The change to F-9.4.2.3: Tracking will stop the propagation of the impact further. Outputs will keep the current performance, format and contents (see 1.3 - Assumptions).

R4. Verify that the Tracking outputs from ARTAS are identical to the current operational ones.

In terms of degraded modes, if the function is not adapted correctly or fails, the flow Integrated Surveillance data could become totally or partially unavailable, corrupt or incorrect. Degraded modes are addressed in paragraph 2.1.5.

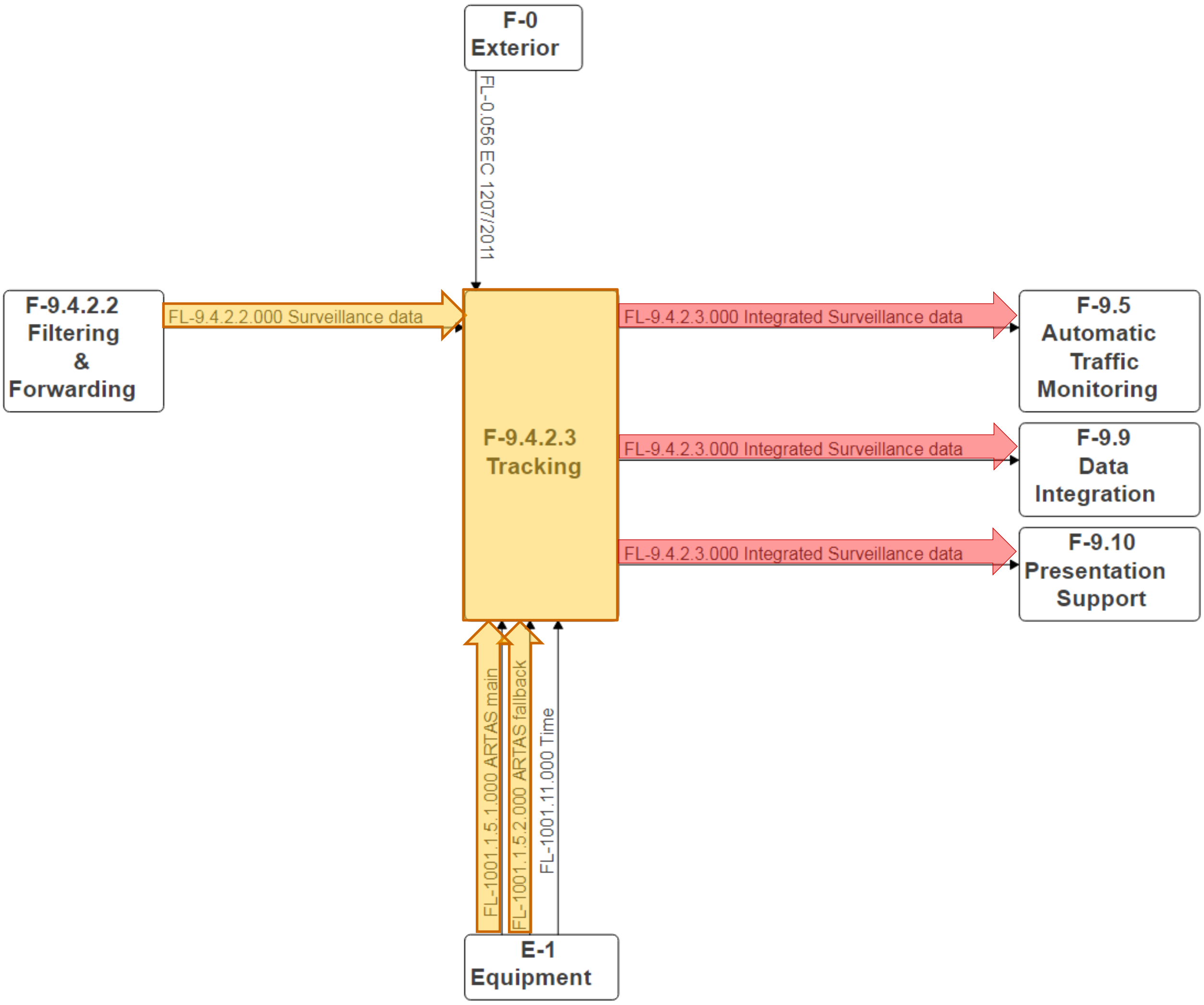
F-0
Exterior
FL-0.056 EC 1207/2011
F-9.4.2.2
Filtering
&
Forwarding
FL-9.4.2.2.000 Surveillance data
F-9.4.2.3
Tracking
FL-9.4.2.3.000 Integrated Surveillance data
F-9.5
Automatic
Traffic
Monitoring
FL-9.4.2.3.000 Integrated Surveillance data
F-9.9
Data
Integration
FL-9.4.2.3.000 Integrated Surveillance data
F-9.10
Presentation
Support
FL-1001.1.5.1.000 ARTAS main
FL-1001.1.5.2.000 ARTAS fallback
FL-1001.11.000 Time
E-1
Equipment

Figure 8: Impact on F-9.4.2.3: Tracking

2.1.3.5 F-9.5.2: Automatic Air Traffic Monitoring

The change to F-9.5.2: Automatic Air Traffic Monitoring implies changing the enablers' software to process ASTERIX cat 34/48, Mode S data. The change will have to be performed to the enablers:

- ATSS Lisboa
- ATSS Funchal

As mitigation, in case these enablers are not changed in due time, the new Porto Santo radar will also be able to provide data in ASTERIX category 01/02, similar to the previous radar. Using this data flow will avoid the need to adapt this function and remove the identified degraded modes.

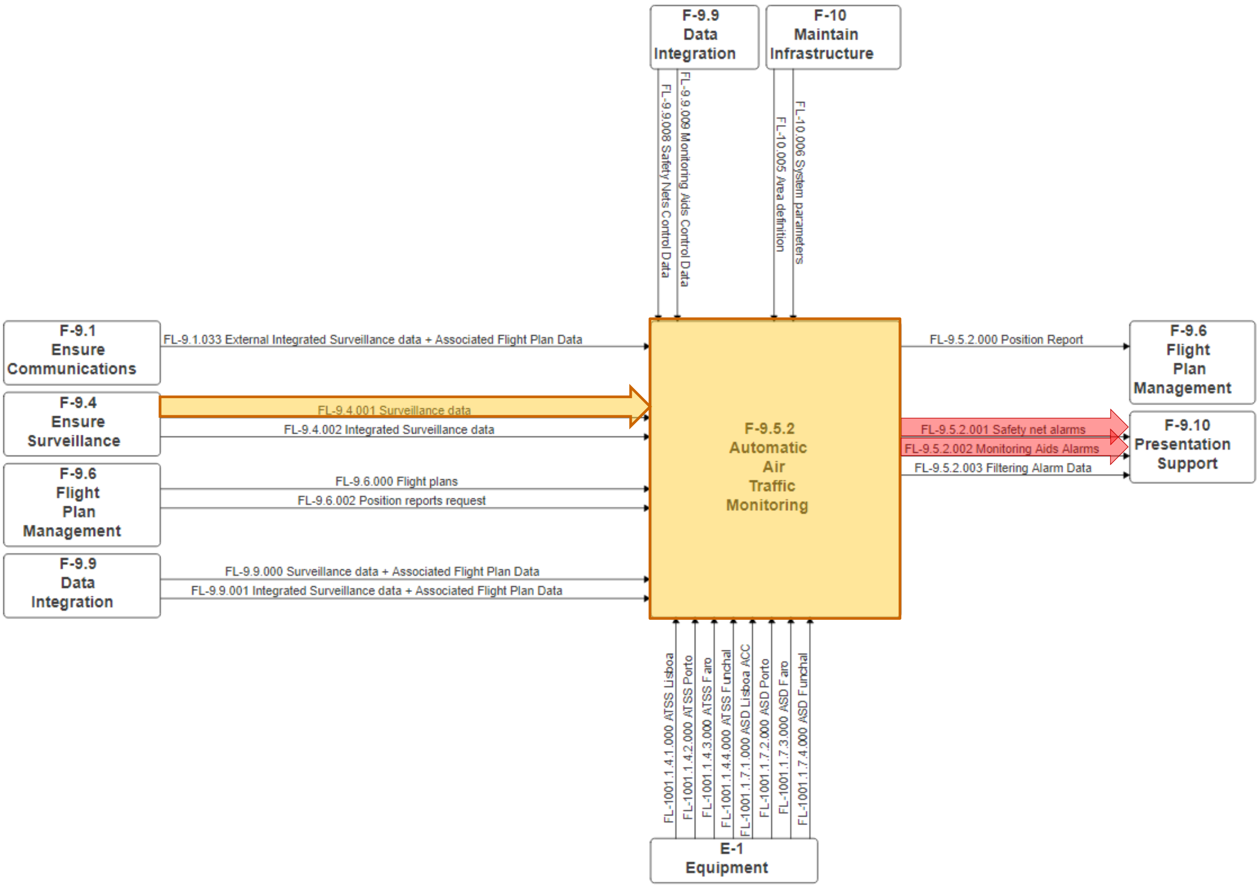
F-9.9
Data
Integration
F-10
Maintain
Infrastructure
FL-9.9.008 Safety Nets Control Data
FL-9.9.009 Monitoring Aids Control Data
FL-10.005 Area definition
FL-10.006 System parameters
F-9.1
Ensure
Communications
FL-9.1.033 External Integrated Surveillance data + Associated Flight Plan Data
F-9.4
Ensure
Surveillance
FL-9.4.001 Surveillance data
FL-9.4.002 Integrated Surveillance data
F-9.6
Flight
Plan
Management
FL-9.6.000 Flight plans
FL-9.6.002 Position reports request
F-9.9
Data
Integration
FL-9.9.000 Surveillance data + Associated Flight Plan Data
FL-9.9.001 Integrated Surveillance data + Associated Flight Plan Data
F-9.5.2
Automatic
Air
Traffic
Monitoring
FL-9.5.2.000 Position Report
F-9.6
Flight
Plan
Management
FL-9.5.2.001 Safety net alarms
FL-9.5.2.002 Monitoring Aids Alarms
FL-9.5.2.003 Filtering Alarm Data
F-9.10
Presentation
Support
FL-1001.1.4.1.000 ATSS Lisboa
FL-1001.1.4.2.000 ATSS Porto
FL-1001.1.4.3.000 ATSS Faro
FL-1001.1.4.4.000 ATSS Funchal
FL-1001.1.7.1.000 ASD Lisboa ACC
FL-1001.1.7.2.000 ASD Porto
FL-1001.1.7.3.000 ASD Faro
FL-1001.1.7.4.000 ASD Funchal
E-1
Equipment

Figure 9: Impact on F-9.5.2: Automatic Air Traffic Monitoring

The change to F-9.5.2: Automatic Air Traffic Monitoring will have no impact as the outputs will keep the current format and contents.

R5. Verify that the Automatic Air Traffic Monitoring outputs are not changed.

In terms of degraded modes, if the function is not adapted correctly or fails the flows Safety net alarms and Monitoring Aids Alarms could become totally or partially unavailable, corrupt or incorrect.

Additionally, if the Automatic Air Traffic Monitoring enablers are not changed, the impact is that there will be limitations on the flows Safety net alarms and Monitoring Aids Alarms for the Porto Santo radar flow.

2.1.3.6 F-9.9.2: Air Coupler

The change to F-9.9.2: Air Coupler implies changing the enablers' software to process ASTERIX cat 34/48, Mode S data. The change will have to be performed to the enablers:

- ATSS Lisboa
- ATSS Funchal

As mitigation, in case these enablers are not changed in due time, the new Porto Santo radar will also be able to provide data in ASTERIX category 01/02, similar to the previous radar. Using this data flow will avoid the need to adapt this function and remove the identified degraded modes.

The change to 9.9.2: Air Coupler will have no impact as the outputs will keep the current format and contents.

R6. Verify that the Air Coupler outputs are not changed.

In terms of degraded modes, if the function is not adapted correctly or fails the flows Surveillance data + Associated Flight Plan Data and Integrated Surveillance data + Associated Flight Plan Data could become totally or partially unavailable, corrupt or incorrect.

Additionally, if the Air Coupler enablers are not changed, the impact is that there will be limitations on the flow FL-9.9.2.000 Surveillance data + Associated Flight Plan Data. The data from Porto Santo radar will not be available as mono sensor flow associated with flight plan information, i.e. it will not be selectable for presentation and Automatic Traffic Monitoring will also not be performed on this flow.

R7. Verify that Air Coupler enablers are capable of processing Mode S radar data.

Degraded modes are addressed in paragraph 2.1.5.

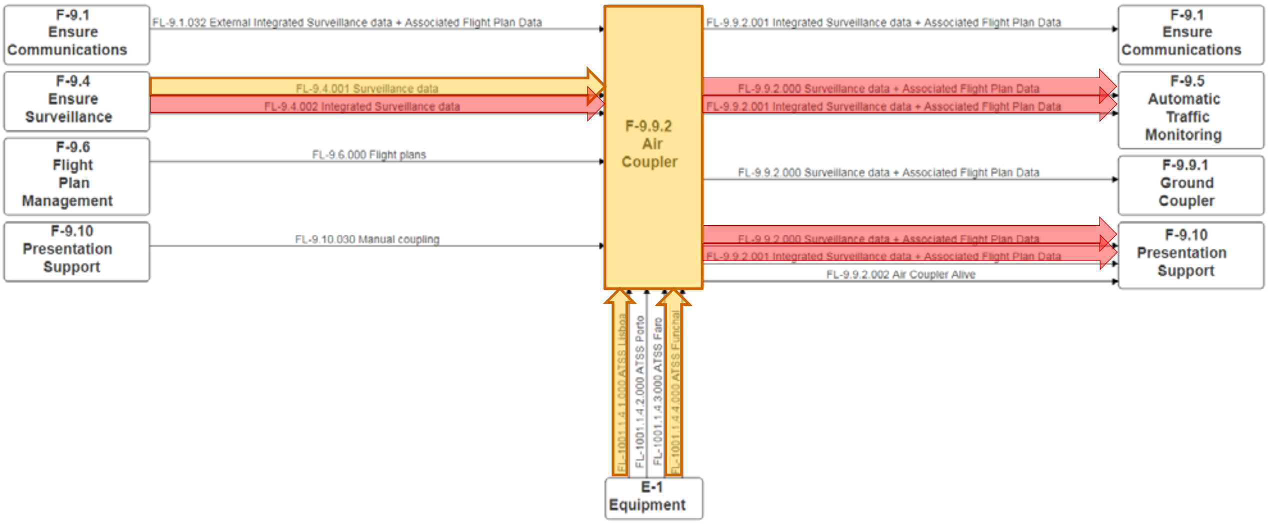
F-9.1
Ensure
Communications
FL-9.1.032 External Integrated Surveillance data + Associated Flight Plan Data
F-9.4
Ensure
Surveillance
FL-9.4.001 Surveillance data
FL-9.4.002 Integrated Surveillance data
F-9.6
Flight
Plan
Management
FL-9.6.000 Flight plans
F-9.10
Presentation
Support
FL-9.10.030 Manual coupling
F-9.9.2
Air
Coupler
FL-9.9.2.001 Integrated Surveillance data + Associated Flight Plan Data
F-9.1
Ensure
Communications
FL-9.9.2.000 Surveillance data + Associated Flight Plan Data
FL-9.9.2.001 Integrated Surveillance data + Associated Flight Plan Data
F-9.5
Automatic
Traffic
Monitoring
FL-9.9.2.000 Surveillance data + Associated Flight Plan Data
F-9.9.1
Ground
Coupler
FL-9.9.2.000 Surveillance data + Associated Flight Plan Data
FL-9.9.2.001 Integrated Surveillance data + Associated Flight Plan Data
FL-9.9.2.002 Air Coupler Alive
F-9.10
Presentation
Support
FL-1001.1.4.1.000 ATSS Lisboa
FL-1001.1.4.2.000 ATSS Porto
FL-1001.1.4.3.000 ATSS Faro
FL-1001.1.4.4.000 ATSS Funchal
E-1
Equipment

Figure 10: Impact on F-9.9.2: Air Coupler

2.1.3.7 F-9.10.1.1: Air Surveillance Presentation

The change F-9.10.1.1: Air Surveillance Presentation implies changing the enablers' software to process ASTERIX cat 34/48, Mode S data. The change will have to be performed to the enablers:

- ASD Lisboa
- ASD Funchal

As mitigation, the new Porto Santo radar can provide data in ASTERIX category 01/02, similar to the previous radar. Using this data flow will avoid the need to adapt this function.

The change to F-9.10.1.1: Air Surveillance Presentation will have no impact as the outputs will keep the current format and contents (see 1.3 - Assumptions).

R8. Verify that the Surveillance views are not changed, e.g. no Mode S specific data is displayed.

In terms of degraded modes, if the function is not adapted correctly or fails the flows Surveillance views could become totally or partially unavailable, corrupt or incorrect.

Additionally, if the Air Surveillance Presentation enablers are not changed, the impact is that there will limitations on the flow FL-9.10.1.1.003 Surveillance views. The data from Porto Santo radar will not be available as non-correlated mono sensor flow, i.e. it will not be selectable for presentation.

R9. Verify that Air Surveillance Presentation enablers are capable of displaying Mode S radar data.

Degraded modes are addressed in paragraph 2.1.5.

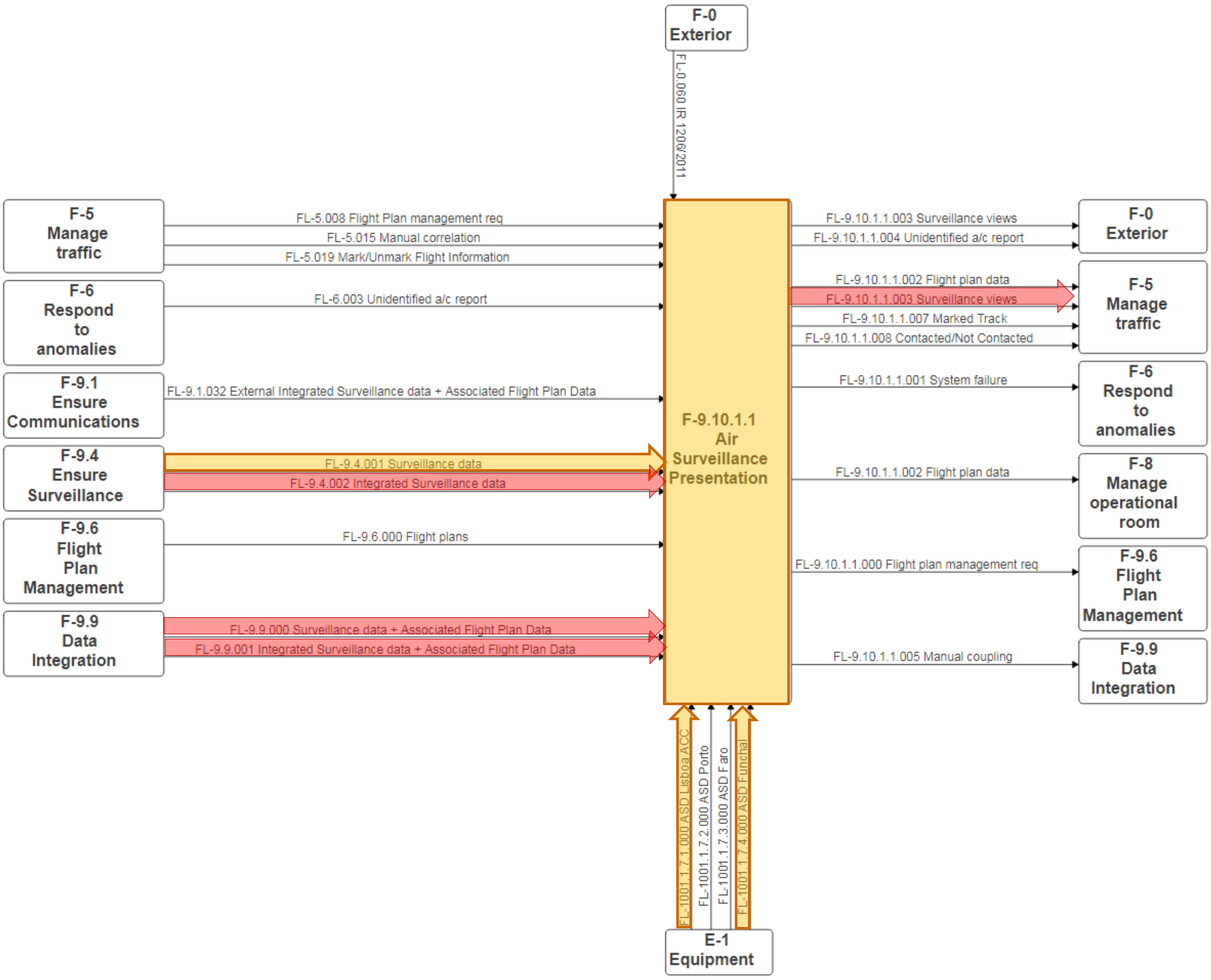
F-0 Exterior
FL-0.060 IR 1206/2011
F-5 Manage traffic
FL-5.008 Flight Plan management req
FL-5.015 Manual correlation
FL-5.019 Mark/Unmark Flight Information
F-6 Respond to anomalies
FL-6.003 Unidentified a/c report
F-9.1 Ensure Communications
FL-9.1.032 External Integrated Surveillance data + Associated Flight Plan Data
F-9.4 Ensure Surveillance
FL-9.4.001 Surveillance data
FL-9.4.002 Integrated Surveillance data
F-9.6 Flight Plan Management
FL-9.6.000 Flight plans
F-9.9 Data Integration
FL-9.9.000 Surveillance data + Associated Flight Plan Data
FL-9.9.001 Integrated Surveillance data + Associated Flight Plan Data
F-9.10.1.1 Air Surveillance Presentation
FL-9.10.1.1.003 Surveillance views
FL-9.10.1.1.004 Unidentified a/c report
F-0 Exterior
FL-9.10.1.1.002 Flight plan data
FL-9.10.1.1.003 Surveillance views
FL-9.10.1.1.007 Marked Track
FL-9.10.1.1.008 Contacted/Not Contacted
F-5 Manage traffic
FL-9.10.1.1.001 System failure
F-6 Respond to anomalies
FL-9.10.1.1.002 Flight plan data
F-8 Manage operational room
FL-9.10.1.1.000 Flight plan management req
F-9.6 Flight Plan Management
FL-9.10.1.1.005 Manual coupling
F-9.9 Data Integration
FL-1001.1.7.1.000 ASD Lisboa ACC
FL-1001.1.7.2.000 ASD Porto
FL-1001.1.7.3.000 ASD Faro
FL-1001.1.7.4.000 ASD Funchal
E-1 Equipment

Figure 11: Impact on F-9.10.1.1: Air Surveillance Presentation

Note: The Surveillance views flow to Exterior is not impacted as the mono sensor views are not provided.

2.1.4 Change impact - Required adaptations

This paragraph summarizes all the required additional adaptations.

For this change, namely the upgrade to Mode S and the use of a new ASTERIX category, the following functions will also need to be changed:

- F-9.1.2.4.3: Distribution Surveillance Messages
- F-9.4.2.2: Filtering & Forwarding
- F-9.4.2.3: Tracking
- F-9.5.2: Automatic Air Traffic Monitoring
- F-9.9.2: Air Coupler
- F-9.10.1.1: Air Surveillance Presentation

2.1.5 Planned degraded modes

Analyse planned degraded modes:

1. Identify degraded modes and represent them using the model functions at the highest level of abstraction possible.

2. For each degraded mode, determine its impact (apply process described in 2.1.3)

3. Identify hazards
   - Check all outputs to Exterior that might be impacted
     - For all impacted outputs, check existing hazards
     - For all new outputs identify possible new hazards
   - Check all outputs to Ensure communications that might be impacted
     - For all impacted outputs, check existing hazards
     - For all new outputs that are forwarded to Exterior identify possible new hazards
   - Check all outputs to non-technical functions that might be impacted
     - For all changed or new ones perform an Operational Safety Assessment

4 – Identify possible causes; e.g. enabler problem (wrong implementation)
   - For all impacted functions, identify what can go wrong

5 – Define mitigations for the identified causes using one or more of the following strategies:
   - Avoidance – Stop the propagation of the problem in the functional system
   - Reduction or control – Reduce the probability or the impact of the problem
   - Acceptance – Acknowledge and then define ways to handle the problem

Some elements require a geographical analysis, which is performed via an Operational Safety Assessment, covered in other documents and referenced here.

The following planned degraded modes are identified:

- Problems with surveillance data – radar unavailable:
  - No data from Porto Santo radar

2.1.5.1 F-9.4.2: Ensure Air Surveillance

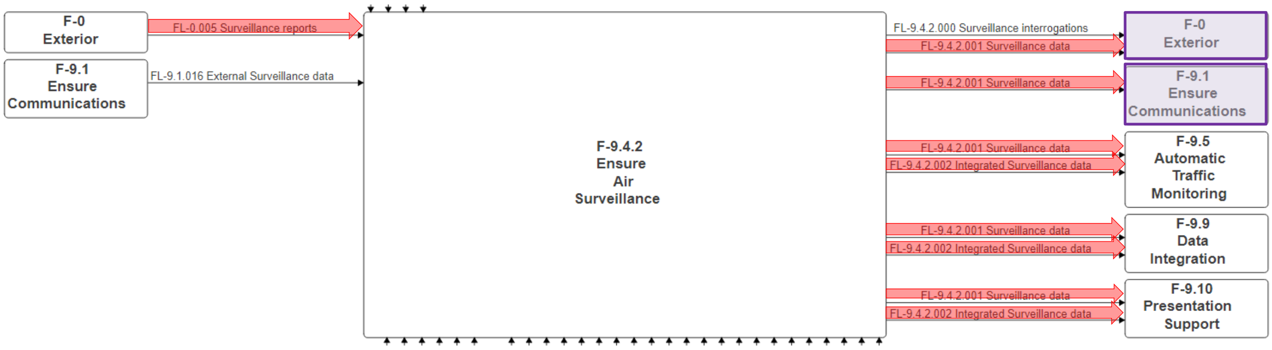
F-0
Exterior
FL-0.005 Surveillance reports
F-9.1
Ensure
Communications
FL-9.1.016 External Surveillance data
F-9.4.2
Ensure
Air
Surveillance
FL-9.4.2.000 Surveillance interrogations
FL-9.4.2.001 Surveillance data
F-0
Exterior
FL-9.4.2.001 Surveillance data
F-9.1
Ensure
Communications
FL-9.4.2.001 Surveillance data
FL-9.4.2.002 Integrated Surveillance data
F-9.5
Automatic
Traffic
Monitoring
FL-9.4.2.001 Surveillance data
FL-9.4.2.002 Integrated Surveillance data
F-9.9
Data
Integration
FL-9.4.2.001 Surveillance data
FL-9.4.2.002 Integrated Surveillance data
F-9.10
Presentation
Support

Figure 12: Planned degraded modes: Impact on F-9.4.2: Ensure Air Surveillance

Adjacent centres will not receive data from Porto Santo radar which might impact their surveillance service. To minimize the impact the following actions were defined:

- Inform Spain, Morocco and Santa Maria about the Porto Santo outage
- Propose alternative surveillance means

R10. Ensure that the adjacent centres are informed well in advance of Porto Santo outage.

The adjacent centres have been informed via several means about this outage, both in bilateral contacts and at the AEFMP group meetings.

R11. Propose alternate surveillance means to adjacent centres.

The sharing of WAM and ADS-B data from the Madeira WAM system has been proposed to the adjacent centres.
ONDA and Santa Maria ACC are correctly receiving and processing Madeira ADS-B data.

A Safety Support Case should be produced.

2.1.5.2 F-9.5.2: Automatic Air Traffic Monitoring

The loss of data from the Porto Santo radar will reduce the surveillance coverage areas, namely the traffic above FL380 and at the north the Madeira sector will not be covered.

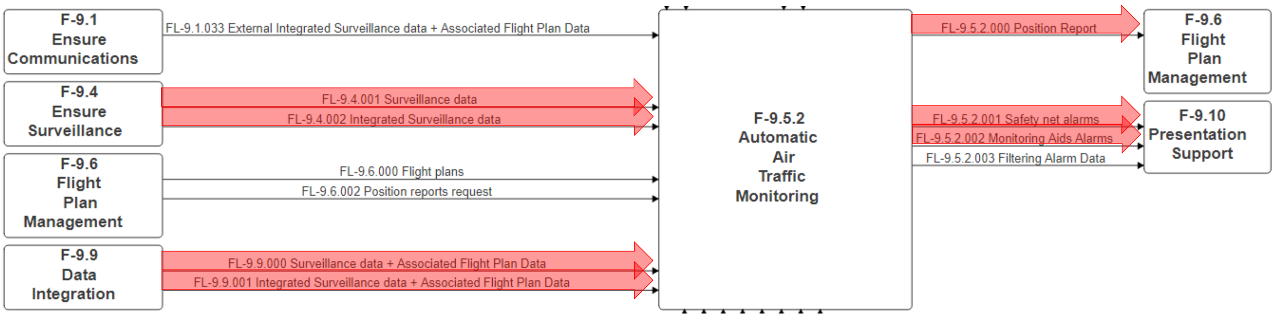
F-9.1 Ensure Communications
FL-9.1.033 External Integrated Surveillance data + Associated Flight Plan Data
F-9.4 Ensure Surveillance
FL-9.4.001 Surveillance data
FL-9.4.002 Integrated Surveillance data
F-9.6 Flight Plan Management
FL-9.6.000 Flight plans
FL-9.6.002 Position reports request
F-9.9 Data Integration
FL-9.9.000 Surveillance data + Associated Flight Plan Data
FL-9.9.001 Integrated Surveillance data + Associated Flight Plan Data
F-9.5.2 Automatic Air Traffic Monitoring
FL-9.5.2.000 Position Report
F-9.6 Flight Plan Management
FL-9.5.2.001 Safety net alarms
FL-9.5.2.002 Monitoring Aids Alarms
FL-9.5.2.003 Filtering Alarm Data
F-9.10 Presentation Support

Figure 13: Planned degraded modes: Impact on F-9.5.2: Automatic Air Traffic Monitoring

There will be no position reports for aircraft without surveillance coverage. Safety nets and monitoring aids will also not be available for these aircraft.

2.1.5.3 F-9.6: Flight Plan Management

The flights crossing the area with no surveillance coverage will not be updated with position reports.

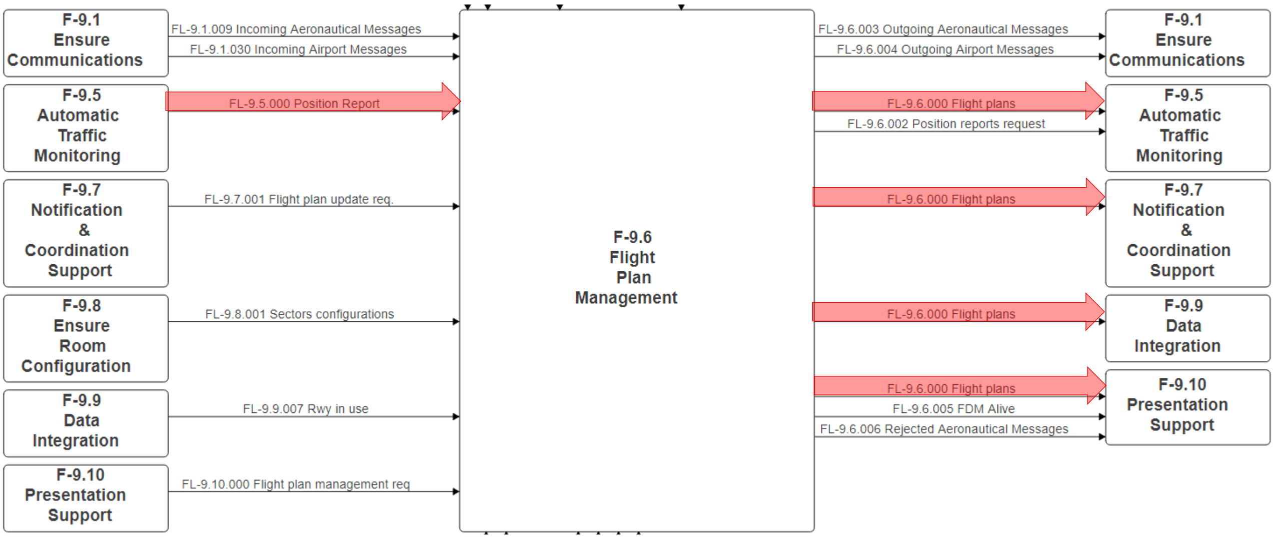
F-9.1 Ensure Communications
FL-9.1.009 Incoming Aeronautical Messages
FL-9.1.030 Incoming Airport Messages
F-9.5 Automatic Traffic Monitoring
FL-9.5.000 Position Report
F-9.7 Notification & Coordination Support
FL-9.7.001 Flight plan update req.
F-9.8 Ensure Room Configuration
FL-9.8.001 Sectors configurations
F-9.9 Data Integration
FL-9.9.007 Rwy in use
F-9.10 Presentation Support
FL-9.10.000 Flight plan management req
F-9.6 Flight Plan Management
FL-9.6.003 Outgoing Aeronautical Messages
FL-9.6.004 Outgoing Airport Messages
F-9.1 Ensure Communications
FL-9.6.000 Flight plans
FL-9.6.002 Position reports request
F-9.5 Automatic Traffic Monitoring
FL-9.6.000 Flight plans
F-9.7 Notification & Coordination Support
FL-9.6.000 Flight plans
F-9.9 Data Integration
FL-9.6.000 Flight plans
FL-9.6.005 FDM Alive
FL-9.6.006 Rejected Aeronautical Messages
F-9.10 Presentation Support

Figure 14: Planned degraded modes: Impact on F-9.6: Flight Plan Management

The estimated times in the flight plan will not be updated with surveillance data reports resulting in less accurate estimates.

2.1.5.4 F-9.7: Notification & Coordination Support

The loss of data from the Porto Santo radar will reduce the surveillance coverage areas, namely the traffic above FL380 and at the north the Madeira sector will not be covered. The Notification & Coordination Support function will not be performed for flights without surveillance reports.

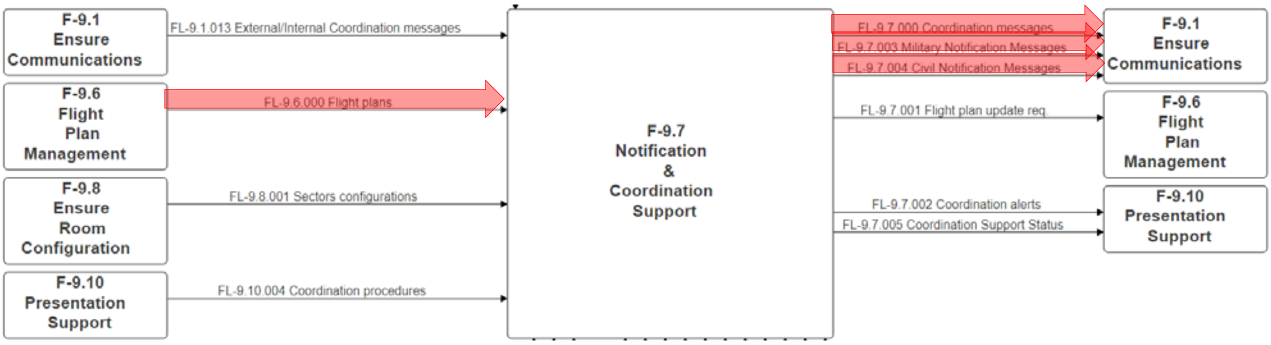
F-9.1
Ensure
Communications
F-9.6
Flight
Plan
Management
F-9.8
Ensure
Room
Configuration
F-9.10
Presentation
Support
FL-9.1.013 External/Internal Coordination messages
FL-9.6.000 Flight plans
FL-9.8.001 Sectors configurations
FL-9.10.004 Coordination procedures
F-9.7
Notification
&
Coordination
Support
FL-9.7.000 Coordination messages
FL-9.7.003 Military Notification Messages
FL-9.7.004 Civil Notification Messages
FL-9.7.001 Flight plan update req
FL-9.7.002 Coordination alerts
FL-9.7.005 Coordination Support Status
F-9.1
Ensure
Communications
F-9.6
Flight
Plan
Management
F-9.10
Presentation
Support

Figure 15: Planned degraded modes: Impact on F-9.7: Notification & Coordination Support

2.1.5.5 F-9.9.2: Air coupler (in Data Integration)

The loss of data from the Porto Santo radar will reduce the surveillance coverage areas, namely the traffic above FL380 and at the north the Madeira sector will not be covered.

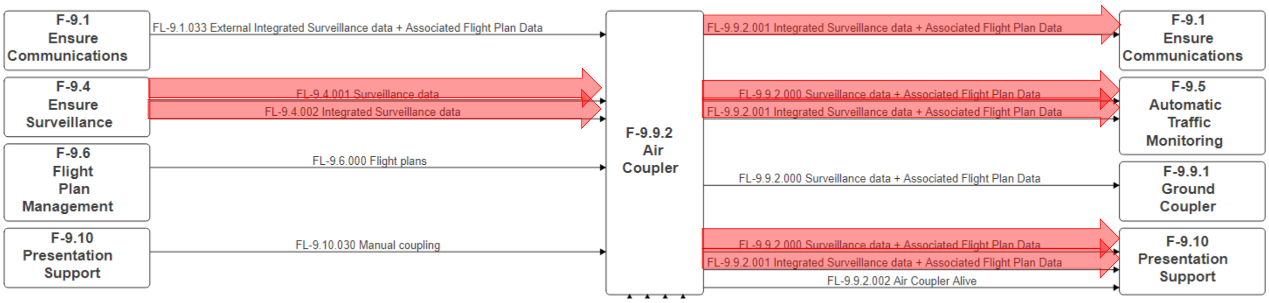
F-9.1
Ensure
Communications
F-9.4
Ensure
Surveillance
F-9.6
Flight
Plan
Management
F-9.10
Presentation
Support
FL-9.1.033 External Integrated Surveillance data + Associated Flight Plan Data
FL-9.4.001 Surveillance data
FL-9.4.002 Integrated Surveillance data
FL-9.6.000 Flight plans
FL-9.10.030 Manual coupling
F-9.9.2
Air
Coupler
FL-9.9.2.001 Integrated Surveillance data + Associated Flight Plan Data
FL-9.9.2.000 Surveillance data + Associated Flight Plan Data
FL-9.9.2.001 Integrated Surveillance data + Associated Flight Plan Data
FL-9.9.2.000 Surveillance data + Associated Flight Plan Data
FL-9.9.2.000 Surveillance data + Associated Flight Plan Data
FL-9.9.2.001 Integrated Surveillance data + Associated Flight Plan Data
FL-9.9.2.002 Air Coupler Alive
F-9.1
Ensure
Communications
F-9.5
Automatic
Traffic
Monitoring
F-9.9.1
Ground
Coupler
F-9.10
Presentation
Support

Figure 16: Planned degraded modes: Impact on F-9.9.2: Air coupler

2.1.5.6 F-9.10.1: Surveillance Presentation

The loss of data from the Porto Santo radar will reduce the surveillance coverage areas, namely in the Madeira sector.

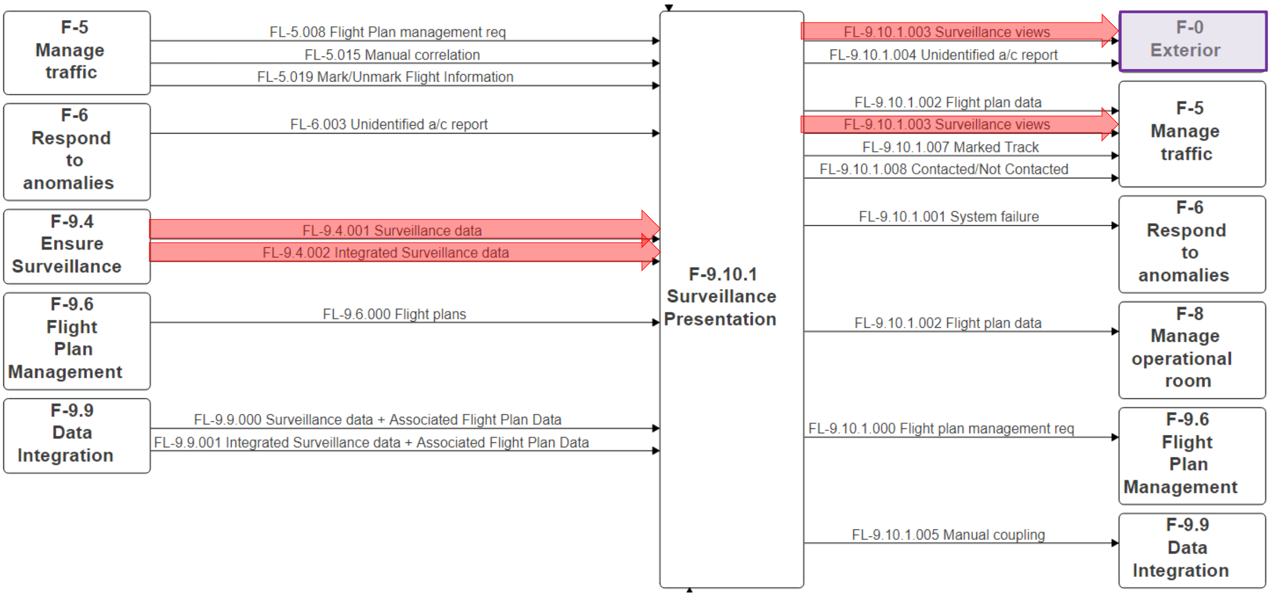
F-5
Manage
traffic
FL-5.008 Flight Plan management req
FL-5.015 Manual correlation
FL-5.019 Mark/Unmark Flight Information
F-6
Respond
to
anomalies
FL-6.003 Unidentified a/c report
F-9.4
Ensure
Surveillance
FL-9.4.001 Surveillance data
FL-9.4.002 Integrated Surveillance data
F-9.6
Flight
Plan
Management
FL-9.6.000 Flight plans
F-9.9
Data
Integration
FL-9.9.000 Surveillance data + Associated Flight Plan Data
FL-9.9.001 Integrated Surveillance data + Associated Flight Plan Data
F-9.10.1
Surveillance
Presentation
FL-9.10.1.003 Surveillance views
FL-9.10.1.004 Unidentified a/c report
F-0
Exterior
FL-9.10.1.002 Flight plan data
FL-9.10.1.003 Surveillance views
FL-9.10.1.007 Marked Track
FL-9.10.1.008 Contacted/Not Contacted
F-5
Manage
traffic
FL-9.10.1.001 System failure
F-6
Respond
to
anomalies
FL-9.10.1.002 Flight plan data
F-8
Manage
operational
room
FL-9.10.1.000 Flight plan management req
F-9.6
Flight
Plan
Management
FL-9.10.1.005 Manual coupling
F-9.9
Data
Integration

Figure 17: Planned degraded modes: Impact on F-9.10.1: Surveillance Presentation

2.1.5.7 F-5: Manage traffic

The information from Porto Santo radar is the only independent means of surveillance in a big area of the Madeira sector including the transition to the West sector. Without this surveillance data source, surveillance services in this area cannot be provided.

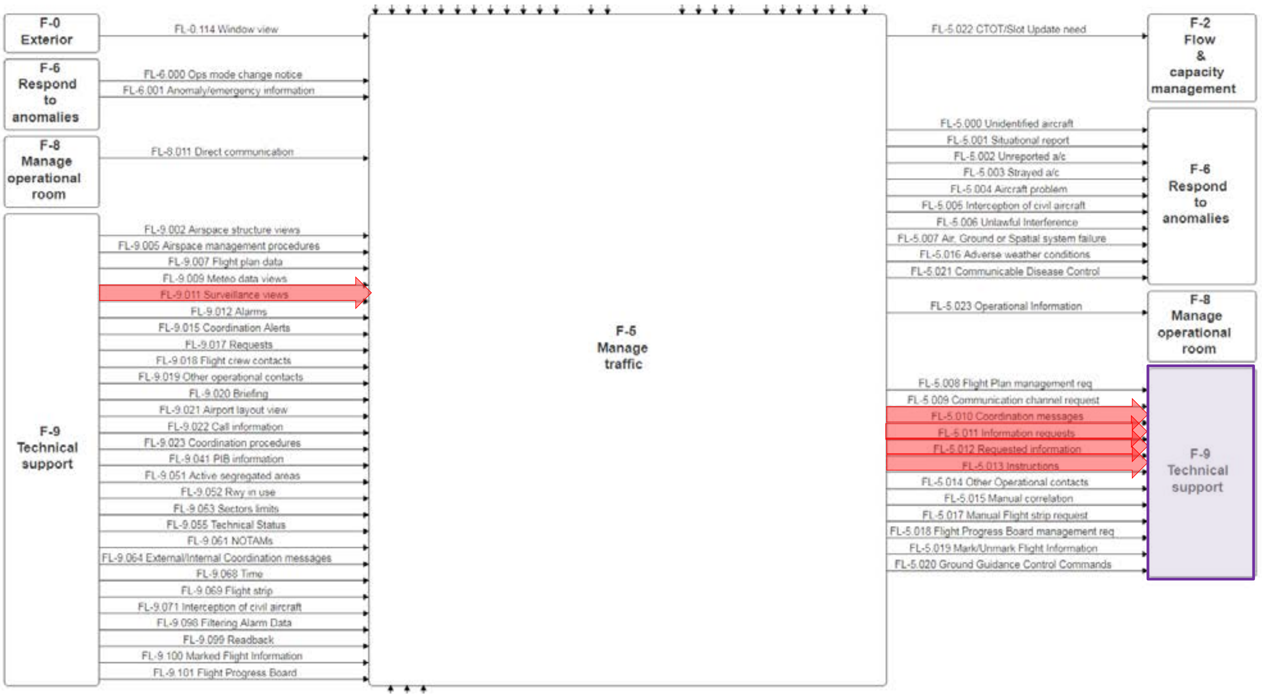
F-0
Exterior
FL-0.114 Window view
F-6
Respond
to
anomalies
FL-6.000 Ops mode change notice
FL-6.001 Anomaly/emergency information
F-8
Manage
operational
room
FL-8.011 Direct communication
F-9
Technical
support
FL-9.002 Airspace structure views
FL-9.005 Airspace management procedures
FL-9.007 Flight plan data
FL-9.009 Meteo data views
FL-9.011 Surveillance views
FL-9.012 Alarms
FL-9.015 Coordination Alerts
FL-9.017 Requests
FL-9.018 Flight crew contacts
FL-9.019 Other operational contacts
FL-9.020 Briefing
FL-9.021 Airport layout view
FL-9.022 Call information
FL-9.023 Coordination procedures
FL-9.041 PIB information
FL-9.051 Active segregated areas
FL-9.052 Rwy in use
FL-9.053 Sectors limits
FL-9.055 Technical Status
FL-9.061 NOTAMs
FL-9.064 External/Internal Coordination messages
FL-9.068 Time
FL-9.069 Flight strip
FL-9.071 Interception of civil aircraft
FL-9.098 Filtering Alarm Data
FL-9.099 Readback
FL-9.100 Marked Flight Information
FL-9.101 Flight Progress Board
F-5
Manage
traffic
FL-5.022 CTOT/Slot Update need
F-2
Flow
&
capacity
management
FL-5.000 Unidentified aircraft
FL-5.001 Situational report
FL-5.002 Unreported a/c
FL-5.003 Strayed a/c
FL-5.004 Aircraft problem
FL-5.005 Interception of civil aircraft
FL-5.006 Unlawful Interference
FL-5.007 Air, Ground or Spatial system failure
FL-5.016 Adverse weather conditions
FL-5.021 Communicable Disease Control
F-6
Respond
to
anomalies
FL-5.023 Operational Information
F-8
Manage
operational
room
FL-5.008 Flight Plan management req
FL-5.009 Communication channel request
FL-5.010 Coordination messages
FL-5.011 Information requests
FL-5.012 Requested information
FL-5.013 Instructions
FL-5.014 Other Operational contacts
FL-5.015 Manual correlation
FL-5.017 Manual Flight strip request
FL-5.018 Flight Progress Board management req
FL-5.019 Mark/Unmark Flight Information
FL-5.020 Ground Guidance Control Commands
F-9
Technical
support

Figure 18: Planned degraded modes: Impact on F-5: Manage traffic

Although there are other surveillance means for the Madeira sector, namely Madeira WAM and ADS-B system, the WAM has limited range (the vertical limit is FL380 and the maximum range from PST is 186NM) and ADS-B only tracks are not being provided. These limitations will impact the service inside part of the Madeira sector and the adjacent units in the areas not covered by other sensors.

An evaluation of the current surveillance system without Porto Santo radar was performed to clearly assess the impact of its outage (ref. [4]).

The operational impact of this degradation was assessed (see ref. [5]) and mitigations defined. Below is a list of identified mitigation actions:

R12. Enable the display of flight plan tracks in the Madeira Sector and part of the West sector.

Implemented and in use in Lisboa ACC.

R13. Tune ATM system to ensure higher adherence of flight plans to surveillance data.

R14. Include the new points in the surveillance display systems.

R15. Review the radar degradation tables for en-route, including Madeira sector.

R16. Develop degradation tables for Madeira TMA.

R17. Implement a procedure to print contingency flight strips.

Contingency procedures were studied and defined to ensure a safe ATC service during the outage of Porto Santo radar. These procedures were assessed in the ASO (see ref. [5]).

R18. Define contingency procedures for surveillance failures affecting the Madeira sector.

R19. Define the Madeira sector capacities for contingency operations.

R20. Assess the safety of the contingency procedures for the Madeira sector.

R21. Train the contingency procedures for surveillance failures affecting the Madeira sector.

Training took place. It started in February 2018.

R22. Publish the contingency procedures for surveillance failures affecting the Madeira sector.

Published in AIP SUP 057/2017.

2.1.5.8 Hazards in Planned degraded modes

As there are no new outputs of the border functions, there are no new hazards.

The list of existing hazards, as identified in the unit FHA for Lisboa ACC and the Madeira tower, and relevant for this change, are covered in Table 5: Normal operations: Hazard list.

The flows that might be affected by this change are:

- Surveillance interrogations – Already covered in paragraph 2.2 - Normal operations
- Surveillance data – Already covered in paragraph 2.2 - Normal operations
- Surveillance views - Already covered in paragraph 2.2 - Normal operations
- Coordination messages
- Instructions

The following table examines the impact this change might have on the existing hazards:

Flow	Hazard	Probability of hazard
Coordination messages	Not provided	Possible increase due to reduction in surveillance coverage area.
Coordination messages	Corrupt	Same as in normal operations.
Coordination messages	Incorrect	Possible increase due to reduction in surveillance coverage area.
Instructions	Not provided	Possible increase due to reduction in surveillance coverage area.
Instructions	Corrupt	Same as in normal operations.
Instructions	Incorrect	Possible increase due to reduction in surveillance coverage area.

Table 1: Planned degraded modes: Impact on existing hazards

2.1.5.8.1 Planned degraded modes – External hazards

Hazards outside the system are addressed by the model as inputs to the functional model that might impact its functioning. These inputs might be correct, incorrect or missing. The fact that the Porto Santo radar is out of service during its replacement will cause the missing of surveillance information in the impacted area. The mitigations defined for this planned degraded mode aim also at reducing the risk associated with these external hazards.

As an example, in cases of communication failure in an aircraft, the system will miss the communication inputs from this aircraft. If it is also in an area where there is no surveillance data, the system will not detect this problem as easily as before, but there are processes that ensure a safe provision of service in areas with no surveillance.

2.1.5.9 Cause identification in Planned degraded modes

All the causes covered in paragraph 2.2 - Normal operations are not repeated here.

The following table identifies possible causes for the hazards identified above:

Hazard	Possible causes
Not provided Coordination messages	Aircraft ignored as it is not shown on the screen, moving and entering adjacent area. Error on the FPL track position causes lack of awareness of need to coordinate. When applying procedural control, routes in Madeira sector are too close to adjacent area routes (BEXAL-KOMBA) requiring coordination of all traffic, with high probability of not coordinating some aircraft due to workload.
Incorrect Coordination messages	Aircraft coordinated based on outdated flight strip information. Error on the FPL track position causes wrong coordination of aircraft, e.g. wrong estimated exit time or flight level. When applying procedural control, routes in Madeira sector are too close to adjacent area routes (BEXAL-KOMBA) requiring coordination of all traffic, with high probability of wrong coordination due to workload.
Not provided Instructions	Aircraft in conflict with other traffic is ignored because it is not shown on the screen, causes ATCO not issuing instruction. Error on the FPL track position misleads awareness of real aircraft separation and causes ATCO not to issue required separation instruction.
Incorrect Instructions	Wrong awareness of aircraft not shown on the screen causes ATCO to issue wrong instruction. Error on the FPL track position misleads awareness of real aircraft separation and causes ATCO to issue wrong separation instruction.

Table 2: Planned degraded modes: Cause identification

2.1.5.10 Mitigation actions for planned degraded modes

The following actions have already been identified during the analysis of each hazard:

Hazard	Mitigation Actions
Not provided Coordination messages	Strategy: Reduction or control R21. Train the contingency procedures for surveillance failures affecting the Madeira sector. R12. Enable the display of flight plan tracks in the R13. Tune ATM system to ensure higher adherence of flight plans to surveillance data. Strategy: Avoidance R18. Define contingency procedures for surveillance failures affecting the Madeira sector. R22. Publish the contingency procedures for surveillance failures affecting the Madeira sector.
Incorrect Coordination messages	Strategy: Reduction or control R21. Train the contingency procedures for surveillance failures affecting the Madeira sector. R12. Enable the display of flight plan tracks in the Madeira Sector and part of the West sector. R13. Tune ATM system to ensure higher adherence of flight plans to surveillance data. Strategy: Avoidance R18. Define contingency procedures for surveillance failures affecting the Madeira sector. R22. Publish the contingency procedures for surveillance failures affecting the Madeira sector.
Not provided Instructions	Strategy: Reduction or control R21. Train the contingency procedures for surveillance failures affecting the Madeira sector. R12. Enable the display of flight plan tracks in the Madeira Sector and part of the West sector. R13. Tune ATM system to ensure higher adherence of flight plans to surveillance data.
Incorrect Instructions	Strategy: Reduction or control R21. Train the contingency procedures for surveillance failures affecting the Madeira sector. R12. Enable the display of flight plan tracks in the Madeira Sector and part of the West sector. R13. Tune ATM system to ensure higher adherence of flight plans to surveillance data.

Table 3: Planned degraded modes: Risk mitigation actions

2.1.6 Transition

During the installation and transition, the main impact will be the loss of data from the Porto Santo radar. When the upgrade of the Porto Santo radar is complete, its information will be evaluated. During this time the data will still not be provided. After successful evaluation, the data will be integrated in the systems and surveillance services in Madeira sector and Madeira Tower will return to normal. Only at this time will data be again sent to adjacent centres.

The loss of data from the Porto Santo radar impacts the Surveillance data output from F-9.42.1: Sensor & Local Tracking and the downstream functions:

- F-9.4.2: Ensure Air Surveillance
- F-9.10.1: Surveillance Presentation

- F-5: Manage traffic

This impact requires a geographical analysis.

The loss of data from the Porto Santo radar can also occur during normal operations due to a failure of in case of maintenance interventions.

The Porto Santo radar will be out of service until the radar data and the required system changes are successfully evaluated and the NSA accepts the proposed change.

Degraded mode	Plan	Impact
No data	From 17th October until January 2019	See below.
Corrupt data	May occur during test phases (From December to May)	Avoided by following procedure: Radar will be disconnected from operational system. All tests and evaluations will be conducted on the test environment.
Incorrect data	May occur during test phases (From December to May)	Avoided by following procedure: Radar will be disconnected from operational system. Evaluations will be conducted on the test environment and system will only be connected to the operational environment after data is validated.

Table 4: Planned degraded modes

With these actions it can be ensured that during transition the only relevant degraded mode is the loss of Porto Santo radar data.

Note: In the period following any transition issues may arise. During these times additional awareness is required to actively identify unforeseen consequences, evaluate them and act is needed. Special monitoring requirements may need to be put in place during these transient functional system states.

2.2 Normal operations

1 – Identify the impacted border functions, i.e. with interfaces to either non-technical functions or Ensure communications or Exterior.

2 – Identify hazards, Identify possible causes and Define mitigations as described in 2.1.5.

From the above analysis of the change, the impacted border functions, i.e. with interfaces to either non-technical functions or Ensure communications or Exterior are:

- Sensor & Local Tracking
- Filtering & Forwarding
- Air Surveillance Presentation

2.2.1 Hazards in Normal operations

As there are no new outputs of the border functions, there are no new hazards.
The existing hazards, as identified in the unit FHA for Lisboa ACC and the Madeira tower and relevant for this change are:

Data Flow	Destination	Harmful effect
F-5 – Manage Traffic		
- Requested Information Not provided Incorrect Corrupted	Flight crew	Possible MAC (Help needed for scenarios)
- Instructions	Flight crew	Possible CFIT, MAC or Taxiway Collision in case of

Data Flow	Destination	Harmful effect
Not provided Incorrect Corrupted		wrong or missing instructions causing erosion of separation not detected or prevented by aircrew(s).
- Coordination messages [1] Not provided Incorrect Corrupted	Adjacent units	Possible MAC (Help needed for scenarios)

Table 5: Normal operations: Hazard list

The flows that might be affected by this change are:

- Surveillance interrogations – see analysis in 2.1.3.1
- Surveillance data – see analysis in 2.1.3.2
- Surveillance views

Analysis of the impact on Surveillance views requires a geographical analysis.

The flow Surveillance views impacts the function Manage traffic (see F-9.5.2:) and can indirectly impact the following flows:

- Requested Information
- Instructions
- Information requests
- Coordination messages

R23. Perform Operational Safety Assessment of the possible impacts of Surveillance views, including a geographical analysis.

ASO ???

2.2.1.1.1 Normal operations – External hazards

Hazards outside the system are addressed by the model as inputs to the functional model that might impact its functioning. These inputs might be correct, incorrect or missing. In normal operations there is no change to the way Hazards outside the system are handled.

2.2.2 Cause identification in Normal operations

As this is a technical change, the causes are associated with the changed components, namely enablers.

The following image depicts the flow of surveillance information from the radar to the ATCO display:

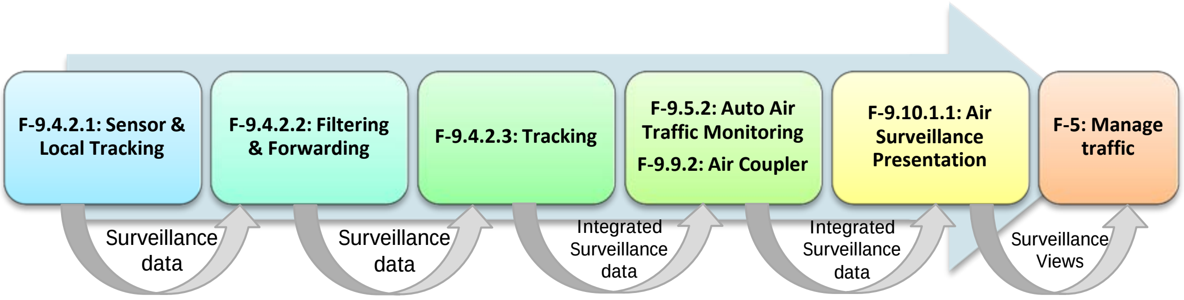
F-9.4.2.1: Sensor & Local Tracking
F-9.4.2.2: Filtering & Forwarding
F-9.4.2.3: Tracking
F-9.5.2: Auto Air Traffic Monitoring
F-9.9.2: Air Coupler
F-9.10.1.1: Air Surveillance Presentation
F-5: Manage traffic
Surveillance data
Surveillance data
Integrated Surveillance data
Integrated Surveillance data
Surveillance Views

Figure 19: Flow of surveillance data

[1] Coordination messages include also the ones generated by the “Notification and Coordination Support” function.

Function	Possible causes - Enablers
F-9.4.2.1: Sensor & Local Tracking	Radar with lower performance or coverage can cause partial loss of surveillance data in the Porto Santo coverage area. Misalignment of the radar may cause corrupt or incorrect surveillance data in the Porto Santo coverage area.
F-9.4.2.2: Filtering & Forwarding	SDDS-NG not capable to process data or wrong configuration might cause losses of surveillance data.
F-9.4.2.3: Tracking	Wrong configuration of ARTAS might cause losses of, incorrect or corrupt Integrated Surveillance data.
F-9.5.2: Automatic Air Traffic Monitoring	ATSS not able to process Mode S data will cause loss of safety net and monitoring aid alarm data for Porto Santo flow. Wrong configuration of ATSS might cause losses of, incorrect or corrupt Surveillance data.
F-9.9.2: Air Coupler	ATSS not able to process Mode S data will cause loss of integrated surveillance data for Porto Santo flow. Wrong configuration of ATSS might cause losses of, incorrect or corrupt Surveillance data.
F-9.10.1.1: Air Surveillance Presentation	ASD not able to process Mode S data will cause loss of Surveillance views for Porto Santo flow. Wrong configuration of ASD might cause losses of, incorrect or corrupt Surveillance views.

Table 6: Normal operations: Cause identification

Note: If a function is not adapted correctly or fails the output flows could become totally or partially unavailable, corrupt or incorrect. This is considered a degraded mode and is addressed in paragraph 2.1.5.

2.2.3 Mitigation actions for Normal Operations

The following actions have already been identified during the analysis of each function:

Function	Actions
F-9.4.2.1: Sensor & Local Tracking	Strategy: Avoidance R2. The new Porto Santo radar shall detect cooperative non Mode S equipped aircraft.
F-9.4.2.2: Filtering & Forwarding	Strategy: Reduction or control R3. External partners (ONDA & ENAIRE) shall be informed of the change in the data format.
F-9.4.2.3: Tracking	Strategy: Avoidance R4. Verify that the Tracking outputs from ARTAS are identical to the current operational ones.
F-9.5.2: Automatic Air Traffic Monitoring	Strategy: Avoidance R5. Verify that the Automatic Air Traffic Monitoring outputs are not changed.
F-9.9.2: Air Coupler	Strategy: Avoidance R6. Verify that the Air Coupler outputs are not changed. R7. Verify that Air Coupler enablers are capable of processing Mode S radar data.
F-9.10.1.1: Air Surveillance Presentation	Strategy: Avoidance R8. Verify that the Surveillance views are not changed R9. Verify that Air Surveillance Presentation enablers are capable of displaying Mode S radar data.

Table 7: Normal operations: Risk mitigation actions

To address the identified possible causes, the following additional actions to reduce the safety risk are proposed:

R24. Evaluate Porto Santo radar performance and analyse shortcomings and their impact.

An initial evaluation was performed and limitations to the coverage range were identified. The cause was determined and the following actions taken:

- Change ASTERIX data format to allow for ranges above 256NM, extended range, in category 048.
- Request change in ARTAS (ACP 595).
- SDDS-NG is already capable of handling the extended range reports.

3 Safety Argument

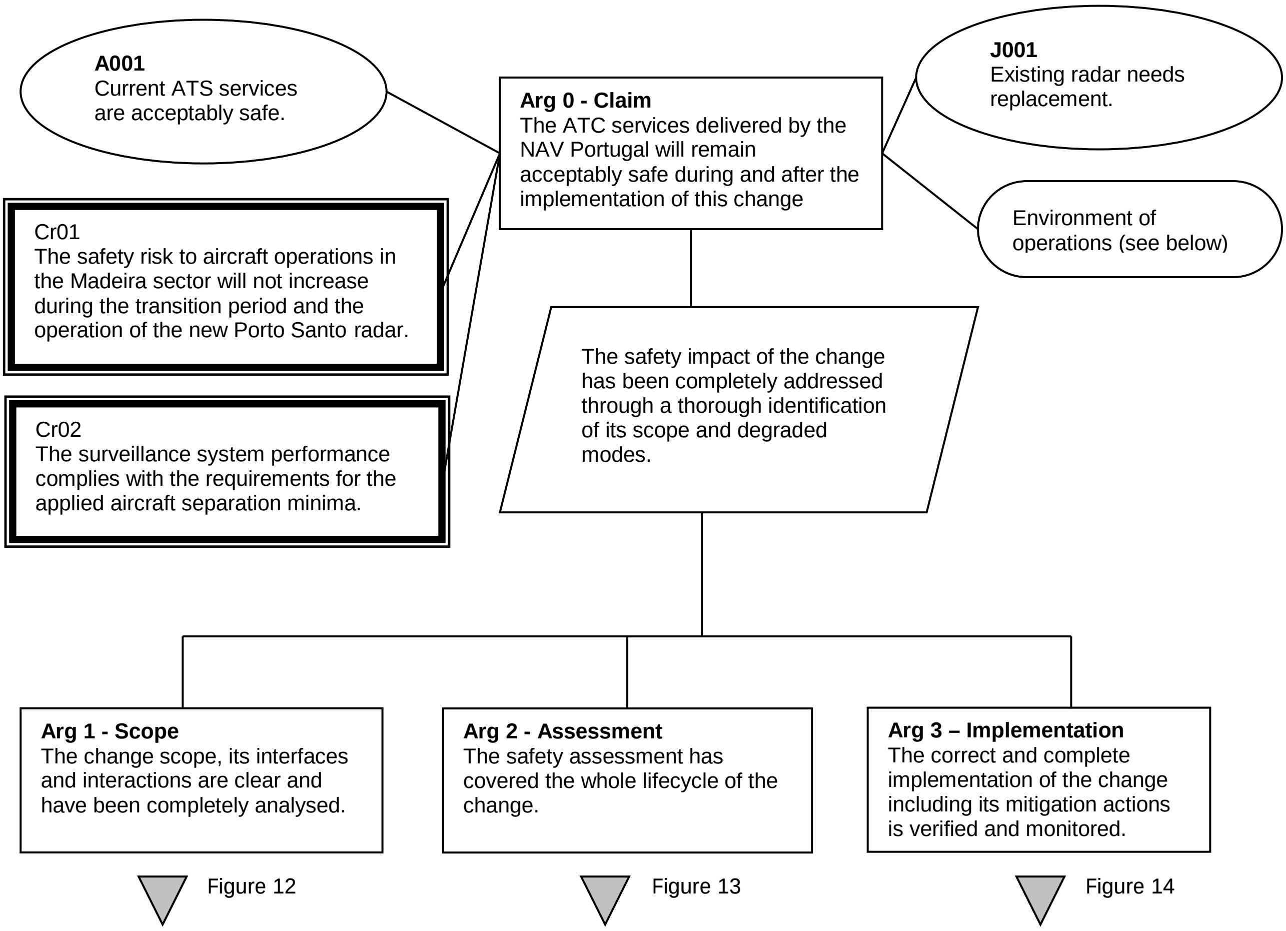
A001
Current ATS services are acceptably safe.
Arg 0 - Claim
The ATC services delivered by the NAV Portugal will remain acceptably safe during and after the implementation of this change
J001
Existing radar needs replacement.
Environment of operations (see below)
Cr01
The safety risk to aircraft operations in the Madeira sector will not increase during the transition period and the operation of the new Porto Santo radar.
Cr02
The surveillance system performance complies with the requirements for the applied aircraft separation minima.
The safety impact of the change has been completely addressed through a thorough identification of its scope and degraded modes.
Arg 1 - Scope
The change scope, its interfaces and interactions are clear and have been completely analysed.
Arg 2 - Assessment
The safety assessment has covered the whole lifecycle of the change.
Arg 3 – Implementation
The correct and complete implementation of the change including its mitigation actions is verified and monitored.
Figure 12
Figure 13
Figure 14

Figure 20: Top level argument

Note: The argument's graphical presentation uses the GSN notation as described in the Safety Case Development Manual (Ref. [9]).

A001 – Assumption

The ATS services provided by NAV Portugal are considered acceptably safe.
There are no reservations from the regulator with regards to the safety of the services provided by the NAV Portugal neither are there impeditive issues identified by NAV Portugal.

J001 – Justification for the change

The existing radar has reached its end of life. Performance is degrading and maintenance can no longer ensure its normal functioning. The degradation is notorious and has been reported in the monthly evaluation reports.

Context

The environment of operations relevant for this assessment is:

- Lisboa ACC, described in [2]
- Madeira Tower, described in [3]

Safety Criteria

Cr01
The safety risk to aircraft operations in the Madeira sector will not increase during the transition period and the operation of the new Porto Santo radar.
This criterion is translated to:

1. There will be no increase of separation infringements in the Madeira sector.
2. There will be no increase of lack of coordination occurrences between the Madeira sector and adjacent areas and sectors.

Safety objectives / Proxies: There will be no separation infringements or lack of coordination with adjacent centres attributable to this change, from the stopping of the existing radar until 2 years after the operational use of the new Porto Santo radar.

Cr02
The surveillance system performance complies with the requirements for the applied aircraft separation minima.

Safety objective / Proxy: The surveillance system performance, in the Madeira sector, Madeira TMA and the transition to the West sector, where the current defined separation minima is 8NM, will comply with the performance requirements applicable for the surveillance services provided by NAV Portugal.

3.1 Argument 1 – Change scope

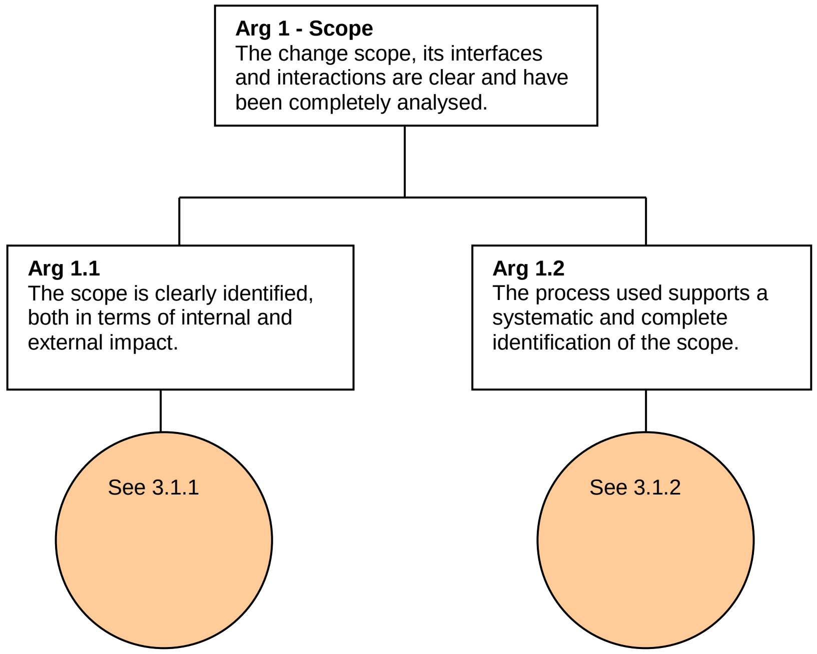
Arg 1 - Scope
The change scope, its interfaces and interactions are clear and have been completely analysed.
Arg 1.1
The scope is clearly identified, both in terms of internal and external impact.
Arg 1.2
The process used supports a systematic and complete identification of the scope.
See 3.1.1
See 3.1.2

Figure 21: Argument 1 – Change scope

3.1.1 Argument 1.1 – Change impact

The change impact is analysed in 2.

There is impact to the Lisboa ACC, Madeira tower and adjacent units of Santa Maria.
There is impact to Morocco and Spain.
There are changes to the surveillance data interfaces.

The identified impacted functions are:

- F-9.4.2.1: Sensor & Local Tracking – see 2.1.3.1
- F-9.4.2.2: Filtering & Forwarding – see 2.1.3.2

- F-9.4.2.3: Tracking – see 2.1.3.4
- F-9.9.2: Air Coupler – see 2.1.3.5
- F-9.10.1.1: Air Surveillance Presentation – see 2.1.3.7

3.1.2 Argument 1.2 – Process

The process used to analyze the change is described in the blue boxes inserted in 2.
It is systematic and can be repeated by other experts.
It ensures that the scope of the change is completely and correctly identified covering:

(i) the equipment, procedural and human elements being changed;
(ii) interfaces and interactions between the elements being changed and the remainder of the functional system;
(iii) interfaces and interactions between the elements being changed and the context in which it is intended to operate;
(iv) the life cycle of the change from definition to operations including transition into service;
(v) planned degraded modes of operation of the functional system;

And the identification of hazards.

Appendix A - Traceability to regulation EU 1035/2011 and Appendix B - Traceability to regulation 2017/373 AMC & GM present the compliance with applicable regulation, AMC and GM.

3.2 Argument 2 – Safety Assessment

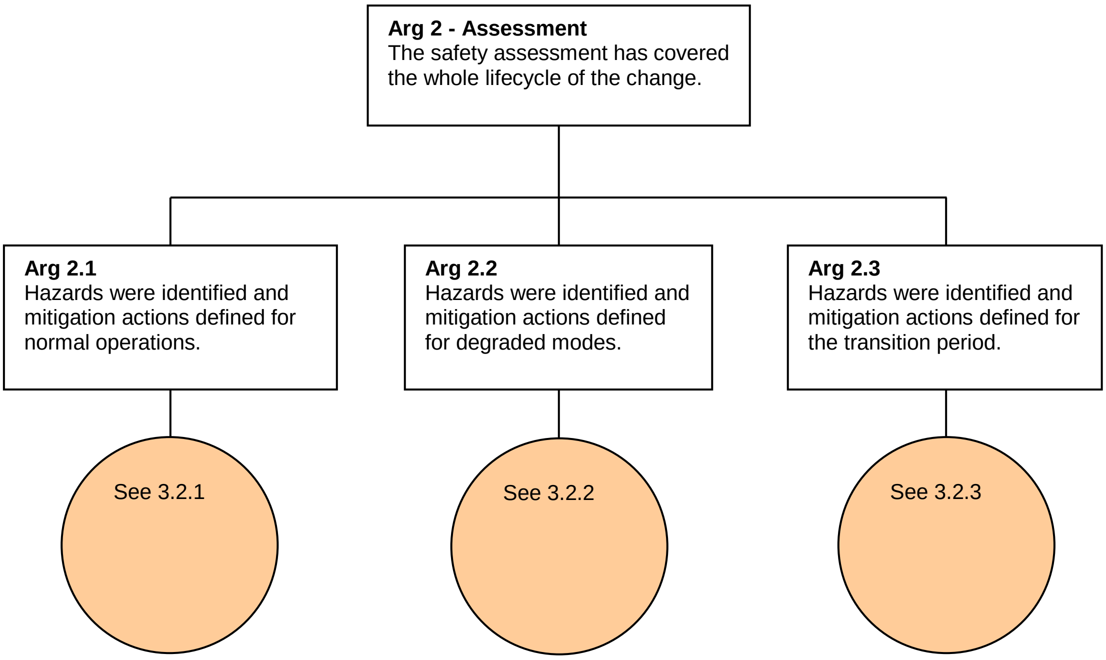
Arg 2 - Assessment
The safety assessment has covered the whole lifecycle of the change.
Arg 2.1
Hazards were identified and mitigation actions defined for normal operations.
Arg 2.2
Hazards were identified and mitigation actions defined for degraded modes.
Arg 2.3
Hazards were identified and mitigation actions defined for the transition period.
See 3.2.1
See 3.2.2
See 3.2.3

Figure 22: Argument 2 – Safety Assessment

3.2.1 Argument 2.1 – Normal operations

Normal operations have been analyzed in 2.2 - Normal operations.
As there are no new outputs of the border functions, there are no new hazards.
Impacts on existing hazards have been assessed. Causes have been identified.
Actions to reduce the impact on existing hazards were defined. See 2.2.3 - Mitigation actions.

3.2.2 Argument 2.2 – Degraded modes

Degraded modes have been analyzed in paragraph 2.1.5. - Planned degraded modes

An evaluation of the current surveillance system without Porto Santo radar was performed to clearly assess the impact of its outage (ref. [4]).

The operational impact of this degradation was assessed (see ref. [5]) and mitigations defined.

Contingency procedures were studied and defined to ensure a safe ATC service during the outage of Porto Santo radar. These procedures were assessed in the ASO (see ref. [5]).

3.2.3 Argument 2.3 – Transition

Transition was assessed in paragraph 2.1.6 - Transition.
The impact during transition will be the loss of Porto Santo radar data.
Alternative surveillance means will be provided to external users to mitigate loss of surveillance coverage.
To minimize the impact of the loss of Porto Santo radar on the provision of ATC services in the Madeira sector, changes were proposed to both the airspace and operational procedures. An Operational Safety Assessment was performed on the transition period covering both the loss of surveillance coverage in the Madeira sector and the proposed airspace and procedure changes (see ref. [5]).

ID	Description
R14.	Include the new points in the surveillance display systems.
R15.	Review the radar degradation tables for en-route, including Madeira sector.
R16. R17.	Develop degradation tables for Madeira TMA.
R17.	Implement a procedure to print contingency flight strips.
R18.	Define contingency procedures for surveillance failures affecting the Madeira sector.
R19.	Define the Madeira sector capacities for contingency operations.
R20.	Assess the safety of the contingency procedures for the Madeira sector.
R21.	Train the contingency procedures for surveillance failures affecting the Madeira sector.
R22.	Publish the contingency procedures for surveillance failures affecting the Madeira sector.

3.3 Argument 3 – Change Implementation

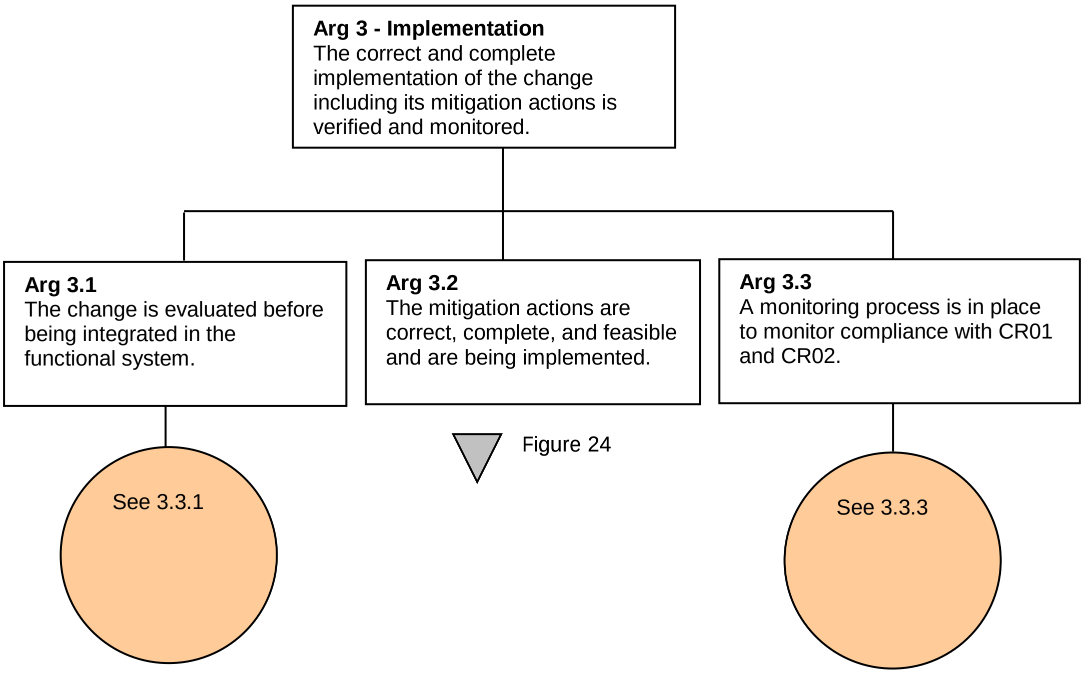
Arg 3 - Implementation
The correct and complete implementation of the change including its mitigation actions is verified and monitored.
Arg 3.1
The change is evaluated before being integrated in the functional system.
Arg 3.2
The mitigation actions are correct, complete, and feasible and are being implemented.
Arg 3.3
A monitoring process is in place to monitor compliance with CR01 and CR02.
Figure 24
See 3.3.1
See 3.3.3

Figure 23: Argument 3 – Change Implementation

3.3.1 Argument 3.1 – Verification

The start of the transition, i.e. the stop of the radar station, was only performed after a successful completion of the following actions:

ID	Description
R18.	Define contingency procedures for surveillance failures affecting the Madeira sector.
R19.	Define the Madeira sector capacities for contingency operations.
R20.	Assess the safety of the contingency procedures for the Madeira sector.
R21.	Train the contingency procedures for surveillance failures affecting the Madeira sector.
R22.	Publish the contingency procedures for surveillance failures affecting the Madeira sector.

Table 8: Verification of conditions for transition

The integration into normal operations will only be performed after the evaluation of the radar performance and of the tracking behavior with the changed radar integrated. The change will only be integrated in the functional system after the successful completion of the following evaluation actions:

ID	Description
R4.	Verify that the Tracking outputs from ARTAS are identical to the current operational ones.
R5.	Verify that the Automatic Air Traffic Monitoring outputs are not changed.
R6.	Verify that the Air Coupler outputs are not changed.
R8.	Verify that the Surveillance views are not changed
R24.	Evaluate Porto Santo radar performance and analyse shortcomings and their impact.

Table 9: Normal operations evaluation actions

3.3.2 Argument 3.2 – Mitigation

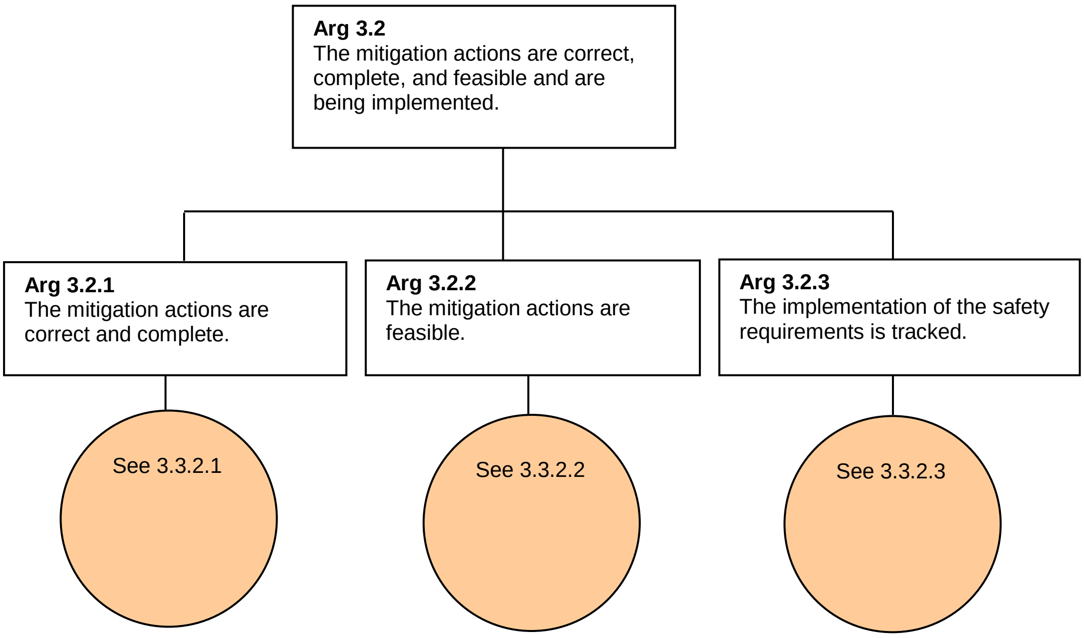
Arg 3.2
The mitigation actions are correct, complete, and feasible and are being implemented.
Arg 3.2.1
The mitigation actions are correct and complete.
Arg 3.2.2
The mitigation actions are feasible.
Arg 3.2.3
The implementation of the safety requirements is tracked.
See 3.3.2.1
See 3.3.2.2
See 3.3.2.3

Figure 24: Argument 3.2 – Mitigation

3.3.2.1 Argument 3.2.1 – Mitigation is correct & complete

The impact of the change is systematically identified with the help of a model in both the normal operation mode and the planned degraded modes. The model is used to help ensure completeness of the analysis, as

it captures in a systematic way, knowledge from various experts. All functions that are directly or indirectly affected are listed and analyzed.
The identification of hazards is performed by checking all outputs that directly or indirectly are sent to Exterior (the outside world) that might be impacted. For all impacted outputs, check existing hazards; for all new outputs identify possible new hazards. Also all outputs to non-technical functions that might be impacted are checked and for all changed or new ones an Operational Safety Assessment is performed.
After identifying the hazards, the possible causes that might arise from the change under analysis are identified. The experts from the area identify what can go wrong for all impacted functions. The model is in fact used as a check list that will allow for a systematic process to define the mitigation actions and also allows for the reproducibility of the outputs.

The last step is to define mitigations for the identified causes using one or more of the following strategies, in order of decreasing preference:

- Avoidance – Stop the propagation of the problem in the functional system
- Reduction or control – Reduce the probability or the impact of the problem
- Acceptance – Acknowledge and then define ways to handle the problem

The fact that impacted interfaces and all causes are addressed ensures completeness. The review performed by experts of both the application of the process and the list of mitigation actions is aimed at the correctness of the mitigation strategy.

The risk mitigation actions for the planned degraded modes were identified in paragraph 2.1.5.10, and are:

ID	Description
R1.	The new Porto Santo maintenance team shall be trained to maintain the new radar.
R2.	The new Porto Santo radar shall detect cooperative non Mode S equipped aircraft.
R3.	External partners (ONDA & ENAIRE) shall be informed of the change in the data format.
R4.	Verify that the Tracking outputs from ARTAS are identical to the current operational ones.
R5.	Verify that the Automatic Air Traffic Monitoring outputs are not changed.
R6.	Verify that the Air Coupler outputs are not changed.
R7.	Verify that Air Coupler enablers are capable of processing Mode S radar data.
R8.	Verify that the Surveillance views are not changed
R9.	Verify that Air Surveillance Presentation enablers are capable of displaying Mode S radar data.
R10.	Ensure that the adjacent centres are informed well in advance of Porto Santo outage.
R11.	Propose alternate surveillance means to adjacent centres.
R12.	Enable the display of flight plan tracks in the Madeira Sector and part of the West sector.
R13.	Tune ATM system to ensure higher adherence of flight plans to surveillance data.
R14.	Include the new points in the surveillance display systems.
R15.	Review the radar degradation tables for en-route, including Madeira sector.
R16.	Develop degradation tables for Madeira TMA.
R17.	Implement a procedure to print contingency flight strips.
R18.	Define contingency procedures for surveillance failures affecting the Madeira sector.
R19.	Define the Madeira sector capacities for contingency operations.
R20.	Assess the safety of the contingency procedures for the Madeira sector.
R21.	Train the contingency procedures for surveillance failures affecting the Madeira sector.
R22.	Publish the contingency procedures for surveillance failures affecting the Madeira sector.
R23.	Perform Operational Safety Assessment of the possible impacts of Surveillance views, including a geographical analysis.
R24.	Evaluate Porto Santo radar performance and analyse shortcomings and their impact.

Table 10: Risk mitigation actions

The risk mitigation actions for normal operations were identified in paragraph 2.2.3, and are:

- R2. The new Porto Santo radar shall detect cooperative non Mode S equipped aircraft.
- R3. External partners (ONDA & ENAIRE) shall be informed of the change in the data format.
- R4. Verify that the Tracking outputs from ARTAS are identical to the current operational ones.
- R6. Verify that the Air Coupler outputs are not changed.

- R7. Verify that Air Coupler enablers are capable of processing Mode S radar data.
- R8. Verify that the Surveillance views are not changed
- R9. Verify that Air Surveillance Presentation enablers are capable of displaying Mode S radar data.

3.3.2.2 Argument 3.2.1 – Mitigation is feasible

All mitigation actions are validated with the subject matter experts. The list of mitigation actions is reviewed and responsibilities for their implementation are allocated. The responsible for the mitigation actions validate them and propose alternatives in case they are not feasible.

3.3.2.3 Argument 3.2.1 – Mitigation is tracked

The defined risk mitigation actions are being followed. The following tables cover the current status of risk mitigation actions, which are in fact safety requirements:

ID	Action / Notes	Plan	Status
R1.	Train maintenance team.	AM	Planned
R2.	Requirement	AM	
R3.	Spain, Morocco and Santa Maria were informed.	2018	Completed
R4.	Evaluation of the tracker outputs will be performed.	2Q 2019	Planned
R5.	A test will be performed.	2Q 2019	Planned
R6.	A test will be performed.	2Q 2019	Planned
R7.	To be checked.	Asap.	Planned
R8.	A test will be performed.	1Q 2019	
R9.	To be checked.	Asap.	Planned
R10.	Spain, Morocco and Santa Maria were informed.	2017	Completed
R11.	ADS-B data from Madeira WAM system was proposed. Integration in Santa Maria is completed. Spain reported no interest. Morocco is evaluating.	2017	Completed.
R12.	Flight plan tracks are available. The functionality and the HMI were validated during the ATCO training.	3Q2018	Completed
R13.	The tuning was tested and validated during the ATCO training.	2Q2018	Completed
R14.	The display maps were changed.	3Q2018	Completed.
R15.	Radar degradation tables were reviewed and now cover the Madeira sector and its surveillance means.	3Q2018	Completed.
R16.	The new radar separation minima for the Lisbon FIR were published in IS 025/TRALIS/18.	October 2018	Completed.
R17.	A tactical procedure exists. The supervisor requests that a flight data assistant prints the contingency flight strips.		Completed.
R18.	A working group was set up to define the contingency procedures, and these procedures are described in AIP SUP032/2018. (Ref. [11])	2Q2018	Completed.
R19.	An email message was sent to NMOC with the he Madeira sector capacities for contingency operations: • *WITH WAM/WITHOUT MSSR – 16/H* • *WITHOUT WAM/WITHOUT MSSR – 9/H*	11th October 2018	Completed.
R20.	The contingency procedures were evaluates using simulation and during the training sessions. (Ref. [10])	2Q2018	Completed
R21.	The training plan was defined in IS 079/18/CONLIS (Ref. [10])	2Q2018	Completed.
R22.	Contingency procedures for surveillance failures affecting the Madeira sector were published in AIP SUP032/2018.	3Q2018	Completed.
R23.	ASO was performed.	2018	Completed
R24.	Evaluation of the sensor will be performed.	2Q 2019	Planned

Table 11: Implementation of risk mitigation actions

3.3.3 Argument 3.3 – Monitoring

3.3.3.1 CR01

ATCO and supervisors are required to report all safety related occurrences to NAPATM. This department then processes and forwards the reports to the official entities. The aim of the analysis carried out by NAPATM is to identify risk areas in the ATM system, evaluate the safety performance and its trends as well as monitor the impact of changes to the ATM system and take remedial action when required.
These procedures ensure that compliance with safety criteria CR01 is monitored.

3.3.3.2 CR02

The surveillance system performance is continuously monitored and deviations are promptly reported and acted upon. NAV Portugal performs real time monitoring of the surveillance infrastructure to verify that the integrated surveillance data, also known as surveillance picture, is fit for purpose, i.e. complies with the requirements for the separation minima applied in each area.

The performance of the sensors (F-9.4.2.1: Sensor & Local Tracking) and the tracker is evaluated every month, using the EUROCONTROL SASS-C tool. This evaluation covers probability of detection, accuracy, false target rate and bias measurements and checks the compliance with ESASSP requirements for the separation minima applied in each area.
The purpose of these analyses is to have an early detection of problems and avoiding any impact on the provision of air traffic services.

Appendix A - Traceability to regulation EU 1035/2011

	Proposed process
3.2. Safety requirements for risk assessment and mitigation with regard to changes	
3.2.1. Section 1 *Within the operation of the SMS, providers of air traffic services shall ensure that hazard identification as well as risk assessment and mitigation are systematically conducted for any changes to those parts of the ATM functional system and supporting arrangements within their managerial control, in a manner which addresses:* *(a) the complete life cycle of the constituent part of the ATM functional system under consideration, from initial planning and definition to post-implementation operations, maintenance and decommissioning;* *(b) the airborne, ground and, if appropriate, spatial components of the ATM functional system, through cooperation with responsible parties* *(c) the equipment, procedures and human resources of the ATM functional system, the interactions between these elements and the interactions between the constituent part under consideration and the remainder of the ATM functional system.*	This safety cases covers from initial planning to operations. Decommissioning is addressed as any other change. The MARIA model covers the whole scope of NAV Portugal ANS and ATM services and can be considered complete at each level of detail. It covers all the elements including equipment, procedures and human resources. The followed process analysis all the components including airborne, ground and special, if applicable.
3.2.2. Section 2 *The hazard identification, risk assessment and mitigation processes shall include:* *(a) a determination of the scope, boundaries and interfaces of the constituent part being considered, as well as the identification of the functions that the constituent part is to perform and the environment of operations in which it is intended to operate;* *(b) a determination of the safety objectives to be placed on the constituent part, incorporating:* *(i) an identification of ATM-related credible hazards and failure conditions, together with their combined effects;* *(ii) an assessment of the effects they may have on the safety of aircraft, as well as an assessment of the severity of those effects, using the severity classification scheme set out in Section 4;* *(iii) a determination of their tolerability, in terms of the hazard's maximum probability of occurrence, derived from the severity and the maximum probability of the hazard's effects, in a manner consistent with Section 4;* *(c) the derivation, as appropriate, of a risk mitigation strategy which:* *(i) specifies the defences to be implemented to protect against the risk-bearing hazards;* *(ii) includes, as necessary, the development of safety requirements potentially bearing on the constituent part under consideration, or other parts of the ATM functional system, or environment of operations;* *(iii) presents an assurance of its feasibility and effectiveness;*	The scope is a determined, covering the boundaries and interfaces of the constituent part being considered, as well as the identification of the functions that the constituent part is to perform and the environment of operations in which it is intended to operate. See paragraphs: • 2.1 - Change scope • 2.1.1 - Changed components • 2.1.2 - Affected units • 2.1.3 - Affected interfaces and interactions The unit FHA, done using MARIA, identifies hazards at service level by analyzing all the data flows that are output by the unit functional system. An assessment of the effects of the hazards on the safety of aircraft, as well as an assessment of the severity of those effects, is performed using the referenced severity classification scheme. The probability of occurrence of the hazard as well as the probability of the hazard's effects is documented in the unit's FHA. New hazards will only arise due to changes to the outputs of the functional system. These changes are detected by the proposed approach, in both nominal and degraded modes of operation. By following the change impact until it can be demonstrated that the impact is not propagating further, proposed approach evaluates the impact on existing hazards. See paragraphs: • 2.2 - Normal operations • 2.1.5 - Planned degraded modes For the risk mitigation strategy see paragraphs:

(d) verification that all identified safety objectives and safety requirements have been met: *(i) prior to its implementation of the change;* *(ii) during any transition phase into operational service;* *(iii) during its operational life;* *(iv) during any transition phase until decommissioning.*	• 2.2.3 - Mitigation actions for Normal Operations • 2.1.5.10 - Mitigation actions for planned degraded modes Safety objectives are not defined.
3.2.3. Section 3 *The results, associated rationales and evidence of the risk assessment and mitigation processes, including hazard identification, shall be collated and documented in a manner which ensures that:* *(a) complete arguments are established to demonstrate that the constituent part under consideration, as well as the overall ATM functional system are, and will remain tolerably safe by meeting allocated safety objectives and requirements. This shall include, as appropriate, specifications of any predictive, monitoring or survey techniques being used;* *(b) all safety requirements related to the implementation of a change are traceable to the intended operations/ functions.*	This is covered in the safety argument presented in paragraph 3 - Safety Argument.
3.2.4. Section 4 *Hazard identification and severity assessment*	A systematic identification of the hazards shall be conducted. Severities are allocated in the FHA for each unit in accordance with the referenced classification scheme. Safety objectives are not defined.
3.2.5. Section 5 *Software safety assurance system*	Covered in Safety Manual and ED153 compliance matrix.

Appendix B - Traceability to regulation 2017/373 AMC & GM

The table below provides information on how the process proposed above complies with regulation EU 2017/373 and its Accepted Means of Compliance (AMC) and Guidance Material (GM) for the requirements related to changes to a functional system, namely:

- ATM/ANS.OR.A.045 Changes to a functional system
- ATS.OR.205 Safety assessment and assurance of changes to the functional system.

Conformity assessment table

	Proposed process
ATM/ANS.OR.A.045 Changes to a functional system	The proposed approach aims at being fully compliant with ATM/ANS.OR.A.045.
AMC1 ATM/ANS.OR.A.045(a) Changes to a functional system *(b) Early and accurate notification facilitates the interactions between the provider and the competent authority and, thus, maximises the likelihood of introducing a change into service in due time according to the service provider's initial schedule when the competent authority has decided to review an assurance case. Therefore, it is advisable that the change description identified in AMC1 ATM/ANS.OR.A.045(a) is completed as soon as possible and contains the following data:* *(1) Purpose of the change;* *(2) Reasons for the change;* *(3) Place of implementation;* *(4) New/modified functions/services brought about by the change;* *(5) High-level identification of the constituents of the functional system being changed, and what is modified in their functionality;* *(6) Consequence of the change, i.e. the harmful effects of the hazards associated with the change* (f*) For air traffic services (ATS) providers, the consequences of the change specified in (b)(6), should be expressed in terms of the harmful effects of the change, i.e. the effects of the hazards associated with safety risks. These could be the result of a preliminary safety assessment, if available, or an early hazard analysis that concentrates on the service level effects.*	(1) See Justification. (2) See Justification The proposed approach supports the understanding of the change and provides the information required for notification of changes, points (3), (4) and (5), at an earlier stage. The MARIA model covers the whole scope of NAV Portugal ANS and ATM services and can be considered complete at each level of detail. To ensure that the scope of the change is completely and correctly identified, it is described by pin-pointing the elements of the MARIA model for NAV Portugal that are changed. The next step is to identify all the units that are affected by the change. This is done by checking the presence of the changed elements in the different units. In addition expert judgement is used to complement and validate the results. The impact on the specific units is made explicit and covered in the global assessment. See paragraphs: • 2.1 - Change scope • 2.1.1 - Changed components • 2.1.2 - Affected units • 2.1.3 - Affected interfaces and interactions (6) The unit FHA, done using MARIA, identifies hazards at service level by analyzing all the data flows that are output by the unit functional system. The distance between these hazards and the harmful effects is lower making it easier to associate them. As the same model is used the consequence of the change on the functional system hazards is obtained via the analysis of affected interfaces and interactions, performed in 2.1.3. The same approach can be used for both nominal and degraded modes of operation.
GM1 ATS.OR.205(a)(1) GM2 ATS.OR.205(a)(1) GM1 ATS.OR.205(a)(1)(iii) And GM4 ATM/ANS.OR.C.005(a)(1) GM6 ATM/ANS.OR.C.005(a)(1)	The proposed approach supports compliance with the listed guidance material. See paragraphs: • 2.1 - Change scope • 2.1.1 - Changed components • 2.1.2 - Affected units • 2.1.3 - Affected interfaces and interactions

ATS.OR.205 Safety assessment and assurance of changes to the functional system	The proposed approach aims at being fully compliant with ATS.OR.205
Not compliant yet: *(2) the determination and justification of the safety criteria applicable to the change in accordance with point ATS.OR.210;*	(a) The safety assessment covers the scope of the change: (i) the equipment, procedural and human elements being changed; (ii) interfaces and interactions between the elements being changed and the remainder of the functional system; (iii) interfaces and interactions between the elements being changed and the context in which it is intended to operate; (iv) the life cycle of the change from definition to operations including transition into service; (v) planned degraded modes of operation of the functional system; (b) The safety assessment comprises: (1) the identification of hazards; (3) the risk analysis of the effects related to the change; (4) the risk evaluation and, if required, risk mitigation for the change such that it can meet the applicable safety criteria; (5) the verification that: (i) the assessment corresponds to the scope of the change; (ii) the change meets the safety criteria; (6) the specification of the monitoring criteria necessary to demonstrate that the service delivered by the changed functional system will continue to meet the safety criteria.
AMC1 ATS.OR.205(b)(1) *COMPLETENESS OF HAZARD IDENTIFICATION* *The air traffic services provider should ensure that hazard identification:* *(a) targets complete coverage of any condition, event, or circumstance related to the change, which could, individually or in combination, induce a harmful effect;* *(b) has been performed by personnel trained and competent for this task; and* *(c) need only include hazards that are generally considered as credible.*	The unit FHA, done using MARIA, identifies hazards at service level by analyzing all the data flows that are output by the unit functional system. During the FHA sessions the experts assess the credibility of each hazard, As for the analysis of the change links its impact to the outputs of the system, compliance with AMC1 ATS.OR.205(b)(1) is achieved.
AMC2 ATS.OR.205(b)(1) *HAZARDS TO BE IDENTIFIED* *The following hazards should be identified:* *(a) New hazards (...)* *(b) Already existing hazards that are affected by the change and are related to:* *(1) the existing parts of the functional systems; and* *(2) hazards outside the functional system, for example, those inherent to aviation.*	New hazards will only arise due to changes to the outputs of the functional system. These changes are identified by the proposed approach, in both nominal and degraded modes of operation. By following the change impact until it can be demonstrated that the impact is not propagating further, proposed approach evaluates the impact on existing hazards. See paragraphs: • 2.2 - Normal operations • 2.1.5 - Planned degraded modes • 2.1.5.8.1 - Planned degraded modes – External hazards • 2.2.1.1.1 - Normal operations – External hazards

GM1 ATS.OR.205(b)(1) Methods to identify hazards *(2) The air traffic services provider needs to make sure that the method is appropriate for the change and produces (either individually or in combination) a valid (necessary and sufficient) set of hazards. This may be aided by drawing up a list of the functions associated with part of the functional system being changed. The air traffic services provider needs to make sure their personnel that use these techniques are appropriately trained to apply these methods and techniques.*	Fully compliant. The list of functions associated with part of the functional system being changed is systematically identified with the help of a model. The process to identify hazards is clearly defined and applied by trained staff.