

**Preliminary Safety Case for  
Enhanced Air Traffic  
Services in Non-Radar Areas  
using ADS-B surveillance  
PSC ADS-B-NRA**

<b>Edition</b>	<b>:</b>	<b>1.0</b>
<b>Edition Date</b>	<b>:</b>	<b>09 September 2008</b>
<b>Status</b>	<b>:</b>	<b>General Public</b>
<b>Class</b>	<b>:</b>	<b>Proposed Issue</b>

## DOCUMENT IDENTIFICATION SHEET

### DOCUMENT DESCRIPTION

**Document Title**

Preliminary Safety Case for Enhanced Air Traffic Services in Non-Radar Areas using ADS-B surveillance

<b>EDITION :</b> 1.0	<b>EDITION DATE :</b> 09 September 2008
----------------------	---

**Abstract**

This Preliminary Safety Case documents the results of the safety assessment and other related activities performed for the use of ADS-B-NRA (ADS-B surveillance in Non Radar Areas application). This document aims at being the basis for Safety Regulation Commission regulatory review and an input to ANSPs to produce their own local Safety Case for the ADS-B-NRA application.

**Keywords**

Preliminary Safety Case	Safety Argument	ADS-B-NRA	ADS-B
CASCADE Programme	RFG	EUROCAE ED-126	RTCA DO-303
ESARR-4	Safety Evidence	Non Radar Area	Generic Specification

<b>CONTACT PERSON:</b> Gilbert CALIGARIS	TEL: +32.2.729.33.65	<b>Business Division:</b> DAP/SUR
--	-------------------------	-----------------------------------

### DOCUMENT STATUS

STATUS	CATEGORY	CLASSIFICATION
Working Draft	Executive Task	General Public <input checked="" type="checkbox"/>
Draft	Specialist Task	EATMP <input type="checkbox"/>
Proposed Issue	Lower Layer Task	Restricted <input checked="" type="checkbox"/>
Released Issue		

### ELECTRONIC BACKUP

**INTERNAL REFERENCE NAME :** CASCADE ADS-B-NRA Preliminary Safety Case v1.0 for SRC Regulatory Review

## DOCUMENT PRODUCTION, APPROVAL, ENDORSEMENT and REVIEW

The following table identifies all management authorities who have successively produced, approved, endorsed and reviewed the present issue of this document.

DOCUMENT PRODUCTION		
Function	Name and signature	Date
Author/preparer	Gilles CALIGARIS	09 September 2008
APPROVAL		
Function	Name and signature	Date
(Document owner)	Alex WANDELS	
ENDORSEMENT		
Function	Name and signature	Date
EATM SMS Service	Gilles LE GALO	
Deputy Director ATM Programmes (DDAP)	Alexander SKONIEZKI	
SAFETY REGULATORY AUTHORITY		
Function	Name and signature	Date
Safety Regulation Commission Regulatory Review	SRC Chairman	

## DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

<b>EDITION</b>	<b>DATE</b>	<b>REASON FOR CHANGE</b>	<b>SECTIONS PAGES AFFECTED</b>
0.1	29/06/2007	First issue: Safety Argument structure.	All
0.2	12/07/2007	Modification of level 2 arguments and following ones. More information about the kind of evidence per argument is included.	All
0.3	16/07/2007	Modification based on internal discussions. More detail included specially on arguments description.	All
0.4	03/08/2007	Modifications based on internal discussions. More detail included specially on arguments description.	All
0.5	11/09/2007	More detail included specially on Evidence. Internal working review.	All
0.6	31/10/2007	Preliminary Safety Case draft version.	All
0.7	20/02/2008	Draft version addressing comments from the CASCADE PSG (Programme Steering Group) and comments from EUROCONTROL DAP/SSH	All
0.8	February 2008	Further improvements	All
0.9	February 2008	Preliminary Safety Case for ADS-B-NRA: Proposed Issue	All
1.0	August 2008	Preliminary Safety Case for ADS-B-NRA: version including comments from SRU and DAP/SSH. For SRC Regulatory Review.	All

## TABLE OF CONTENTS

EXECUTIVE SUMMARY .....	11
1 INTRODUCTION .....	13
1.1 Background .....	13
1.2 Aim .....	13
1.3 Purpose .....	14
1.4 Scope .....	14
1.5 Reference Documents .....	14
1.6 Operational Context .....	15
1.7 Document Layout .....	15
2 ADS-B-NRA APPLICATION DESCRIPTION .....	17
2.1 Operational description of the application .....	17
2.2 Description of the high level functional system .....	19
3 OVERALL SAFETY ARGUMENT .....	21
3.1 Claim .....	21
3.2 Safety Criteria .....	22
3.3 Strategy for Decomposing the Claim .....	23
3.4 Safety Specification (Arg1) .....	25
4 INTRINSIC SAFETY OF THE (GENERIC) ADS-B-NRA APPLICATION (ARG1.1.1).....	31
4.1 Safety Criteria .....	31
4.2 Strategy .....	31
4.3 Procedures and Surveillance data items (Arg1.1.1.1) .....	33
4.4 Differences between Radar and ADS-B based ATS Operations (Arg1.1.1.2).....	38
4.5 Performance Characteristics (Arg1.1.1.3) .....	43
4.6 Impact on Adjacent Sectors (Arg1.1.1.4).....	47
4.7 Conclusions on Arg1.1.1 - Intrinsic Safety of the Application .....	48
5 DESIGN COMPLETENESS FOR ADS-B-NRA (ARG1.1.2) .....	49
5.1 Safety Criteria .....	49
5.2 Strategy .....	49
5.3 ADS-B System Boundaries and Functions (Arg1.1.2.1) .....	50
5.4 Description of ADS-B-NRA Operations (Arg1.1.2.2) .....	51
5.5 ADS-B NRA Safety Requirements Arg1.1.2.3).....	52

5.6	External Elements (Arg1.1.2.4).....	63
5.7	Conclusions on Arg1.1.2 - Design Completeness .....	66
6	ADS-B-NRA DESIGN CORRECTNESS (ARG1.1.3).....	67
6.1	Safety Criteria .....	67
6.2	Strategy .....	67
6.3	Coherency of the ADS-B-NRA Procedures (Arg1.1.3.1) .....	68
6.4	Coherency of the ADS-B-NRA Human Actions (Arg1.1.3.2) .....	69
6.5	Coherency of the ADS-B-NRA Data (Arg1.1.3.3).....	69
6.6	Absence of Undefined States in ADS-B-NRA (Arg1.1.3.4).....	71
6.7	Conclusions on Arg1.1.3 - Design Correctness.....	71
7	DESIGN ROBUSTNESS (ARG1.1.4).....	73
7.1	Safety Criteria .....	73
7.2	Strategy .....	73
7.3	Reaction to External Failures (Arg1.1.4.1).....	74
7.4	Reaction to Abnormal External Conditions (Arg1.1.4.2) .....	77
7.5	Conclusions on Arg1.1.4 - Design Robustness .....	79
8	MITIGATION OF INTERNAL FAILURES (ARG1.1.5).....	81
8.1	Safety Criteria .....	81
8.2	Strategy .....	81
8.3	Hazards Identification (Arg1.1.5.1) .....	84
8.4	Hazards Assessment and Severity Assignment (Arg1.1.5.2) .....	87
8.5	Determination of Safety Objectives (Arg1.1.5.3) .....	98
8.6	Hazards Causes Identification and internal mitigation MEans (Arg1.1.5.4).....	103
8.7	Safety Requirements and Assumptions (Arg1.1.5.5).....	105
8.8	Conclusions on Arg1.1.5 - Internal Failures.....	112
9	REALISM OF ALL REQUIREMENTS AND ASSUMPTIONS (ARG1.1.6) .....	113
9.1	Strategy .....	113
9.2	Validation of Specification Requirements .....	113
10	APPROACH USED FOR THE SPECIFICATION (ARG1.1.7).....	115
10.1	Strategy .....	115
10.2	Approach and Methods for Specification .....	115
11	ASSUMPTIONS, ISSUES AND LIMITATIONS .....	117
11.1	Assumptions .....	117

11.2	Outstanding Safety Issues.....	123
11.3	Limitations.....	123
12	CONCLUSIONS .....	125
13	REFERENCES: .....	127
14	GLOSSARY .....	129
ANNEX A	HAZARD CLASSIFICATION MATRIX.....	131
ANNEX B	ORGANISATIONS INVOLVED IN SPECIFICATION OF ADS-B-NRA.....	133
ANNEX C	COMPARISON BETWEEN ADS-B-NRA AND RADAR CASES W.R.T. COORDINATION AND TRANSFER.....	134
ANNEX D	GOAL STRUCTURING NOTATION LEGEND .....	137
ANNEX E	SUMMARY OF THE MONTE-CARLO ANALYSIS SUPPORTING THE CALCULATION OF THE PE VALUES FOR HAZARDS OH3 AND OH4 – UNDETECTED CASES .....	139

## TABLE OF TABLES

Table 1: Required technical surveillance data items (in input to ground ATC processing) ...	35
Table 2: Surveillance Functions .....	37
Table 3: Reference Radar Performance Parameters .....	44
Table 4: ADS-B Performance Parameters .....	46
Table 5: Performance on Aircraft Vertical Position.....	47
Table 6: ADS-B NRA Phases of Operation .....	52
Table 7: Safety Requirements on ATS Procedures for ADS-B-NRA.....	53
Table 8: Safety Requirements on ADS-B-NRA data items at ATCo Interface .....	54
Table 9: Safety Requirements on ADS-B-NRA data items ATC Processing system input ...	55
Table 10: Safety Requirements on data items at Airborne Domain output level.....	56
Table 11: Safety Requirements at ATC Processing system level .....	57
Table 12: Safety Requirements at ADS-B Receiver subsystem level .....	59
Table 13: Safety Requirements at Aircraft Domain level.....	62
Table 14 : ADS-B-NRA Hazards list.....	85
Table 15 : Safety Requirements and Assumptions relating to Environmental Conditions.....	89
Table 16 : Safety Requirements and Assumptions relating to External Mitigation Means .....	89
Table 17 : ADS-B-NRA Hazards Effects, Severity, Pe and EMM & EC .....	97
Table 18 : Risk Classification Scheme and apportionment for ADS-B-NRA .....	99
Table 19 : SO for hazards OH1 to OH4.....	102
Table 20 : Internal Mitigation Means list.....	105
Table 21 : Safety Requirements related to hazards causes.....	107
Table 22 : Assumptions related to hazards causes.....	108
Table 23 : Safety Objectives versus Top event results .....	111



Table 24 : Compliance with ESARR4 section 5 ..... 116

### TABLE OF FIGURES

Figure 1: System Functional Description..... 19

Figure 2: Overall Safety Argument ..... 21

Figure 3: Decomposition of Argument 1 ..... 25

Figure 4: Decomposition of Generic Specification Argument (Arg1.1) ..... 27

Figure 5: Decomposition of Argument on Intrinsic Safety (Arg1.1.1) ..... 32

Figure 6: Decomposition of Argument on Design Completeness (Arg1.1.2)..... 50

Figure 7: Decomposition of Argument on Design Correctness (Arg1.1.3) ..... 68

Figure 8: Decomposition of Argument on Design Robustness (Arg1.1.4)..... 74

Figure 9: Decomposition of Argument on Internal Failures Mitigation (Arg1.1.5)..... 83

Figure 10: Functional System description for ADS-B-NRA ..... 103

Figure 11: Realism of requirements and assumptions (Arg1.1.6) ..... 113

Figure 12: Approach and Methodology used (Arg1.1.7)..... 115

Figure 13: Monte Carlo Scenario Definitions..... 141

Figure 14 Example Trajectory for Monte-Carlo Model (Based on Scenario C-1)..... 141

**Page intentionally left blank**

## EXECUTIVE SUMMARY

Part of the EUROCONTROL CASCADE Programme, the ADS-B-NRA application is designed to support and enhance Air Traffic Services (ATS) in both En-route and TMA airspaces in Non-Radar Areas (NRA). This application is expected to provide benefits to capacity, efficiency and safety in a way similar to what would be achieved by use of SSR radar where it is not in use today.

EUROCAE ED-126/RTCA DO-303 joint standard [Ref.1] provides the minimum operational, safety and performance requirements (SPR) and interoperability requirements (INTEROP) for the implementation of this application.

The purpose of this Preliminary Safety Case (PSC) is to document the results of this assessment, as well as results from some other standards and related activities, as a basis for Safety Regulation Commission regulatory review and as input to ANSPs to produce their own, local safety cases.

This Safety Case is preliminary in that it addresses only the specification stage of the Application. It does not include local specification, implementation or security issues, although the structure of the Safety Argument presented herein does include a high-level framework for the development of assurance relating to the implementation, transition and in-service stages of the safety lifecycle.

The principal Argument addressed herein is that using ADS-B surveillance in Non-Radar Areas for ATS has been specified to be *acceptably safe*, in particular for a given set of separation minima. The safety criteria used are a) comparison with a radar-based ATS operation in the nominal mode of operation and b) a relevant target level of safety (compliant with ESARR4) in the non nominal mode of operation (failure case). In addressing this Argument, Evidence has been presented to show, for a generic level of specification, that:

- The application underlying ADS-B surveillance in NRA is intrinsically safe.
- The design of the system which underlies the Application is complete and correct.
- The system design functions correctly and coherently under all normal environmental conditions.
- The system design is robust against external abnormalities in the operational environment.
- All risks from internal system failure have been mitigated sufficiently.
- The requirements and assumptions obtained for the application specification are realistic
- The approach and methodology used on the safety assessment are adequate to show that the application is acceptably safe, and were applied by competent personnel.

Thus, subject to certain caveats presented in section 11 it is concluded overall that ADS-B surveillance in Non-Radar Areas for ATS has been specified to be *acceptably safe*.

## **1 INTRODUCTION**

### **1.1 BACKGROUND**

The ADS-B-NRA application is designed to support and enhance Air Traffic Services in both En-route and TMA airspaces which are currently without radar surveillance (Non-Radar Areas -NRA) by ADS-B as sole surveillance means.

The introduction of ADS-B in Non-Radar Areas will provide enhancements to these services (compared to current capabilities) in a way similar to the introduction of secondary surveillance radar (SSR). In particular, the Air Traffic Control Service will be enhanced by providing controllers with improved surveillance of aircraft positions that will result in the use of separation standards similar to that of radar. The target environment to be considered for this application is low traffic density as a first step; but more stringent provisions have been made in this assessment of ADS-B-NRA that are consistent with areas of greater density.

This application is expected to provide benefits to capacity, efficiency and safety in a way similar to what would be achieved by use of SSR radar where it is not in use today.

### **1.2 AIM**

The aim of this Preliminary Safety Case is to demonstrate that using ADS-B surveillance to support Air Traffic Services (ATS), including the prevention of collisions through the application of appropriate separation minima, in both en-route and TMA airspace, for a given separation minima set, has been specified to be acceptably safe.

For the purpose of this report, “acceptably safe” is defined as the risk of an accident being:

Cr001 No higher under the operation of the ADS-B-NRA application than for reference current operations (radar-based surveillance),

Cr002 Within an appropriate portion of the relevant safety target, and

Cr003 Reduced as far as reasonably practicable.

The safety criteria comparing ADS-B-based and radar-based ATS operations (Cr001) is mainly used in the nominal mode of operation (success case), and the safety criteria addressing a relevant target level of safety (compliant with ESARR-4) (Cr002) is mainly used in the non nominal mode of operation (failure case). More detail on the combination of these three criteria is provided case by case in the document.

### 1.3 PURPOSE

As a means of supporting European Air Navigation Service Providers (ANSPs) in optimising their implementation of ADS-B NRA operations, several standards and procedures have been developed.

The purpose of this Preliminary Safety Case is to document the results of these activities as a basis for Safety Regulation Commission regulatory review, and as input to the ANSPs to produce their own, local full safety cases in accordance with the requirements of the local regulator.

### 1.4 SCOPE

This Safety Case is preliminary in that it addresses only the specification stage of the application, and more precisely, the generic aspects of the specification (I001).

It does not include either local aspects of the specification or implementation issues, although the structure of the Safety Argument presented herein does include a high-level framework for the development of assurance relating to the local specification, implementation, transition and in-service stages of the safety lifecycle (I002).

Note: each issue identified throughout this document is labelled "Ixxx" and is dealt with in section 11.2 ("Outstanding Safety Issues").

Security issues are out of scope of this document.

Note: the information presented in this Preliminary Safety Case has been in some cases adapted and summarized from its original form in order to obtain a coherent and simplified document. The original text is available through the corresponding references (mainly from ED-126/DO-303 [Ref.1] standard).

### 1.5 REFERENCE DOCUMENTS

This Preliminary Safety Case refers largely to the Performance, Safety and Interoperability constituents from EUROCAE ED-126 / RTCA DO-303 document [Ref.1]. This joint standard provides a description of the ADS-B-NRA application, the generic environment in which it will operate, the corresponding safety and performance assessments and requirements together with interoperability and other related requirements.

This joint standard has been developed by the Requirement Focus Group - RFG. This working group consists of members from FAA, RTCA, EUROCONTROL and EUROCAE with participation of AirServices Australia and Japan, providing technical and operational expertise to RFG activities.

Other results from additional related activities (e.g. ICAO documents, EASA reference documents, other standards, other CASCADE Programme work) have also been used and referred to in this Preliminary Safety Case.

## 1.6 OPERATIONAL CONTEXT

The ADS-B-NRA application will provide enhanced Air Traffic Services in areas where radar surveillance currently does not exist (areas where ADS-B and radar will provide overlapping coverage are covered by the “ADS-B-RAD” application<sup>1</sup>).

Examples are remote, off-shore, oil rig and small island environments, which, due to traffic levels, location, or equipment cost cannot justify the installation of radar. Another example is areas where existing radar is to be decommissioned and the replacement costs are not justified.

Currently, Air Traffic Services within Non-Radar Areas employ procedural separation methods. The intention of the ADS-B-NRA application is to allow the separation procedures using radar surveillance to be enabled by ADS-B (including 3 and 5 Nm separation service), on the basis that the quality of service of ADS-B surveillance is similar to (or better than) SSR radar and that appropriate (VHF) air-ground communications coverage is available.

**GM001.** At the time of the edition of this document, ICAO does not consider separation minima lower than 5Nm when using ADS-B. Implementers shall check the status of this regulation in order to determine the separation minima to be locally applied.

**(Note:** Proposed Guidance is directly included in the corresponding sections of this document in the form of Guidance Material Boxes as shown for GM001. See section 3.4.2 for more information concerning these Guidance Material Boxes).

Hence, in terms of capacity, efficiency and safety<sup>2</sup> the potential benefits provided by this Application are expected to be similar to what would be achieved by the introduction of SSR radar. See section 3.1 for capacity, efficiency and safety benefits.

Further details on the scope of the Application are given in section 2.

## 1.7 DOCUMENT LAYOUT

**Section 2** provides an operational description of the system addressed in this Preliminary Safety Case, i.e. the ADS-B-NRA application.

**Section 3** presents a complete, high-level Safety Argument (Arg0), covering the whole safety lifecycle, in order to provide a framework for the development of a full Safety Case by individual ANSPs. The Safety Argument (Arg1)

---

<sup>1</sup> ADS-B-RAD application covers the provision of ATS in areas where both ADS-B and radar surveillance exist in tandem.

<sup>2</sup> Note that this Preliminary Safety Case does not claim that safety will actually improve with ADS-B in NRA – rather that it will be no less safe than would be the situation if a conventional radar-based ATS service were introduced into NRA

relating to the main subject of this Preliminary Safety Case (i.e. the specification of Requirements for the Concept) is decomposed to a further level in Section 3, as a lead-in to the subsequent sections of the document.

**Sections 4 to 10**, respectively, take each of the immediate sub-Arguments of Arg1 in turn and present assurance (i.e. lower-level Arguments, together with supporting Evidence) to show that each of these sub-Arguments is valid.

**Section 11** presents the caveats (i.e. assumptions, operational limitations, and outstanding safety issues) associated with the safety assessment on which this Preliminary Safety Case is based.

**Section 12** then provides overall conclusions concerning the safety of the (generic) specifications of the ADS-B surveillance in NRA application, subject to the caveats presented in section 11.

Document references and a glossary are provided in **sections 13 and 14** respectively.

**Annex A** presents the hazard classification matrix used for sub-Argument presented in section 8 concerning the mitigation of internal failures.

**Annex B** lists the organisations involved in the specification of the ADS-B-NRA application.

**Annex C** provides a comparison between ADS-B-NRA and radar cases w.r.t. coordination and transfer

**Annex D** provides the Goal Structuring Notation (GSN) legend, i.e. the symbology used to represent Safety Arguments links and Preliminary Safety Case structure.

**Annex E** provides a summary of the Monte-Carlo Analysis supporting the calculation of the Pe values for hazards OH3 and OH4 – undetected cases



## 2 ADS-B-NRA APPLICATION DESCRIPTION

### 2.1 OPERATIONAL DESCRIPTION OF THE APPLICATION

The operational context and scope of the application is described in ED-126/DO-303 [Ref.1] §1.2.1.3 and §A.3 using reference to the relevant ICAO Doc 4444 amendments for ADS-B [Ref.2].

The following extract from ED-126/DO-303 illustrates the concept of operation for ADS-B-NRA:

*“The ADS-B-NRA application will provide enhanced Air Traffic Services in areas where radar surveillance currently does not exist.*

*Examples of environments which might be candidates for the ADS-B-NRA application include remote off-shore, oil rig and small island environments. Further, areas now under radar coverage might determine a business case for introducing ADS-B instead of replacing ageing radar systems.*

*The ADS-B-NRA application is designed to enhance the following ICAO Air Traffic Services (refer to PANS-ATM Doc 4444 [Ref.2]):*

*a. Air Traffic Control Service and Flight Information Service principally for:*

- Air Traffic control separation services*
- Transfer of responsibility for control*
- Air Traffic control clearances*
- Flight Information services*

*b. Alerting services, principally for:*

- Notification of rescue co-ordination centres*
- Plotting aircraft in a state of emergency*

*c. [Air Traffic Advisory Services (including avoidance advice)]*

*[...] In particular, the Air Traffic Control Service will be enhanced by providing controllers with improved situational awareness of aircraft positions and the possibility of applying separation minima equivalent to radar separation minima [5NM and 3NM], rather than minima used with procedural separation. The Alerting Service will be enhanced by more accurate information on the latest position of aircraft.*

*It is expected that this application will provide benefits to capacity and safety in a way similar to what would be achieved by use of SSR radar where it is not in use today. [...]* “

Direct Controller Pilot communications (VHF) and an adequate navigation infrastructure will be necessary to support this application<sup>3</sup>.

The question of airborne ADS-B equipage rates associated with the implementation of NRA is an important one for the safety case. This issue can be solved at the local/regional level through various methods from mandating airborne equipage, segregating airspace between equipped/certified and the rest of the traffic or permitting controllers to tactically manage a mixed equipage environment. It is recognized however that the objective in many regions will be to have all aircraft equipped and certified to maximize benefits.

*“The responsibilities of the controller and pilot remain unchanged compared to the radar-based ATS. Compared to the current procedural environment, there may be changes in procedure with the introduction of surveillance services [leading to a potential increase of controller and pilot workload]. On the other hand, there may be some reduction in workload due to, inter alia, a simplification of the separation standards expected to be used within the target ADS-B environment as well as reduced need for voice position reports, since the aircraft parameters will be broadcast and received automatically via ADS-B [...].”*

With respect to adjacent sectors, specific procedures similar to those described in PANS-ATM may be applied [Ref.2] Chapters 8 (“ATS Surveillance Services”) and Chapter 10 “Coordination In Respect Of The Provision Of ATC Service” (as indicated in §Table 10 from [Ref.1]):

- For transfer of control (§8.7.4. (“Transfer Of Control”) of [Ref.2])
- Separation minima (to establish appropriate procedural separation if next sector applies procedural control).

*“The ADS-B-NRA application is designed for use in airspace classes A to E and complies with ATC procedures detailed in PANS-ATMP Doc 4444 [Ref.2].”*

As mentioned in section 1.1, the target environment to be considered in a first period is low traffic density. But some provisions have been made in the assessment to ensure that the system will remain safe even with some more stringent figures. The higher typical traffic conditions considered for the ADS-B-NRA airspace are (see ED-126/DO-303 [Ref.1] §Annex A):

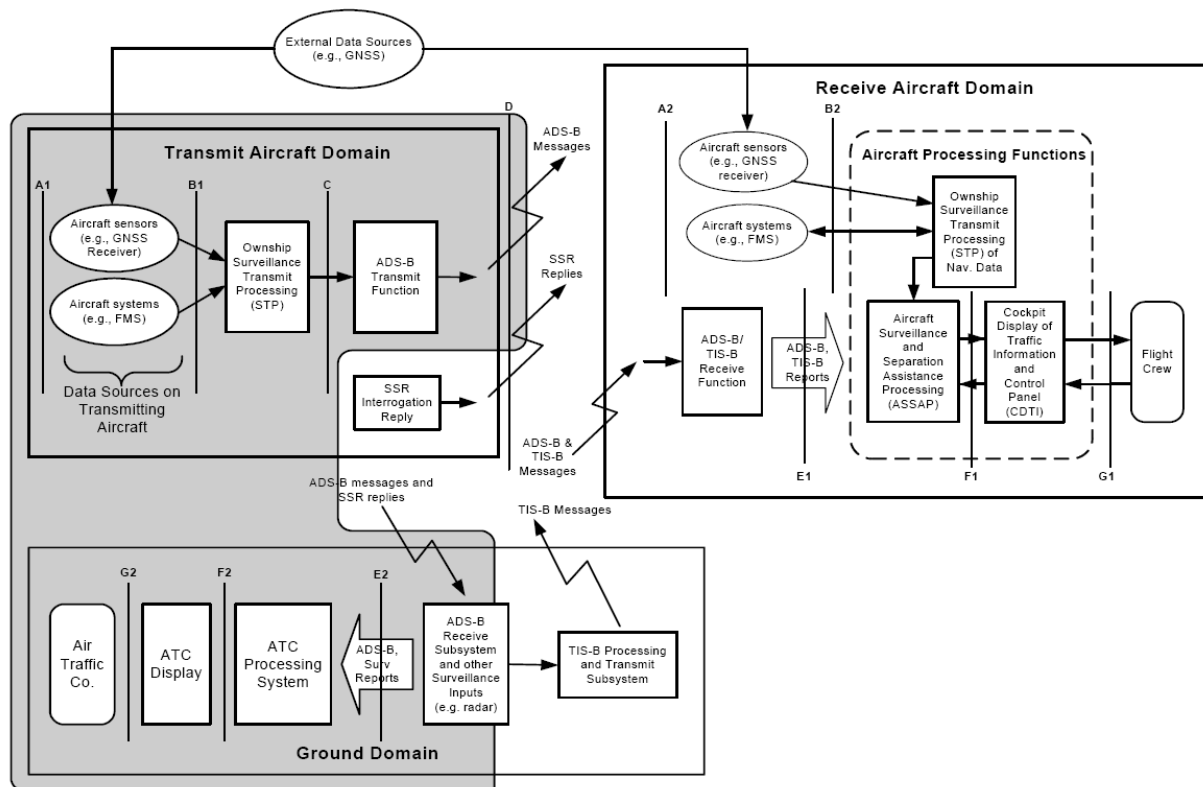
- Average duration of a flight within a single ATC sector: 20 minutes for en-route and 6 minutes for TMA,
- Average number of aircraft managed per ATSU hour: 30 en-route and 10 in TMA,
- Maximum instantaneous count of traffic: 15 aircraft en-route and 7 aircraft for TMA at any one time.

---

<sup>3</sup> In order to cover the possibility of ADS-B failure it will be necessary to retain the existing navigational air infrastructure

## 2.2 DESCRIPTION OF THE HIGH LEVEL FUNCTIONAL SYSTEM

Technical boundaries related to the ADS-B system aspects are illustrated below with Figure 1 representing a functional outline of the system necessary to support the ADS-B-NRA application (§Figure 6 from [Ref.1] ).



**Figure 1: System Functional Description**

The shaded area illustrates the relevant parts to the ADS-B-NRA application for which requirements are identified in section 5.5, i.e. the “Transmit Aircraft Domain” and “Ground Domain”.

The various “points of measurement” indicated in this Figure 1 (e.g. D, E2, G2) will be used throughout the PSC ADS-B-NRA document in order to clearly indicate to which part of the functional system the different results apply (performance values, requirements, etc.).

A part from those functions presented in previous Figure 1, ground-air VHF communication is also available for controller and pilot (as indicated in §A.3.5.3 from [Ref.1]).

More detail on identified functions is included in section 5.3.

**Page intentionally left blank**

### 3 OVERALL SAFETY ARGUMENT

A high-level view of the safety argument structure is presented, in the form of Goal-Structuring Notation (GSN)<sup>4</sup>, in Figure 1 below.

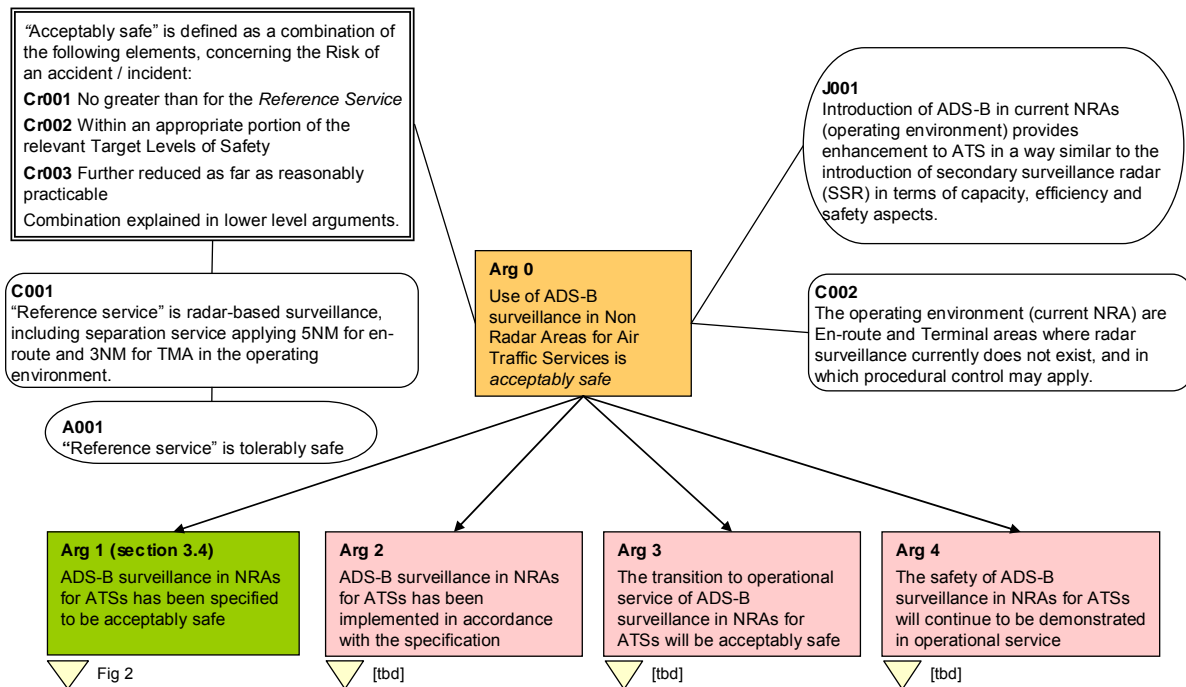


Figure 2: Overall Safety Argument

#### 3.1 CLAIM

The Safety Argument starts with the top-level Claim (**Arg0**) that using ADS-B surveillance in Non Radar Areas for Air Traffic Services is *acceptably safe*.

As indicated in section 1.1 above, the justification (**J001**) for introducing ADS-B surveillance in Non-Radar Areas is that it will provide enhancements to ATS - compared to current capabilities - in a way similar to the introduction of secondary surveillance radar (SSR), in terms of Capacity, Efficiency and Safety. The most important Safety, Capacity and Efficiency benefits in the context of this Preliminary Safety Case are provided in the next paragraph (a more comprehensive list is provided in §A.3.3 of [Ref.1]):

<sup>4</sup> A guide to GSN symbology is given in Annex A

Safety Benefits:

- *Improve controller situational awareness providing controllers with improved recognition (detection) of potentially unsafe situations*
- *Reduce workload associated with conflict resolution*
- *More precise traffic information issued to flight crews reducing visual acquisition time and failure rates.*
- *[...]*

Capacity and efficiency Benefits:

- *Reduce pilot position reports resulting in reduced communications congestion and in increased sector capacity*
- *Enabler to more efficient traffic flow through a combination of accurate position information and a reduction in separation minima (compared to procedural)*
- *[...]*

**Arg0** is made within the context (**C002**) of En-route and Terminal Areas where radar surveillance currently does not exist. Further details on the scope, the operational context and the typical traffic conditions are given in section 2.

## 3.2 SAFETY CRITERIA

The main safety criteria are that the risk of an accident or incident arising from the use of ADS-B surveillance in NRA shall be:

- Cr001.** No higher than the equivalent risk associated with “reference service” – i.e. radar-based surveillance, including separation service provided by ATS (for the given set of separation minima).
- Cr002.** Within an appropriate portion of the relevant Target Levels of Safety.
- Cr003.** Reduced as far as reasonably practicable<sup>5</sup>.

The way in which these criteria are combined is explained in the lower-level arguments detail below.

For Safety Criterion Cr001, it is assumed that:

**A001.** Reference service (i.e. radar-based surveillance as defined in ICAO PANS-ATM Doc4444 [Ref.2] - (C001)) is tolerably safe.

---

<sup>5</sup> This is also a general obligation placed on ANSPs by ESARR 3 [Ref.6].

A001 is based on years of experience using radar based ATS. However as no ESARR4 compliant Safety Assessment has been conducted for radar-based ATS, it cannot be claimed for the reference radar service to be “acceptably safe” but rather “tolerably<sup>6</sup> safe”

Taking into account that:

**C001** Reference service is radar-based surveillance, including separation service applying 5NM for en-route and 3NM for TMA in the operating environment.

**GM002.** Implementers shall ensure that their reference service to compare with is safe and that the expected capacity and efficiency benefits are still valid in their local case.

**(Note:** Proposed Guidance is directly included in the corresponding sections of this document in the form of Guidance Material Boxes as shown for GM001. See section 3.4.2 for more information concerning these Guidance Material Boxes).

### 3.3 STRATEGY FOR DECOMPOSING THE CLAIM

The Claim is decomposed into four principal Safety Arguments, using the Goal Structuring Notation (GSN) convention that an Argument can be considered to be true, if (and only if) each of its immediate ‘offspring’ can be shown to be true.

These four Arguments provide a potential framework for the development of a full Safety Case, as will have to be produced prior to bring ADS-B surveillance into operational service in Non-Radar Areas<sup>7</sup>. However, for the purposes of this Preliminary Safety Case only generic part of Arg1 is covered in any detail.

**Arg1** asserts that the use of ADS-B surveillance in NRA application has been specified to be *acceptably safe*. Corresponding Evidence is largely based on the EUROCAE ED-126/RTCA DO-303 joint standard document [Ref.1], that includes comprehensive, *a priori*, performance and safety<sup>8</sup> assessments. Additional elements from ICAO, EASA and the EUROCONTROL CASCADE Programme are considered as well as Evidence in support to Arg1. Local evidence will have to be added to complement all the generic evidence mentioned above as a result of a local Functional Hazards Assessment (FHA) / Preliminary System Safety Assessment (PSSA). This Argument is the main

---

<sup>6</sup> The notion of “tolerably safe” is also used in the context of ED-125 – Guidance to specify an ATM Risk Classification Scheme “Tolerable risk” defines the target risk for a National Regulator as defined in their Risk Classification Scheme (RCS) versus “acceptable risk” that defines the target risk for an ATMSP as defined in their Risk Classification Scheme (RCS). Acceptable risk is more demanding than tolerable risk.

<sup>7</sup> Except for Arg.4 which will apply after bringing ADS-B-NRA into operational service

<sup>8</sup> Carried out in accordance with section 5 of ESARR4 [Ref.5] (see section 10.2 for more detail)

subject of this Preliminary Safety Case and is discussed further in section 3.4 below.

**Arg2** asserts that the Application has been implemented in accordance with the specification (derived under Arg1). This Argument would be supported by the results of a full System Safety Assessment (SSA), to be carried out by the responsible ANSP.

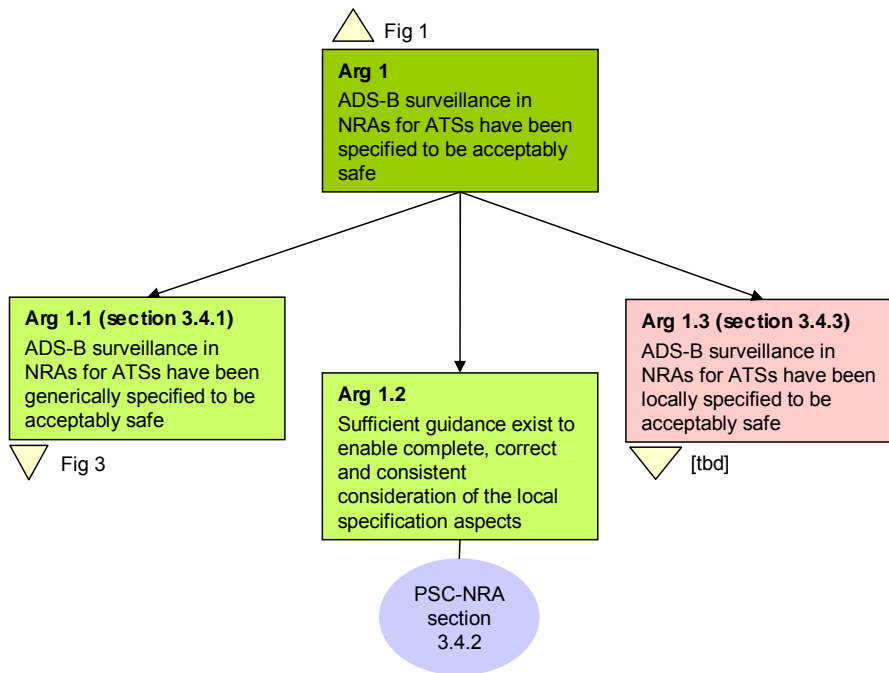
**Arg3** asserts that the transition to operational service of the Application will be *acceptably safe*. This Argument requires Evidence that all final preparations for operational service have been completed. Again this Argument would be supported by the results of a full System Safety Assessment (SSA), and it is also the responsibility of the relevant ANSP.

**Arg4** asserts that the Application will continue to be shown to be acceptably safe in operational service. It is important for the relevant ANSP to monitor operational safety, for two reasons: firstly, to validate the conclusions of the *a priori* safety assessment (Arg1); and, secondly, to ensure that any problems that might arise in operational service are properly investigated and the appropriate corrective action taken. As in two previous arguments, this one also would be supported by the results of a full System Safety Assessment (SSA).



### 3.4 SAFETY SPECIFICATION (ARG1)

The decomposition of Arg1 is shown in Figure 3 below. It comprises the following three sub-Arguments which reflect the generic and local part of the specification of the application, as well as the guidance available concerning this argument.



**Figure 3: Decomposition of Argument 1**

These sub-arguments are addressed in more detail in the next sections.

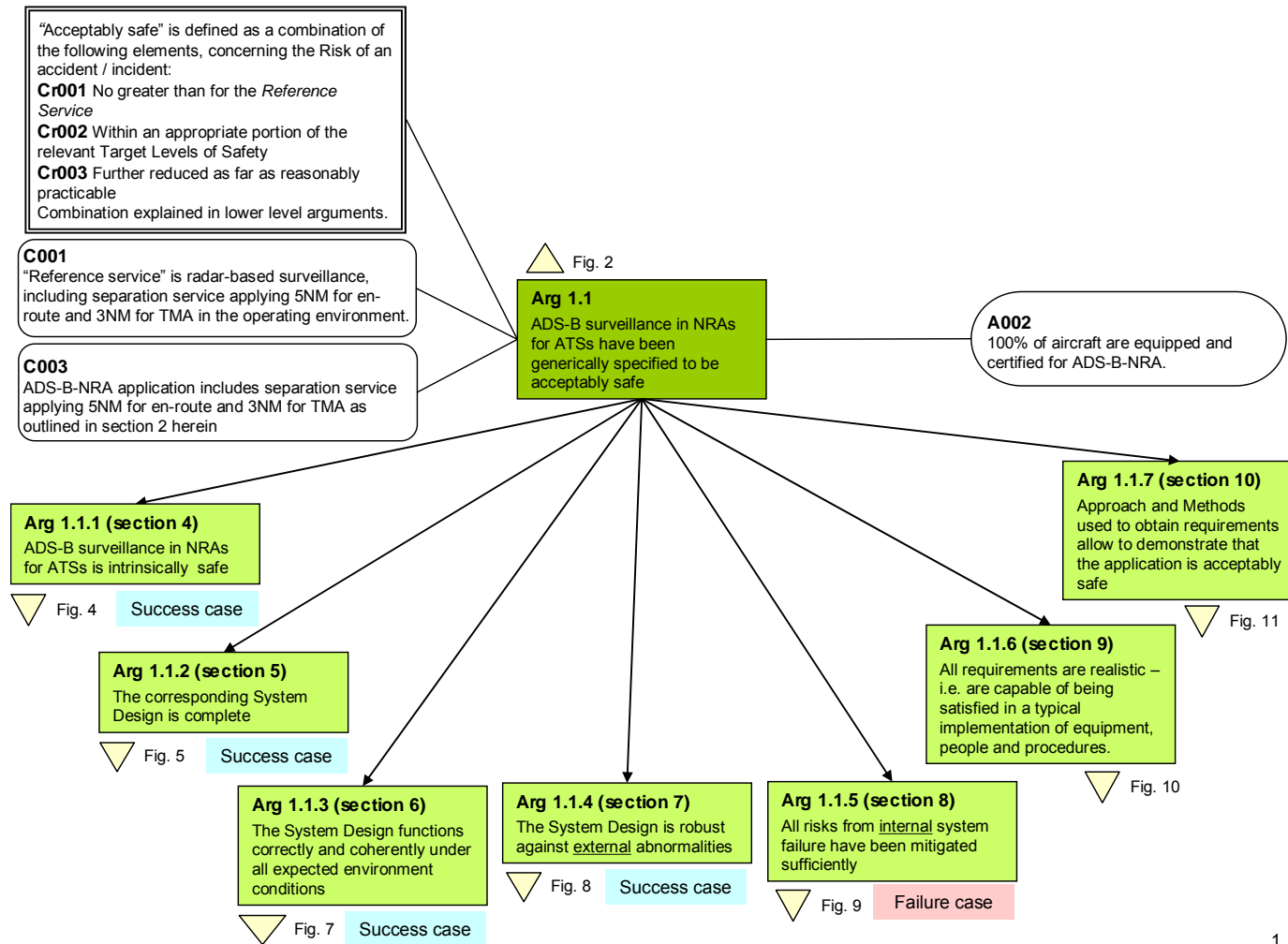
### 3.4.1 Generic<sup>9</sup> Specification (Arg1.1)

The decomposition of **Arg1.1** is shown in Figure 4 below. It comprises the following seven sub-Arguments which reflect the *Success* and *Failure* approaches to safety assessment defined in the EUROCONTROL ANS Safety Assessment Methodology [Ref.4] (SAM)<sup>10</sup> corresponding to the generic part of the application specification.

---

<sup>9</sup> For local specification see section 3.4.3

<sup>10</sup> In practice, the distinction between the *success* and *failure* approaches, and which sub-Argument belongs to which approach is not important – what is crucial is ensuring overall that everything required by the seven sub-Arguments is covered.



**Figure 4: Decomposition of Generic Specification Argument (Arg1.1)**

For this generic part, the specification of ADS-B-NRA has been done assuming that:

**A002.** 100% of aircraft are equipped and certified for ADS-B-NRA

**GM003.** As explicitly stated in ED126/DO303 ([Ref.1], section 3.4.4 of its Annex A), partial equipage issues are, in particular, left open for decision at local implementation level (through e.g. mandating airborne equipage or segregating airspace between equipped and certified and the rest of the traffic or permitting controllers to tactically manage a mixed equipage environment) . Implementers shall assess the safety impact of their choice regarding the management of the mixed equipage environment.

**(Note:** See section 3.4.2 for more information concerning Guidance Material Boxes)

### **Arg1.1.1 - Intrinsic Safety of the Application**

Arg1.1.1 asserts that the ADS-B-NRA (generic) application is intrinsically safe, for the given set of separation minima as outlined in section 2 above (C003) – i.e. that the Application is capable of satisfying the safety criteria, assuming that a suitable system design could be produced and implemented – and what are the parameters that make it so.

### **Arg1.1.2 - Design Completeness**

Arg1.1.2 asserts that the design of the system which underlies the ADS-B-NRA (generic) application is complete and correct. The objective here is to show that requirements have been specified to cover all elements, in terms of the system design, that are necessary to implement the (generic) ADS-B-NRA application in the “success case” – i.e. in the absence of failure.

### **Arg1.1.3 - Design Correctness**

Arg1.1.3 asserts that the system design underlying the (generic) ADS-B-NRA application functions correctly and coherently under all normal<sup>11</sup> environmental conditions. The main issues here are the internal coherency of the system, and the dynamic behaviour of the system, over the full range of conditions to which the system is expected to be subjected in its operational environment.

### **Arg1.1.4 - Design Robustness**

Arg1.1.4 asserts that the system design underlying the (generic) ADS-B-NRA application is robust against external abnormalities in the operational environment, from two perspectives: can the system continue to operate

---

<sup>11</sup> Abnormal conditions are addressed under Arg1.1.4. The distinction between *normal* and *abnormal* is not important provided all issues are addressed by the two sub-Arguments.

effectively; and could such conditions cause the system to behave in a way that could actually induce a risk that would otherwise not have arisen?

#### **Arg1.1.5 - Mitigation of Internal Failures**

Arg1.1.5 asserts that all risks from system failure internal to the (generic) ADS-B-NRA application have been mitigated sufficiently. Here, the internal behaviour of the system is assessed from the perspective of how anomalous behaviour of the system could induce a risk that would otherwise not have arisen.

#### **Arg1.1.6 - Realism of requirements**

Arg1.1.6 asserts that all requirements allocated to each domain or sub-system (and assumptions) are realistic - i.e. are capable of being satisfied in a typical implementation involving equipment, people and procedures.

#### **Arg1.1.7 - Approach and methodology**

Arg1.1.7 asserts that the approach and methodology used to obtain all requirements specifying ADS-B-NRA are adequate to show that the application is acceptably safe, and were applied by competent personnel.

The further decomposition of, and Evidence to support, Arg1.1.1 to Arg1.1.7 is presented below in sections 4, 10 and in Annex B respectively.

### **3.4.2 Guidance Material for specification aspects (Arg1.2)**

**Arg1.2** purpose is to ensure that the means of facilitating an ANSP's task relating to local specification exist - e.g. in the form of providing guidance on which are the generic specification issues that need to be reviewed and reconsidered for local implementation.

Proposed Guidance is directly included in the corresponding sections of this document in the form of Guidance Material Boxes as shown here after:

#### **Guidance Material**

**GM000.** Proposed Guidance to implementers is directly included in the corresponding sections of this document in the form of Guidance Material Boxes as this one.

Note: proposed guidance boxes generally use the term "implementer" as the authority responsible for development of the local safety case.

### 3.4.3 Local Specification (Arg1.3)

**Arg1.3** corresponds to the sub-argument related to the local specification of the ADS-B-NRA application, in accordance with, for example, the guidance referred to under Arg1.2. This Argument will have to be supported by local evidence (e.g. impact assessment of the local environment in which the application is going to be used) performed prior to the local implementation of the Application.

As indicated above in section 1.4, this argument Arg1.3 is not further developed in the frame of this Preliminary Safety Case.

**GM004.** To develop this argument Arg1.3, it is proposed to use the same decomposition used for Arg1.1 (see section 3.4.1) by focusing on differences between generic and local specification. The same structure as for this current Preliminary Safety Case (PSC) can also be adapted for the local (full) PSC, providing references to the generic PSC document when necessary.

**GM005.** For developing evidences that will support argument Arg1.3, ED126/DO303 [Ref.1] methodology approach or other ESARR4 [Ref.5] compliant method shall be used.

## 4           **INTRINSIC SAFETY OF THE (GENERIC) ADS-B-NRA APPLICATION (ARG1.1.1)**

The objectives of this section are to show that the (generic) ADS-B-NRA application is capable of satisfying the safety criteria (see 4.1 below), assuming that a suitable system design could be produced and implemented.

### 4.1           **SAFETY CRITERIA**

The Safety Criterion considered for this argument Arg1.1.1 is the combination of main Safety Criteria Cr001 and Cr003 (*Success Case*), i.e.:

Cr001 No higher than the equivalent risk associated with “reference service” – i.e. radar-based surveillance, including separation service provided by ATS (for the given set of separation minima).

Cr003 Reduced as far as reasonably practicable.

### 4.2           **STRATEGY**

The strategy to demonstrate the intrinsic safety of the (generic) ADS-B-NRA (Arg 1.1.1.) is based on:

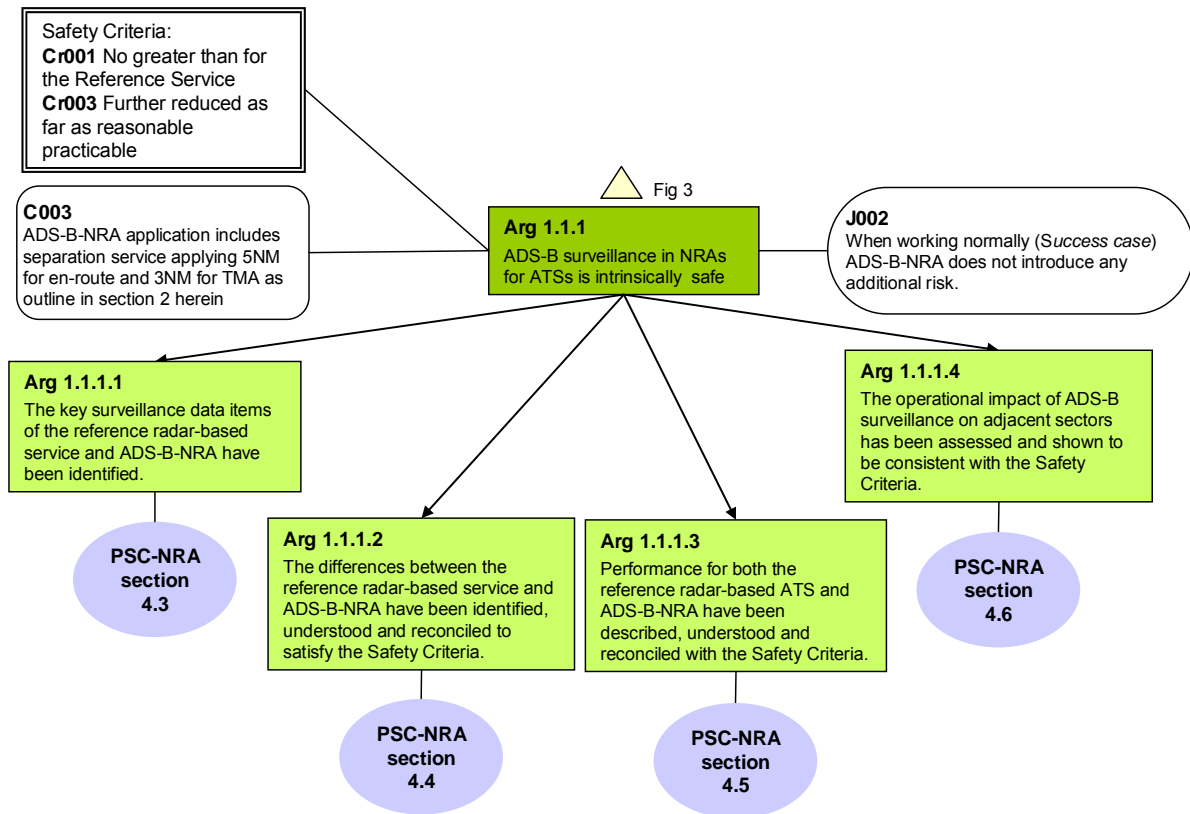
- the comparison with reference ATS operation using a reference radar as sole surveillance means, especially for separation services,
- assuming that those operation are tolerably safe (A001) for certain radar characteristics against which ADS-B performance characteristics will be derived.

Therefore, in order to satisfy Arg1.1.1, Evidence showing that the following lower-level Arguments are true have to be provided to show that ADS-B is both functionally equivalent, and has equivalent performance, to the reference radar-based ATS, as follows:

- a)       **Arg 1.1.1.1.** The surveillance data items for both the reference radar based operations and ADS-B-NRA have been defined.
- b)       **Arg 1.1.1.2.** The differences between those two sets of data items have been described, understood and their impact reconciled with the Safety Criterion Cr001.
- c)       **Arg 1.1.1.3.** The performance characteristics for the radar based operations reference service and ADS-B in NRA have been defined, and shown to be adequate to satisfy the Safety Criterion Cr001, for the specified separation minima.

- d) **Arg 1.1.1.4.** The impact of the Application on adjacent sectors has been assessed and shown to be consistent with the Safety Criterion Cr002.

As indicated in 3.4.1, consideration above relate to the “Success Case” context (J002).



**Figure 5: Decomposition of Argument on Intrinsic Safety (Arg1.1.1)**

These arguments are addressed in turn, in sections 4.3 to 4.6. Conclusions regarding Arg1.1.1 are then drawn, in section 4.7.



## 4.3 PROCEDURES AND SURVEILLANCE DATA ITEMS (ARG1.1.1.1)

### 4.3.1 Procedures

ADS-B-NRA procedures are very similar to those related to reference radar based ATS (as defined in PANS ATM Doc4444 [Ref.2]).

**GM006.** Implementers shall review the national procedures to see whether if any goes beyond the PANS-ATM procedure/phraseology and shall assess the implication with respect to this argument

Concerning flight crew operating procedures, they are similar to those proposed in PANS-OPS Doc 8168 [Ref.8] for SSR (or Mode S) operations.

### 4.3.2 Surveillance Data Item

As explained in sections 4.1 and 4.2 above, this section summarizes the data items required of ADS-B in order to support ATS operations, with 3Nm (Terminal Airspace) and 5Nm (En-Route) separation minima, with an acceptable level of safety.

These data items have been derived by comparison to reference ATS radar-based service (C001), that itself is assumed to be tolerably safe (A001) in the operational context described in the previous section 2, for the above separation minima. This approach should ensure that the surveillance data items required are completely and correctly identified.

It has to be noted that this section focuses on the essential ADS-B characteristics that are at the core of the case for use of ADS-B in NRA, the full safety requirements that are derived from these being dealt with in the next sections 5 to 8.

Two sets of **surveillance data items** are identified: operational surveillance data items at the level of the Controller Working Position (this is addressed in section 4.3.2.1) and technical surveillance data items at the input of the ground ATC processing function (this is addressed in section 4.3.2.2).

References to points of measurement in Figure 1 are provided in following sections in order to clearly indicate which data items are provided by each function in the ADS-B-NRA system.

#### **4.3.2.1 Operational Surveillance data item**

Specific information concerning aircraft, in or planned to enter the sector, has to be provided to the Controller in order to be able to perform ADS-B-based ATS, and in particular for ATC services applying separation minima, as described in the previous section 2.

The surveillance data items, listed hereafter, are equivalent to those provided by the reference radar, and have to be available on the Controller Working Position, i.e. at the point of measurement G2 in Figure 1 (as indicated in annex §A.3.9 of [Ref.1]):

- › Identification
- › Position
- › Pressure-Altitude<sup>12</sup> derived level information
- › Emergency indication
- › Special Position Ident (SPI)
- › Ground Velocity

In addition, in the ADS-B case, the ATCo interface will provide an indication on whether the surveillance quality of a particular aircraft is acceptable for the various functions of ATC (e.g. a track symbol supporting the use of surveillance separation standards) - as indicated in [Ref.1], in Annex A.3.9.8.

#### **4.3.2.2 Technical Surveillance data items**

The technical comparison shown in Table 1 below has been performed at the level of the output of the reference radar - i.e. at the input to the ground ATC processing system which deals with the transformation of radar or ADS-B plots into CWP tracks. This means that it has been assumed that the ground processing system is largely equivalent in its principle for processing ADS-B or reference radar inputs. Specific differences exist however and their impact is addressed in section 4.4 below.

---

<sup>12</sup> As per PANS-ATM Doc4444 [Ref.2] Chapter 1: Definitions: "Pressure-Altitude" is an atmospheric pressure expressed in terms of altitude which corresponds to that pressure in the Standard Atmosphere.

The Technical Surveillance data items required in input to the ATC processing subsystem (i.e. at point of measurement E2 in Figure 1) are listed in Table 1 below, comparing reference radar and ADS-B based surveillance as obtained from §Table11 of ED-126/DO-303 [Ref.1] :

Required Surveillance Data Items	Reference Radar (SSR)	ADS-B-NRA
Identification	Mode 3/A *	Aircraft Identification and/or Mode 3/A code * 24 bit ICAO aircraft address *
Horizontal Position	Range; Azimuth	Latitude; Longitude *
Quality Indicator	In general, no specific data item	Quality Indicator on an individual aircraft basis as a means to determine whether position quality is suitable for surveillance separation *
Pressure-Altitude	Mode C *	Pressure-Altitude *
Emergency Indicators	From Mode A codes *	Emergency indicators from ADS-B messages *
SPI	SPI code bit added to Mode 3/A reply *	SPI indicator from ADS-B message *

**Table 1: Required technical surveillance data items (in input to ground ATC processing)**

In Table above, the (\*) indicates that the information is directly provided by the aircraft. In the ADS-B case, this list corresponds to the minimum data set<sup>13</sup> to be transmitted by the aircraft (i.e. at point of measurement D in Figure 1), as explained in the paragraph §3.4.1 of [Ref.1].

It has to be noted that in the reference radar case, horizontal position is calculated by the radar itself, and that no specific quality indicator (QI) data item is provided. Nevertheless, radar range imposes limits for certain separation minima (affects surveillance quality of individual aircraft according to their range).

Ground velocity which is part of the Controller Working Position data items identified in section 4.3.2.1 is not mentioned in the list of the technical data items of Table 1 above as it is required that for the ADS-B case this data item will be reconstructed by the ground ATC processing system as in the reference radar case.

---

<sup>13</sup> See EASA NPA [Ref.14]for more detail on avionics requirements

### 4.3.3 Surveillance Functions

The main surveillance functions required for ADS-B in order to support ATS operations with an acceptable level of safety are presented in the following table (information derived from §Table 41 from [Ref.1]) in comparison to the radar-based reference:

Element	Functions provided in radar environment	Functions provided in ADS-B-NRA environment
External Data Sources	n/a	Provides external information to aircraft domain (e.g. GNSS).
Transmit Aircraft Domain	<ul style="list-style-type: none"> <li>‣ Processes “radar” data to be transmitted to Ground Domain</li> <li>‣ Assures all other functions allowing the aircraft to fly as expected</li> <li>‣ Provides radar information to ground domain (when requested by ground), based on own processed information.</li> </ul>	<ul style="list-style-type: none"> <li>‣ Receives information from External Data Sources.</li> <li>‣ Verifies availability / integrity of some data provided by External Data Sources</li> <li>‣ Processes ADS-B data to be transmitted to Ground Domain</li> <li>‣ Assures all other functions allowing the aircraft to fly as expected</li> <li>‣ Provides ADS-B information to ground domain (ADS-B messages), based on external data sources and own processed information.</li> </ul>
Receive subsystem	<ul style="list-style-type: none"> <li>‣ Receives radar data from Aircraft Domain</li> <li>‣ Verifies information received from the Aircraft Domain</li> <li>‣ Provides received information in form of radar reports to the ATC Processing &amp; Display system.</li> </ul>	<ul style="list-style-type: none"> <li>‣ Receives ADS-B messages from Aircraft Domain</li> <li>‣ Verifies information received from the Aircraft Domain</li> <li>‣ Provides received information in form of ADS-B reports to the ATC Processing &amp; Display system.</li> </ul>
Ground ATC Processing and Display subsystem	<ul style="list-style-type: none"> <li>‣ Receives and verifies data provided by ground radar system.</li> <li>‣ Notifies controller about loss of radar data for a specific aircraft (i.e. coasting function).</li> </ul>	<ul style="list-style-type: none"> <li>‣ Receives and verifies data provided by ADS-B Receive sub-system.</li> <li>‣ Notifies controller about loss of ADS-B data for a specific aircraft (i.e. coasting function as in reference radar-based surveillance.)</li> </ul>

Element	Functions provided in radar environment	Functions provided in ADS-B-NRA environment
	<ul style="list-style-type: none"> <li>▸ Processes radar information</li> <li>▸ Displays surveillance radar information to the controller</li> </ul>	<ul style="list-style-type: none"> <li>▸ Processes ADS-B information</li> <li>▸ Displays surveillance ADS-B information to the controller</li> </ul>
ATCo	<ul style="list-style-type: none"> <li>▸ Uses all available information (e.g. information displayed by ground system, information obtained from VHF communications with FC, etc.) to provide radar based ATS.</li> </ul>	<ul style="list-style-type: none"> <li>▸ Uses all available information (e.g. information displayed by ground system, information obtained from VHF communications with FC, etc.) to provide ADS-B-NRA.</li> </ul>

**Table 2: Surveillance Functions**

More detailed information on Environment Definition is provided in §Annex A2.4 in [Ref.1], including operational and airspace characteristics, generic air traffic characteristics, and capabilities and performances of CNS infrastructure for current, reference and target environment.

#### 4.4 DIFFERENCES BETWEEN RADAR AND ADS-B BASED ATS OPERATIONS (ARG1.1.1.2)

As described in section 2, reference radar-based ATS services and ADS-B-based ATS services are very similar. Previous section 4.3 identifies two sets of surveillance data items (operational & technical) for those services. Where in general these two sets appear to be very similar in the reference radar and ADS-B cases, there are however some differences which need to be discussed.

The purpose of this section is therefore to:

- Ensure that the differences between these services are identified and that the related procedures exist in the ADS-B case.
- Ensure that the specific differences between the two corresponding sets of data items (operational and technical) for each service are identified and their possible impact on operation has been assessed.

##### 4.4.1 Procedures

ADS-B-NRA procedures are very similar from those related to reference radar based ATS. The specific differences are described in the PANS ATM Doc4444 [Ref.2] (as indicated in §A.3.4.2 of ED-126/DO-303 [Ref.1]). Impact at operational level is also described in the document Guidance for the Provision of Air Traffic Services Using ADS-B in Non Radar Area [Ref.11]).

Flight crew operating procedures are similar to those proposed in PANS-OPS Doc 8168 [Ref.8] for SSR (or Mode S) operations. The NRA Flight Crew Manual [Ref.10] provides the guidance relating to those procedures.

**GM007.** Any divergence in terms of procedure at local implementation level will have to be addressed under argument 1.3 (see section 3.4.3).

#### 4.4.2 Data items

This section focuses on the differences in terms of data items used between reference radar and ADS-B and assesses the corresponding impact at various levels (operational, functional, data items sources). The discussion is organised data item per data item, for which the main differences and their impact at technical and operational level are presented and reference to the corresponding evidence is provided:

**Identification** ADS-B provides aircraft identification (call-sign or the registration marking). Mode A code is only optionally<sup>14</sup> provided while reference radar provides Mode A code only. In addition, aircraft identification data are not broadcast by ADS-B in a synchronised fashion to the position data.

This difference is mitigated by the presence of the 24 bits address, used in ADS-B-NRA for association purposes in ATC processing system (instead of Mode A used in reference radar operations). This data item is described in §3.2 c) and §4.5.1 of [Ref.1].

As mentioned in section 4.4.1, the specific differences related to identification having an impact at operational level are described in the PANS ATM Doc4444 [Ref.2] (as indicated in §A.3.4.2 of ED-126/DO-303 [Ref.1] and in the document Guidance for the Provision of Air Traffic Services Using ADS-B in Non Radar Area [Ref.11]), as well as in the Flight Crew manual [Ref.10] (see section §6 of [Ref.10] concerning the entering of ID into the airborne system).

**Horizontal Position / Quality Indicator** In ADS-B-NRA, horizontal position is provided by the aircraft together with a Position Quality Indicator (QI) characterising its accuracy and integrity.

ADS-B-NRA position information is derived onboard (in general from GNSS), whereas in the reference radar case, it is provided by the radar itself. ED126/303 [Ref.1], specifically identifies the necessary requirements regarding Position Quality Indicator in order to support safe ATS service and in particular the separation services.

Therefore, the risk associated to the dependency of the position information and the use of Position Quality Indicator to indicate if separation service can

---

<sup>14</sup> Mode A code can be only provided when the ADS-B message definitions permits, when the information is available in the airborne system and transmitted (in Europe). At the time of the edition of this document, this is pending the related ICAO Annex 10 ([Ref.9] update).

be provided has been assessed performing a Close Approach Probability (CAP) analysis (§ Annex E in [Ref.1]).

This Close Approach Probability is the means by which Quality indicator values have been derived by comparison with different radar characteristics. Requirements on the ADS-B Quality Indicators (NIC<sup>15</sup>) are levied to ensure that the ADS-B separation risk is no greater than that of radar in the event that the ADS-B position source is in a faulted condition. NIC provides a containment radius around the reported aircraft position which the true position of the aircraft will not exceed with a certain probability for more than a defined time to alert, without the aircraft reporting the excursion to ATC automation (via a change of NIC).

In §Annex I in [Ref.1], time to alert is defined as the elapsed time between the position error exceeding the containment region, and the ADS-B out system annunciating the alert by changing the ADS-B quality indicator, NIC. A maximum time to alert of 10 seconds is required in §Annex B and described in §Annex I in [Ref.1].

Very conservative assumptions are made that the worst case scenario is a satellite failure of a 5 m/s pseudo range ramp error resulting in a 5 m/s position error for 10 seconds, which is 50 meters beyond the integrity containment region (in [Ref.16], the worst-case observed Block I, II and IIA satellite failure is a pseudo-range ramp error of 5.0 m/s. Note that although step errors of greater magnitude are observed, they are easily detected due to the step-monitor algorithm that is executed on top of the integrity monitor).

It is also conservatively assumed that the drift error is in the direction of the adjacent aircraft. Note that if the adjacently separated aircraft are using the same set of satellites, a satellite fault condition will cause similar positional bias on both aircraft, and the net separation error due to the fault will be zero.

It was also assumed that a pair of aircraft would remain in proximity for 30 minutes

As result of all these analysis, the minimum values of Position Quality Indicator allowing a safe separation service using ADS-B surveillance data have been determined (SPR-1, SPR-3, SPR-5, SPR-7 in [Ref.1]). Visual comparison means with the radar case for the required NIC values is provided in this §Annex E in [Ref.1] (§Figure 56 and §Figure 57), and similarly, §Figure 19 in [Ref.1] provides a visual comparison for the derivation of the required

---

<sup>15</sup> Navigation Integrity Category (NIC) expresses the integrity containment radius and Surveillance Integrity Level (SIL) to specify the probability of the true position lying outside that containment radius without alerting.



NACp<sup>16</sup> values. and the related requirements are presented in section 5.5.3.3, in Table 13, including the time to alert values related to a change of Position Quality Indicator.

**GM008.** Implementers shall check whether the CAP assumptions are applicable in their local environment or shall use alternative methods to derive quality indicators. Implementers shall check whether the Quality Indicator values as specified in Table 4 are appropriate at local level. As indicated in EASA material [Ref.14] Appendix 4.2 Note 2: "ED-126 provides, based on its reference collision risk analysis only, arguments for an equally appropriate encoding of a SIL=2<sup>17</sup> as a matter of expressing the system integrity as well, and providing related requirements". "It is at the discretion of the ANSP to decide upon the appropriate threshold values required in support of the separation services in its airspace".

The impact for this data item upon the ground ATC processing system relates to the management of the Position Quality Indicator that is provided together with the corresponding position (see §Table41 of [Ref.1] concerning the functions to be provided by ATC processing system).

The impact for this data item at CWP level is identical to the reference radar case: Controllers will have to be provided with an indication on whether the surveillance quality of a particular aircraft is acceptable for the various functions of ATC (including surveillance separation standards) as developed in Operational Requirements OR-2 and OR-3 in [Ref.1].

**GM009.** Implementers shall specify Position Quality Indicator processing for their Ground ATC Processing and Display system, and in particular how Quality Indicator values below or above threshold are managed. Human Factors have to be considered in this local specification process.

---

<sup>16</sup>NAC: Navigation Accuracy Category. NACp expresses the position accuracy.

<sup>17</sup> The SIL value is established to SIL≥2 in line with the system integrity (10-5/fh) – see SAF048, in section 8.7

### **Other Data Items**

Pressure-Altitude, Emergency mode indicators, SPI: although the technical content differs between the ADS-B and the reference radar case, the use of these data items is identical in both reference radar and ADS-B based cases and therefore this is not further developed in this section.

The Emergency indicators provided include in comparison to the radar-based case, the following additional elements for the Urgency mode: Minimum fuel and Medical (see section 7.4.1 - "Aircraft Emergencies").

## 4.5 PERFORMANCE CHARACTERISTICS (ARG1.1.1.3)

### 4.5.1 Performances at ATC Processing System input

As mentioned in the introduction of section 4.2, specific reference-radar performance values are needed in order to derive the equivalent ADS-B requirements, in compliance with Safety Criteria Cr001.

These reference-radar performance values are documented in §Annex B of [Ref.1] for each of the data items listed in Table 1 above, and are summarized in Table 2 below.

These performance values address in the radar case the characteristics of the data items at a point of measurement equivalent to D-E2 in Figure 1, both in En-route and TMA cases, in terms of update interval and probability (in §B.4.1 Table-12), accuracy (in §B.4.2 Table-14), and other parameters as latency and time stamp accuracy (in §B.4.5 Table-24).

It has to be noted that two typical reference radars allowing separation minima of 5 and 3 NM when used as sole surveillance means have been used for the comparison, i.e. an MSSR, and an SWSSR (Sliding Window).

The following Table 3 presents the reference-radar performance values to be considered for the specification of the ADS-B performance values:

Reference Radar Performance		En-route	TMA
Update interval	Update interval (radar scan period)	≤ 10s	≤ 5s
Update probability	Target report : position	≥ 0.97	≥ 0.97
	Mode A code validation (per target report)	≥ 0.98	≥ 0.98
	Mode C code validation (per target report)	≥ 0.96	≥ 0.96
	Emergency/SPI code validation	≥ 0.98	≥ 0.98
Accuracy Horizontal Position	Core accuracy:		
	MSSR model 95% azimuth accuracy	0.12 °	0.12 °
	SWSSR model 95% azimuth accuracy	0.45 °	0.45 °
	MSSR range of applicability	200Nm	60Nm
	SWSSR range of applicability	200Nm	40Nm
	MSSR model 95% cross range position accuracy	776m	233m
	SWSSR model 95% cross range position accuracy	2910m	582m

Reference Radar Performance		En-route	TMA
Latency	Maximum age for position, Mode A Code, Emergency and SPI in radar report (at the input to the ATC processing system)	2s	2s
Time Stamp	Maximum time stamp inaccuracy of radar reports is determined by the ground system	0.2s	0.2s

**Table 3: Reference Radar Performance Parameters**

**GM010.** The ATS reference service (radar based surveillance) includes a separation service with minima (5 Nm En-Route, 3 Nm in TMA) which may not correspond to those applied by local implementers when such reference radar is used as sole surveillance means. In that case, the different (higher) separation minima applied by a local implementer will replace the 5Nm/3Nm values used in this document. Alternatively, the use of a different (local) reference radar supporting as sole surveillance means a separation service minima of 5 Nm En-Route, 3 Nm in TMA, will require an assessment by implementers of the related safety impact, in particular concerning the derivation of the corresponding Horizontal Quality Indicators.

Note: selecting different reference separation minima impacts OSA – see assumption A019 in section 8.4.3 and can have an impact on local ground requirements in section 5, which will have to be assessed, possibly re-using the ED 126/DO 303 process.

The following Table 4 presents the ADS-B performance values to be required for the ADS-B receiver subsystem (i.e. also at point of measurement D-E2 in Figure 1). They have been derived from reference-radar performance values presented in previous Table 3.

ADS-B-NRA Performance		En-route	TMA
Update interval	for Surveillance Position report (including change in quality indicators) - equivalent to radar scan	≤ 10s	≤ 5s
	For Surveillance report containing any new aircraft Identity (aircraft identification / Mode A code, 24 bits address) associated with any single aircraft.	< 100s <sup>18</sup>	< 100s
	for Surveillance Emergency/SPI change <sup>19</sup>	≤ 10s	≤ 5s
Update probability	for Surveillance Position report (same as for radar target) <sup>20</sup>	≥ 0.95	≥ 0.95
	for Surveillance Identity change (aircraft identification / Mode A code & 24 bits address)	≥ 0.95	≥ 0.95
	for Surveillance Emergency / SPI change	≥ 0.95	≥ 0.95
Horizontal Position Accuracy	Horizontal Position Accuracy 95% <i>See explanation below.</i>	< 0.5 Nm (NAC <sub>p</sub> ≥5)	< 0.3 Nm (NAC <sub>p</sub> ≥6)
Horizontal Position Integrity <sup>21</sup>	Quality Indicators (and maximum radius containment "Rc")	NIC <sub>p</sub> ≥4 (Rc < 2.0 Nm) or NUC <sub>p</sub> <sup>22</sup> ≥4)	NIC <sub>p</sub> ≥5 (Rc < 1.0 Nm) or NUC <sub>p</sub> ≥5

<sup>18</sup> Value derived from RFG operational requirements on Identity change. Note that unlike radar, aircraft identification / Mode A code and the 24 bits ICAO address in ADS-B may be sampled and broadcast separately from the SPI and emergency indicator.

<sup>19</sup> For aircraft capable of Emergency/SPI reporting

<sup>20</sup> Since ADS-B position is accompanied by barometric height, the 0.95 figure for ADS-B is equivalent to combination of radar position and Mode C height update probability (0.97\*0.96).

<sup>21</sup> "Horizontal Position Integrity" relates to a quality of service providing an indication on when ADS-B-NRA separations can be applied or not, in the nominal case.

ADS-B-NRA Performance		En-route	TMA
		(Rc<1.0 Nm)	(Rc < 0.5 Nm)
	Position source failure probability	10-4/h <sup>23</sup>	10-4/h
	Position source alert failure probability	10-3 (per position source failure event)	10-3 (per position source failure event)
	Time to alert	10s	10s
Latency	Maximum latency for surveillance position, identification and Emergency/SPI data at E2. Note any latency uncertainties on board the aircraft have the effects of a reduction in position accuracy.	2s	2s
Time Stamp	Maximum time stamp inaccuracy of ADS-B surveillance reports by the ground system. Note any time uncertainties on board the aircraft have the effects of a reduction in position accuracy.	0.2s	0.2s

**Table 4: ADS-B Performance Parameters**

Accuracy values result from the “reconciliation process” between the radar performances accuracy values (from Table 3) and the CAP results (as referred to in section 4.4.24.4.2). The “reconciliation process” is described in §Appendix B.3.5 of [Ref.1]. The CAP accuracy results being the most stringent ones are therefore values retained for ADS-B position accuracy, i.e. 0.5Nm for en-route and 0.3Nm for TMA. The CAP assumes that:

**A003.** The horizontal plane error distribution for a GNSS positioning source is represented by a radial Rayleigh probability density function (ASSUMPT-70 in [Ref.1]).

<sup>22</sup> NUC: Navigation Uncertainty Category (NUC), a combined expression of (accuracy and) integrity requirements through a single parameter;

<sup>23</sup> For GNSS based functions, expressed as an assumption of GNSS performance – see A011 in section 7.3.2 (USatellite constellation (GNSS) failures

**GM011.** The separation standards applied in the target ADS-B-NRA airspace influence also the accuracy and integrity requirements placed on the horizontal position (accuracy requirements result from a reconciliation process between the CAP analysis ([Ref.1] Annex E) and the OPA ([Ref.1] Annex B). Both make the assumption that the separation standards applied are 5 Nm en-route and 3 Nm in TMA. The CAP analysis has led to the determination of NIC and NAC<sub>p</sub> values to be required from airframes so that the horizontal separation risk is equivalent (or smaller) to that of a radar controlled area in which the above mentioned separation standards are applied. In case of a different reference separation minima at local level, there are possible implications on the required ADS-B horizontal position accuracy and integrity values that are to be considered by implementers

**GM012.** ED-126/DO303 ([Ref.1]) explicitly mentions that less stringent requirements might be placed on NIC/NAC<sub>p</sub> values in NRA airspaces with larger minimum separations, but also indicates that additional studies would be needed in this respect (see [Ref.1] Annex E, section 5).

#### 4.5.2 Performances at Aircraft domain output

Concerning airborne domain (i.e. point of measurement D in Figure 1), the same aircraft performances apply for ADS-B-NRA in terms of vertical position accuracy than for reference radar service (see Table 5 below).

Vertical position		En-route	TMA
Accuracy Vertical Position	Altimeter accuracy <sup>24</sup>	38.1m (125ft) <sup>25</sup>	38.1m (125ft)
	Resolution in Mode C	≤ 100ft <sup>26</sup>	≤ 100ft

**Table 5: Performance on Aircraft Vertical Position**

#### 4.6 IMPACT ON ADJACENT SECTORS (ARG1.1.1.4)

The expected impact on adjacent sector due to the use of ADS-B surveillance is, in general, equivalent to that of the reference radar surveillance case. See section 5.6 for specific requirements and assumptions related to adjacent sectors (i.e. transfer and coordination).

---

<sup>24</sup> This is minimum accuracy requirement for altimeter, and is dependent on the type of airspace. Many airspace regions, such as RVSM, will require better altimeter performance than specified here.

<sup>25</sup> As per Mode C provision in ICAO Annex 10

<sup>26</sup> As per Annex 10, Vol. IV (4.3.9.3.1.) it is recommended to use a source providing a resolution less than or equal to 7.62m (25ft)

#### **4.7 CONCLUSIONS ON ARG1.1.1 - INTRINSIC SAFETY OF THE APPLICATION**

In this section, ADS-B-NRA application has been described and compared to reference radar-based ATS operations. The surveillance data items have been identified and the main differences with reference radar-based operations have been examined (mainly concerning aircraft identification and position data items), and how these differences have been addressed for ADS-B-NRA has been described. This shows that ADS-B-NRA is functionally equivalent to the reference radar-based ATS.

Similarly, the surveillance performance required for ADS-B-NRA in order to support separation minima of 3 Nm (Terminal Airspace) and 5 Nm (En-route) obtained by comparing with reference radar service performance have been described. This shows that ADS-B-NRA has performance that is equivalent to the reference radar-based ATS.

Finally, the way in which the application will impact adjacent sectors has also been considered. It has been shown that this impact is minimal, although some issues regarding coordination and transfer will have to be addressed (see section 5.6).

This section has, therefore, provided adequate Argument and supporting Evidence that, by comparison with reference radar based operations, the ADS-B-NRA application is capable of satisfying the Safety Criteria Cr002 specified in section 4.1 (i.e. demonstrating that the Application is intrinsically safe).



## 5 DESIGN COMPLETENESS FOR ADS-B-NRA (ARG1.1.2)

The objective of this section is to demonstrate that all necessary Safety Requirements (including safety-related operational requirements) have been specified (or assumptions have been stated) to cover all elements, in terms of system design, that are necessary to fully implement the Application.

**Note:** all the requirements provided in this section 5 correspond to the “*Success Case*” only. Requirements and assumptions related to the “*Failure Case*” of the application are provided in section 8.

### 5.1 SAFETY CRITERIA

The Safety Criterion considered for this argument Arg1.1.2 is the same as for Arg1.1.1, i.e. the combination of main Safety Criteria Cr001 and Cr003 (*Success Case*), i.e. the risk of an accident shall be:

Cr001 No higher than the equivalent risk associated with “reference service” – i.e. radar-based surveillance, including separation service provided by ATS (for the given set of separation minima).

Cr003 Reduced as far as reasonably practicable.

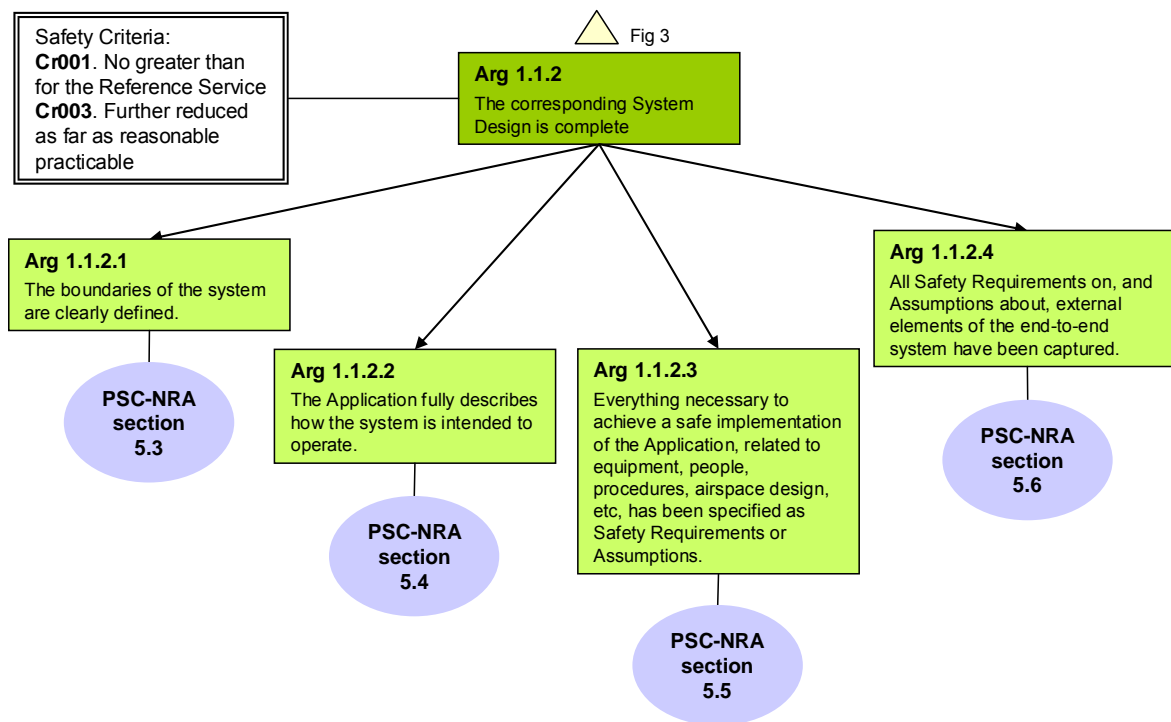
### 5.2 STRATEGY

The strategy for satisfying Arg1.1.2 is to provide Evidence that the following lower-level Arguments are true:

- a) **Arg 1.1.2.1** The boundaries and functions of the ADS-B system underlying ADS-B-NRA application are clearly defined.
- b) **Arg 1.1.2.2** The application Operations fully describes how the ADS-B-NRA is intended to operate.
- c) **Arg 1.1.2.3** Everything necessary to achieve a safe implementation of ADS-B-NRA (including equipment<sup>27</sup>, people, procedures) has been specified as Safety Requirements or Assumptions.
- d) **Arg 1.1.2.4** All Safety Requirements on, and assumptions about, external elements of the end-to-end system have been captured.

---

<sup>27</sup> For generic aspects of ADS-B-NRA, “equipment” has been specified at functional level only. Local full Safety Case will have to address the physical architecture supporting the local implementation. See Guidance Material Box GM019.



**Figure 6: Decomposition of Argument on Design Completeness (Arg1.1.2)**

These are addressed in turn, in sections 5.3 to 5.6. Conclusions regarding Arg1.1.2 are then drawn in section 5.7.

### 5.3 ADS-B SYSTEM BOUNDARIES AND FUNCTIONS (ARG1.1.2.1)

Operational boundaries have already been presented in section 2.1 (Air Traffic Services delivered, responsibilities, environment, etc.) when ADS-B-NRA application has been introduced.

Technical boundaries related to the ADS-B system aspects have also been presented at the beginning of the document in section 2.2. The main functions related to each element have been presented in Figure 1 of this mentioned section and described in more detail in section 4.3.3 Table 2.

As previously mentioned, more detailed information on Environment Definition is provided in §Annex A2.4 in [Ref.1], including operational and airspace Characteristics, generic air traffic characteristics, and capabilities and performances of CNS infrastructure for current, reference and target environment.

**GM013.** Local implementers shall precisely describe the target and the reference environments to be locally considered, and shall address any divergence with the generics environments defined in §Annex A2.4 in [Ref.1].

## 5.4 DESCRIPTION OF ADS-B-NRA OPERATIONS (ARG1.1.2.2)

The table presented below (as per §Table 10 from [Ref.1]) illustrates the various phases of operation relating to the use of ADS-B surveillance to support Air Traffic Control (Separation based on ADS-B) and Alerting Service activities, providing comparison with the related reference radar-based operations as described in PANS-ATM Doc4444 [Ref.2].

Phases of operations	Handling of ADS-B equipped traffic
<p><b>Phase 1 –</b> ADS-B Data Acquisition</p>	<ul style="list-style-type: none"> <li>‣ The aircraft transmits ADS-B messages.</li> <li>‣ The ground processing receives and validates the ADS-B information (similar to radar system capabilities in §8.1 (“ATS Surveillance Systems Capabilities”) from [Ref.2])</li> </ul>
<p><b>Phase 2 –</b> Initiation of ADS-B based Services</p>	<ul style="list-style-type: none"> <li>‣ The ADS-B track automatically appears on the controller’s surveillance display (similar to presentation of radar information in §8.2 (“Situation Display”) from [Ref.2])</li> <li>‣ Direct pilot-controller communications established (§8.3.2 (“Communications”) from [Ref.2])</li> <li>‣ The flight crew receives contact from the ATC to establish ADS-B identification (similar to establishment of radar identification in §8.6.2 (“Identification of Aircraft”) from [Ref.2])</li> <li>‣ Flight plan association of the ADS-B track is established.</li> </ul>
<p><b>Phase 3 –</b> Provision of ADS-B based separation services</p>	<p>Monitoring of ADS-B traffic on the surveillance display and applying (surveillance) control procedures similar to PANS-ATM Chapter 8 (“ATS Surveillance Services”) procedures, in particular for:</p> <ul style="list-style-type: none"> <li>‣ ATC service functions (§8.4 (“Provision of ATS Surveillance Services”) and §8.7.1 (“Functions”) from [Ref.2])</li> <li>‣ Separation application (§8.7.2 (“Separation Application”) and §8.7.3 (“Separation Minima Based On ATS Surveillance Systems”) from [Ref.2])</li> <li>‣ Vectoring (§8.6.5 (“Vectoring”) and §8.9 (“Use of ATS Surveillance Systems In The Approach Control Service”) from [Ref.2])</li> <li>‣ Surveillance monitoring (as per Radar Monitoring)</li> </ul> <p>[The provision of services requiring appropriate quality of surveillance information (like in §8.1.7 from [Ref.2])]</p>
<p><b>Phase 4 –</b> System Alerting</p>	<p>System alerting procedures are similar to those defined for radar emergencies, hazards and equipment failures (§8.8 from [Ref.2]), in particular for:</p> <ul style="list-style-type: none"> <li>‣ Aircraft Emergencies (§8.8.1 (“Emergencies”) from [Ref.2]),</li> </ul>

Phases of operations	Handling of ADS-B equipped traffic
	<ul style="list-style-type: none"> <li>▸ Failure of equipment (§8.8.3 (“Failure of Equipment”) from [Ref.2]), with ‘ADS-B-out’ failure requiring similar action as for SSR transponder failure</li> <li>▸ ADS-B equipment failure (like radar equipment failure in §8.8.4 (“ATS Surveillance System Failure”) from [Ref.2])</li> </ul>
<p><b>Phase 5 –</b> Termination of ADS-B based Service(s) (due to either expected or unexpected terminations)</p>	<p>For unexpected termination, ADS-B Separation can no be longer be applied, and the controller applies procedural separation.</p> <p>For expected termination transfer is coordinated with the adjacent sector (or aerodrome). Control procedures similar to PANS-ATM chapter 8 and Chapter 10:</p> <ul style="list-style-type: none"> <li>▸ Co-ordination of traffic (§8.7.4 (“Transfer Of Control”) from [Ref.2])</li> <li>▸ Transfer of control (§10.1.2.2. (“Transfer Of Control”) from [Ref.2])</li> </ul>

**Table 6: ADS-B NRA Phases of Operation**

As indicated in section 4.3.1, the ADS-B NRA procedures are developed in the ICAO PANS ATM - “Procedures for Air Navigation Services - Air Traffic Management”, Document 4444, Fifteen edition 2007, including ADS-B procedures in Chapter 8 “ ATS Surveillance Services” ([Ref.2]). As a result of work done by ICAO by comparison with the reference radar-based ATS, these procedures are considered as well defined and complete.

## 5.5 ADS-B NRA SAFETY REQUIREMENTS ARG1.1.2.3)

The Requirements and Assumptions to support the above operations are the key elements provided by the ED-126/DO-303 [Ref.1] document. They address all elements of the system described above and are necessary to ensure the intrinsic safety of the ADS-B NRA application.

This section provides safety requirements concerning the operational aspects (ATCo and Flight Crew – see section 5.5.1) and the high level system design (see sections 5.5.2 and 5.5.3), necessary to cover surveillance data items to be provided to controller and ADS-B performance values as derived by comparison to reference radar-based surveillance as identified in sections 4.3 and 4.5.

**Note:** additional requirements are provided in sections 6 to 8 to cover the complementary aspects related to design correctness, design robustness and the mitigation of internal failure (covered under Arg1.1.3 to 1.1.5 respectively).

### 5.5.1 Safety Requirements relating to Operational ADS-B-NRA Procedures

As already mentioned in section 4.3.1 the ATS procedures to be used for ADS-B-NRA are similar to those used in reference radar service. Table 7 below lists the related safety requirements to be applied:

Actor	ADS-B-NRA procedural Safety Requirement
ATCo	<b>SAF001.</b> Controller shall apply PANS ATM Doc4444 [Ref.2] procedures to perform ADS-B-NRA application.
Flight Crew	<b>SAF002.</b> Flight crew shall apply PANS-OPS Doc 8168 [Ref.8] procedures to perform ADS-B-NRA application.

**Table 7: Safety Requirements on ATS Procedures for ADS-B-NRA**

**GM014.** Guidance material to be considered for local implementation: "Guidance for the Provision of Air Traffic Services Using ADS-B in Non Radar Areas" ([Ref.11] and "The NRA Flight Crew Manual" [Ref.10].

**GM015.** Any divergence in terms of procedure at local implementation level will have to be addressed under argument 1.3 (section 3.4.3).

Concerning the conditions on which separation minima can be applied by the controller, the related safety requirements are presented hereafter:

**SAF003.** Separation minima of 5NM shall be only applied by controller to aircraft being eligible for ADS-B-NRA in en-route.

**Note:** see aircraft eligibility conditions in section 5.5.3.3.

**SAF004.** Separation minima of 3NM shall be only applied by controller to aircraft being eligible for ADS-B-NRA in TMA.

**Note:** see aircraft eligibility conditions in section 5.5.3.3.

See GM001 for ICAO provision with respect to separation minima applicability.

### 5.5.2 Safety Requirements relating to Data Items

This section provides safety requirements relating to data items provided and used by the different elements of the ADS-B-NRA system.

#### 5.5.2.1 Safety Requirements on Operational Surveillance Data Items

Concerning the operational surveillance data items required at the ATCo interface (i.e. at point of measurement G2 in Figure 1), the list of related

requirements concerning nominal operational case (as described in section 4.3.2.1) is provided here below (obtained from (OR#) in §A.3.9 in [Ref.1]):

Element	Safety Requirements on ADS-B-NRA Data Items
Operational Data items	<p><b>SAF005.</b> The following list of surveillance data items shall be provided to the controller (OR-1 [Ref.1]):</p> <ul style="list-style-type: none"> <li>▶ Identity (*)</li> <li>▶ Position (see SAF006)</li> <li>▶ Emergency indicator(s)</li> <li>▶ Special Position Identifier(SPI)</li> <li>▶ Pressure-Altitude derived level information</li> <li>▶ Ground Velocity</li> </ul>
Additional ATCO interface features	<p><b>SAF006.</b> The ATCo interface shall provide an indication of whether the surveillance quality of a particular aircraft is acceptable for the various functions of ATC (e.g. a track symbol supporting the use of surveillance separation standards) (OR-2 [Ref.1]).</p>
	<p><b>SAF007.</b> The ATCo interface shall provide an indication whenever the surveillance quality falls below limits that are acceptable for the various functions of ATC (e.g. similar to the track coasting principle in reference radar case) (OR-3 [Ref.1]).</p>
	<p><b>SAF008.</b> When SPI functionality is available ADS-B shall provide it upon ATC request (OR-4 [Ref.1]).</p>
	<p><b>SAF009.</b> Surveillance Information shall be presented to the Controller in a manner similar to the reference radar-based case<sup>28</sup> (ASSUM-14 [Ref.1]).</p>

**Table 8: Safety Requirements on ADS-B-NRA data items at ATCo Interface**

(\*) The description of identity item is provided by ASSUMP-11 in ED-126/DO-303 [Ref.1] : *“It is assumed that aircraft equipped with ADS-B have an aircraft identification feature and will transmit the aircraft identification as specified in Item 7 of the ICAO flight plan or, when no flight plan has been filed, the aircraft will transmit the aircraft registration”.*

For emergency conditions please refers to section 7.4.1.

**GM016.** The implementer shall ensure that the aircraft displayed are time synchronised.

<sup>28</sup> The term “similar” includes in particular the display of position target with a constant refresh cycle (i.e. same as radar) and display targets that are time synchronised.

### 5.5.2.2 Safety Requirements on Technical Data Items at ATC Processing system input level

The technical data items required as input to the ATC processing system have already been identified in section 4.3.2.2.

The following Table 9 presents then the safety requirements related to these data items (at the point of measurement E2 in Figure 1).

Elements	Safety Requirement on ADS-B-NRA Data Items
Mandatory Technical Data Items	<p><b>SAF010.</b> The following ADS-B data items shall be provided at the input of the ATC Processing System ([Ref.1]) §3.5.1):</p> <ul style="list-style-type: none"> <li>▶ Aircraft Horizontal Position information (Longitude, Latitude)</li> <li>▶ Pressure-Altitude derived level information</li> <li>▶ Quality Indication of Latitude and Longitude</li> <li>▶ Aircraft identification (24 bits address and Identity*)</li> <li>▶ Emergency indicators</li> <li>▶ Special Position Information (SPI)</li> <li>▶ Time of applicability</li> </ul>
Optional Technical Data Items	<p>Depending on local implementation, the Mode A code may be required at the input of the ATC Processing System (for example, to assist ATC in flight plan correlation) ([Ref.1]) §3.5.1).</p> <p>Depending on local implementation, Velocity and its associated quality indicator may also be required at the input of the ATC Processing System (for example, to assist the ground automation in the time registering of ADS-B targets on the ATC display ([Ref.1]) §3.5.1).</p>

**Table 9: Safety Requirements on ADS-B-NRA data items ATC Processing system input**

(\*) The same description of Identity as in section 5.5.2.1 applies here.

Consistent definition of data required on airborne and ground domain is ensured by interoperability requirements as presented in correctness argument Arg1.1.3 in section 6.

### 5.5.2.3 Safety Requirements on Technical Data Items at Aircraft domain output level

Finally, technical data items required at the output of the airborne domain have also been identified in section 4.3.2.2. Related safety requirements (at point of measurement D in Figure 1) are provided in Table 10 hereafter:

Element	Safety Requirement on ADS-B-NRA Data Items
Mandatory Technical Data Items	<p><b>SAF011.</b> The transmit Aircraft domain shall transmit a minimum data set that includes the data items listed below ([Ref.1] §3.4.1):</p> <ul style="list-style-type: none"> <li>▶ Aircraft Horizontal Position information (Longitude, Latitude)</li> <li>▶ Aircraft Pressure-Altitude</li> <li>▶ Aircraft Position Quality Indicators</li> <li>▶ Aircraft identification (24 bits address and Identity*)</li> <li>▶ Emergency Indicators</li> <li>▶ Special Position Indication (SPI) report</li> </ul>
Optional Technical Data Item	Depending on local implementation, the Mode A code may be required to be provided by the aircraft (for example, to assist ATC ground system in flight plan correlation) ([Ref.1] §3.5.1).

**Table 10: Safety Requirements on data items at Airborne Domain output level**

(\*) The same description of Identity as in section 5.5.2.1 applies here.

Consistent definition of data required on airborne and ground domain is ensured by interoperability requirements as presented in correctness argument Arg1.1.3 in section 6.



### 5.5.3 Safety Requirements on ADS-B-NRA performances characteristics

The performance requirements have been assigned to the different elements of the functional system presented in Figure 1 (references to the various measurement points presented in this mentioned figure are included when necessary). It is reminded that only requirements concerning “Success case” are presented here; those concerning “Failure case” are addressed in section 8.

#### 5.5.3.1 Safety Requirements at ATC Processing system level

The safety requirements presented in Table 11 below are to be applied at ATC processing system level, i.e. at points of measurement E2-G2 in Figure 1.

Function	ADS-B-NRA performances Safety Requirement
ATC Processing System Features	<b>SAF012.</b> ATC Processing System shall provide typical radar data processing functions (Ground velocity reconstruction, etc.)
	<b>SAF013.</b> ATC Processing System shall process the 24 bit ICAO aircraft address
	<b>SAF014.</b> ATC Processing System shall process the Position Quality Indicator

**Table 11: Safety Requirements at ATC Processing system level**

### 5.5.3.2 Safety Requirements at ADS-B Receiver subsystem level

Performances required at ADS-B receiver subsystem level have been described in section 4.5.1. The following table lists the safety requirements to be applied at this level, i.e. at points of measurement D-E2 in Figure 1.

Parameter	ADS-B-NRA performances Safety Requirement
Ground Timing - Latency	<b>SAF015.</b> The 95% latency for ADS-B Surveillance Reports shall be no greater than 0.5s (SPR-16 [Ref.1])
Ground Timing - Time of applicability Accuracy	<b>SAF016.</b> The time of applicability conveyed in the ADS-B Surveillance Report shall have an absolute accuracy relative to UTC of +/- 0.2 seconds or less (SPR-17 [Ref.1]).
	<b>SAF017.</b> Each type of ADS-B Surveillance Report (i.e. containing position, identity and/or Emergency/SPI data) shall contain a time of applicability (Interface E2) (SPR-18 [Ref.1]).
Ground Update Interval for En-route	<b>SAF018.</b> For 5NM separation: The update interval for Surveillance Reports containing any new ADS-B Position data associated with any single aircraft shall be no longer than 10s with a probability of 95% (SPR-19 [Ref.1]).
	<b>SAF019.</b> For 5NM separation: The update interval for Surveillance Reports containing any new aircraft identification associated with any single aircraft shall be no longer than 100s with a probability of 95% (SPR-21 [Ref.1]).
Ground Time to alert for En-route	<b>SAF020.</b> For 5NM separation: The time to alert for a change in Surveillance Emergency / SPI Reports measured at point E2 shall be no longer than 10s for En-route with a probability of 95% (SPR-22 [Ref.1]).
Ground Update Interval for TMA	<b>SAF021.</b> For 3NM separation: The update interval for Surveillance Reports containing any new ADS-B Position data associated with any single aircraft shall be less than 5s with a probability of 95% (SPR-23 [Ref.1]).
	<b>SAF022.</b> For 3NM separation: The update interval for Surveillance Reports containing only ADS-B Identity data associated with any single aircraft shall be less than 100s with a probability of 95% (SPR-25 [Ref.1]).
Ground Time to alert for TMA	<b>SAF023.</b> For 3NM separation: The time to alert for a change in surveillance Emergency / SPI reports measured at point E2 shall be no longer than 5s for TMA (SPR-26 [Ref.1]).
Coverage	<b>SAF024.</b> The ADS-B ground infrastructure shall have sufficient coverage to assure that all aircraft transmitting ADS-B are acquired by ATC processing system prior to entering the defined airspace volume (ASSUMP-12 [Ref.1]).

**Table 12: Safety Requirements at ADS-B Receiver subsystem level**

**GM017.** SAF019 and SAF022 shall be considered by implementers when deciding on the extend of their coverage for initial acquisition and identification procedures.

**GM018.** The implementer shall ultimately consider the most demanding requirements regarding update date / loss of track information between SAF018 and SAF021 (success case) on the one hand and SAF051 in section 8.7 (failure case) on the other hand.

**GM019.** The above requirements have been allocated according to a functional architecture as described in [Ref.1] section 3, Figure 6. Implementers shall explicit the mapping of their physical architecture to this functional architecture model in order to propagate these requirements to their physical (local) elements.

**GM020.** It is recommended to use/apply EUROCAE ED-129 Technical Specification for 1090MHz Extended Squitter Ground Station.

**GM021.** Update rates in requirements are derived from that of the reference radar (10s). Implementers with reference radar having a different update rate should check the related impact on these requirements.

### 5.5.3.3 Safety Requirements at Aircraft Domain level

This section provides the safety requirements concerning the performances of provided data by the airborne domain (i.e. at point of measurement A1-D in Figure 1).

Note that different requirements are specified for the different conditions in which ADS-B separation services can be applied, i.e.:

- ▶ Aircraft requirements allowing to aircraft be eligible to receive 5NM separation services in en-route airspace,
- ▶ Aircraft requirements allowing aircraft to be eligible to receive 3NM separation services in terminal airspace

Parameter	ADS-B-NRA Performance Safety Requirement
Airborne Safety Requirements for ADS-B-NRA	
Pressure-Altitude Accuracy	<b>SAF025.</b> Altimeter accuracy - including accuracy of measurement and accuracy of reported value through use of encoding - shall be at least as good as Mode C provisions in ICAO Annex 10 [Ref.9] which specifies 38.1m (125ft) <sup>29 30</sup> (SPR-2 and SPR-6 [Ref.1]).

---

<sup>29</sup> This is minimum accuracy requirement for altimeter, and is dependent on the type of airspace. Many airspace regions, such as RVSM, will require better altimeter performance than specified here. In addition, as per Annex 10, Vol. IV (4.3.9.3.1.) it is recommended to use a source providing a resolution less than or equal to 7.62m (25ft).

<sup>30</sup> See also paragraph 8.5 of [Ref.14]

Parameter	ADS-B-NRA Performance Safety Requirement
Quality Indicator	<p><b>SAF026.</b> ADS-B transmit systems shall transmit horizontal position quality indicators consistent with the associated position information at the time of transmission (see GM022 below). For the expression of the position accuracy quality, the related indicator shall therefore reflect (§8.3.3 in [Ref.14]):</p> <ul style="list-style-type: none"> <li>▶ The quality of the position measurement itself; and</li> <li>▶ Any (uncompensated) latency incurring prior to transmission</li> </ul> <p><b>SAF027.</b> Horizontal position source failure probability shall be no more than 10<sup>-4</sup>/h</p> <p><b>SAF028.</b> Horizontal position source alert failure probability shall be no more than 10<sup>-3</sup> (per position source failure event)</p> <p><b>SAF029.</b> The time to alert regarding a change of the position quality indicator value shall be no more than 10s (SPR-4 and SPR-8 [Ref.1]).</p>
Airborne Domain Latency	<p><b>SAF030.</b> The Airborne Transmit Domain shall have a 95% latency of 1.5s or less for horizontal position and quality indicators (SPR-11 [Ref.1]).</p> <p><b>SAF031.</b> The Airborne Transmit Domain shall have a 99.9% of 3s or less for horizontal position ([Ref.14])</p> <p><b>SAF032.</b> For Pressure-Altitude, aircraft identification, mode A code, SPI and Emergency indicators, the Airborne Transmit Domain shall have a latency no greater than specified in current implementations for SSR (SPR-12 [Ref.1]).</p>
<p><b>Airborne Safety Requirements for being ADS-B-NRA eligible in en-route airspace (i.e. to be eligible to receive 5NM separation service)</b></p>	
Horizontal Position Accuracy for En-route	<p><b>SAF033.</b> In en-route airspace, the 95% accuracy of the horizontal position measured at D shall be less than 0.5NM (i.e. <math>NAC_p \geq 5</math>) (SPR-1 [Ref.1]).</p>
Horizontal Position Integrity for En-route	<p><b>SAF034.</b> In en-route airspace, Quality Indicators shall be <math>NIC_{p \geq 4}</math> (i.e. maximum 2.0 NM containment radius) or <math>NUC_p \geq 4</math> (maximum 1.0 NM containment radius) (SPR-3 [Ref.1]).</p>
<p><b>Airborne Safety Requirements for being ADS-B-NRA eligible in TMA airspace (i.e. to be eligible to receive 3NM separation service)</b></p>	
Horizontal Position Accuracy for TMA	<p><b>SAF035.</b> In TMA airspace, the 95% accuracy of the horizontal position measured at D shall be less than 0.3 NM (i.e. <math>NAC_p \geq 6</math>) (SPR-5 [Ref.1]).</p>

Parameter	ADS-B-NRA Performance Safety Requirement
Horizontal Position Integrity for TMA	<b>SAF036.</b> In TMA airspace, Quality Indicators shall be $NIC_p \geq 5$ (i.e. maximum 1.0 NM containment radius) or $NUC_p \geq 5$ (maximum 0.5 NM containment radius) (SPR-7 [Ref.1]).

**Table 13: Safety Requirements at Aircraft Domain level**

**GM022.** section 8 of [Ref.14] lists permissible deviations from the target requirements related to the use of existing aircraft installations in support of initial implementations. [Ref.14] states that these deviations are currently considered operationally acceptable under the assumption that the following ground mitigation means are implemented, at the discretion of the ANSP: in cases where position quality indicators are not consistent with actual position quality (e.g., due to uncompensated latency in position transmissions), the implementing ANSP might

- treat the higher quality indicator encodings as an advised lower one (e.g.  $NUC_p=7$  may be treated as  $NUC_p=5$ ) or,
- consider, for separation purpose, a quality indicator more stringent than the one stated in ED-126 (e.g.  $NUC_p=5$  rather than  $NUC_p=4$ ).

## 5.6 EXTERNAL ELEMENTS (ARG1.1.2.4)

Four main elements have been identified as external elements to ADS-B-NRA application:

- a) The air-ground communication
- b) The sector transfer operations
- c) The external positioning source (i.e. GNSS)
- d) The ground and airborne Safety Nets

**GM023.** The list presented here includes all relevant generic external elements considered. Implementers shall expand this generic list with those specific external elements related to local characteristics.

These elements are also part of the application. Due to their “external” nature, requirement has been assigned to them only when possible. When not possible, several assumptions have then been stated for each of these elements, in order to establish a baseline for the assessment of the Application. This baseline relates to their behaviour and to the information and services they can provide.

Nevertheless, it has to be noted that this document does not supersede all the assumptions made in the reference documents and in particular those from ED126/DO303 [Ref.1]I003).

### 5.6.1 Air ground communication

For air-ground communication aspects, the following Safety Requirement has been defined:

**SAF037.** Direct pilot-controller communications equivalent to the reference radar service case shall be established prior to the provision of ATS surveillance services, unless special circumstances, such as emergencies, dictate otherwise (PANS-ATM Paragraph 8.3.2.).

### 5.6.2 Sector Transfer operations

Concerning sector transfer aspects, and as explained in section 4.6 “the expected impact on adjacent sector due to the use of ADS-B surveillance is, in general equivalent, to that in the reference radar surveillance case”.

It is indicated in §A.3.4.8 in ED-126/DO-303 [Ref.1] that: “Existing coordination procedures in PANS-ATM Chapters 8 and 10 are not impacted on through the implementation of ADS-B in non-radar areas. It is assumed that prior to the aircraft leaving the ‘defined airspace volume’ within which the ADS-B service is being applied, the controller will establish the necessary separation standard applicable to the airspace the aircraft is entering, as per existing requirements for aircraft exiting radar coverage (i.e. PANS-ATM 10.4.1.3h)”.

Specific control procedures will be applied (as described in section 2) similar to those described in PANS-ATM [Ref.2] Chapter 8 and 10 (as indicated in §Table 10 from [Ref.1]):

- For traffic co-ordination (§8.7.4. (“Transfer Of Control”) of [Ref.2])
- For control transfer (§10.1.2.2. (“Transfer Of Control”) of [Ref.2])
- For Separation minima application (to establish appropriate procedural separation if next sector applies procedural control).
- For transfer of identification (§8.6.3 (“Transfer Of Identification”) of [Ref.2])

For transfer of identification, depending on whether the Mode A code is available or not in the ADS-B-NRA sector, either same procedures compared to the reference radar-based ATS can apply (including amongst other the transfer of identification based on Mode A code methods) or alternative procedures as described in section 8.6.3. (“Transfer Of Identification”) of [Ref.2]), in particular in section 8.6.3.2. where methods d, e and f can apply.

For separation provisions, no difference exists compared to the radar-based-ATS case.

Annex C describes the various cases illustrating this.

Thus, taking into account all of this, the following main safety requirements have been established concerning sector transfer aspects for ADS-B-NRA:

**SAF038.** The Flight Crew shall contact controller when entering the NRA airspace in accordance with existing radio procedures (e.g. after receiving radio frequency transfer instruction from a previous ATC unit and/or to obtain a clearance to enter the airspace) (ASSUMP-5 of [Ref.1]).

**SAF039.** Controllers shall follow existing procedures for coordination and transfer of aircraft. This particularly applies to coordinating appropriate information to downstream units and complying with local agreements established between ATC units regarding separation standards to be established prior to entry into a bordering ATC unit. In particular see ICAO requirements for “Coordination In Respect Of The Provision Of Air Traffic Control Service”) in [Ref.2] Chapter 10. (ASSUMP-6 of [Ref.1]).

**GM024.** ANSP shall comply with local agreements established between ATC units regarding separation standards to be established prior to entry into a bordering ATC unit.

**GM025.** ATS Implementers should assess the effect of the introduction of ADS-B in non radar airspace as being equivalent to the introduction of radar in a previously non-radar airspace. ATS Implementers should also consider the ramifications of the change of airspace status upon ATCO licensing, rating/sector qualifications, training and familiarisation and competence assessment processes in addition to operational procedure development



### 5.6.3 External Positioning Service - GNSS

For external positioning service aspects, the following assumption has been stated in order to ensure that position information is mainly provided by GNSS positioning service (availability of this external source):

**A004.** It is assumed that the GNSS constellation is sufficient to assure the availability of ADS-B integrity monitoring or equivalent capabilities confirming the integrity of the surveillance position data (ASSUMP-13 [Ref.1]).

**GM026.** Implementers shall demonstrate that assumption A004 above is valid and remains valid in its local environment.

**GM027.** Implementers may use RAIM prediction as a possible way to ensure availability of GNSS service in own local implementation, as the OSED in [Ref.1] assumes that the coverage is sufficient in terms of both range and availability of adequate data (ASSUMP-12 and ASSUMP-13 in [Ref.1]).

More information concerning GNSS failures and abnormal external conditions is provided for Arg1.1.4 in section 7.3.2 and 7.4.5.

### 5.6.4 Safety Nets

ADS-B-NRA does not require or assume **Ground Safety Nets** availability as explained in §A.3.3 in [Ref.1], and Ground Safety Nets will be dealt with when considering the ADS-B-ADD application<sup>31</sup> (Aircraft Derived Data).

In particular ADS-B-ADD will have to consider the specific potential errors from GNSS & Airborne failures modes which do not exist in the reference radar based situation and which could affect adversely the STCA or the MSAW.

**GM028.** Implementers for which the ATS system includes Ground Safety Nets shall assess the impact of potential GNSS and Airborne failure on such devices.

The use of ADS-B has no impact on the **Airborne Safety Nets** as the result of non-interference certification for ADS-B.

---

<sup>31</sup> ADS-B-ADD application covers Aircraft Derived Data for ATC tools

## **5.7 CONCLUSIONS ON ARG1.1.2 - DESIGN COMPLETENESS**

This section has provided adequate Argument and supporting Evidence that the ADS-B-NRA operational and technical boundaries are clearly defined. Related operations and functions are described and all related requirements and assumptions (concerning “Success Case”) have been specified for both internal and external elements, in accordance with the Safety Criteria (Cr001) specified in section 5.1.

Additional requirements are provided in sections 6 to 8 to cover the complementary aspects related to design correctness, design robustness and the mitigation of internal failure (covered under Arg1.1.3 to 1.1.5 respectively).

## 6 ADS-B-NRA DESIGN CORRECTNESS (ARG1.1.3)

The objective of this section is to show that the ADS-B-NRA design functions correctly and coherently under all normal<sup>32</sup> environmental conditions.

The main question here is whether the opportunity to reduce risk has been maximised, considering the full range of conditions that the system is likely to be subjected to in its operational environment.

### 6.1 SAFETY CRITERIA

The Safety Criteria considered for this argument Arg1.1.3 are the same as for Arg1.1.1, i.e. the combination of main Safety Criterion Cr001 and Cr003 (*Success Case*), i.e.:

Cr001 No higher than the equivalent risk associated with “reference service” – i.e. radar-based surveillance, including separation service provided by ATS (for the given set of separation minima).

Cr003 Reduced as far as reasonably practicable.

### 6.2 STRATEGY

The key elements to be addressed here are the internal coherency of the system, and the dynamic behaviour of the system. It needs to demonstrate that the functionality and data would remain consistent throughout the system, over the full range of conditions to which the system is expected to be subjected in its operational environment. In particular the following questions need to be addressed:

- Are the specified procedures coherent?
- Are the human actions coherent?
- Are the same data about the flight / intentions held by the various actors?
- Are there any undefined states of the system?

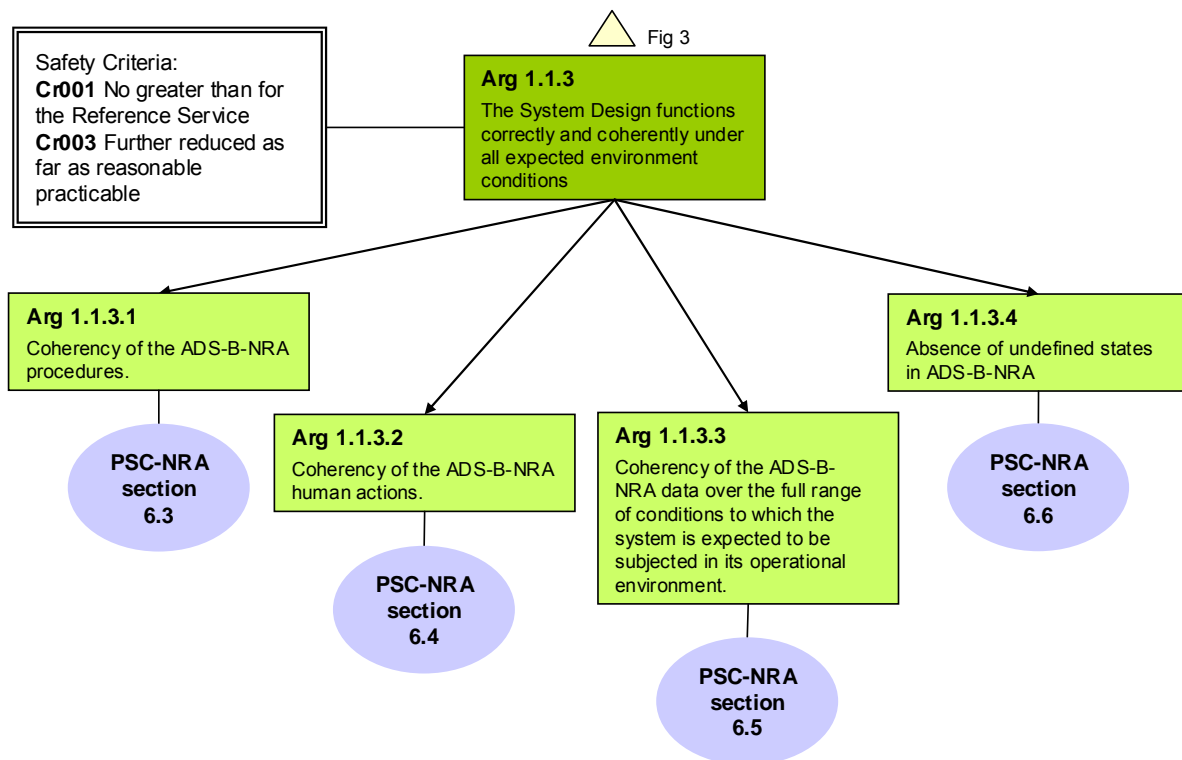
The strategy for satisfying Arg1.1.3 is to provide Evidence that the following lower-level Arguments are true:

- a) **Arg 1.1.3.1.** ADS-B-NRA procedures are coherent over the full range of conditions to which the system is expected to be subjected in its operational environment.
- b) **Arg 1.1.3.2.** ADS-B-NRA human actions are coherent.

---

<sup>32</sup> Abnormal conditions are addressed under Arg1.1.4 in section 7. The distinction between *normal* and *abnormal* is not important provided all issues are addressed by the two sub-Arguments.

- c) **Arg 1.1.3.3** ADS-B-NRA data is coherent over the full range of conditions to which the system is expected to be subjected in its operational environment.
- d) **Arg 1.1.3.4.** All the states in ADS-B-NRA has been defined (absence of undefined states).



**Figure 7: Decomposition of Argument on Design Correctness (Arg1.1.3)**

These are addressed in turn, in sections from 6.3 to 6.6 below. Conclusions regarding Arg1.1.3 are then drawn, in section 6.7.

### 6.3 COHERENCY OF THE ADS-B-NRA PROCEDURES (ARG1.1.3.1)

The approach developed in Annex A of [Ref.1] is to assume that the proposed PANS-ATM procedures as developed in [Ref.2] are fully applicable for ADS-B-NRA and that no specific procedures beyond these are required. Coherency of the procedures over the full range of conditions to which the system is expected to be subjected in its operational environment are therefore ensured through the coherency of the PANS-ATM procedures, which have been derived from radar procedures. Then, Safety Criteria Cr001 satisfied for this argument Arg 1.1.3.1.

#### 6.4 COHERENCY OF THE ADS-B-NRA HUMAN ACTIONS (ARG1.1.3.2)

As indicated in annex §A3.4.6. of [Ref.1], “*there is no change in the roles and responsibilities of the aircrew or controllers*” compared to reference radar-based ATS. Therefore Safety Criteria Cr001 is satisfied based on the following assumptions:

**A005.** With the exception of quality indicator (QI) management, it is assumed that there is no major change regarding ATCo actions for ADS-B-NRA compared to those performed in the reference radar-based ATS.

In case the QI management is implemented through “coasting” by the ground system, there is no major change compared to radar-based ATS (see in that case the resulting requirement SAF052 for the ATC processing system). Otherwise the following guidance applies:

**GM029.** Implementer shall ensure that Human Factors are taken into account concerning the operational management of quality indicators by the controllers. See also “Guidance for the Provision of Air Traffic Services Using ADS-B in Non Radar Area” [Ref.11].

**A006.** With the exception of the aircraft identification (see FC manual [Ref.10] section §6), it is assumed that there is no change regarding pilot action for ADS-B-NRA and the same functionality is applied regarding emergency situation, Mode A code change, SPI or deselection of the Pressure-Altitude.

Extract from FC manual [Ref.10] section §6:

*“Before departure:*

- *The flight crew should verify the consistency between its ADS-B related avionics capabilities and the data inserted in the flight plan.*
- *The aircraft identification as inserted into the system (FMS, etc;) should be consistent with the one inserted in the flight plan, as it is the one that will be transmitter by the ADS-B system.”*

#### 6.5 COHERENCY OF THE ADS-B-NRA DATA (ARG1.1.3.3)

The key issue developed in this section relates to data required for the various actors to operate under the ADS-B-NRA application. The ADS-B-NRA application relying on the broadcast of data from the aircraft (Airborne domain as depicted in Figure 1) to the ground system (ground domain as depicted in Figure 1), the key question relates here to the interoperability between these two elements.

This aspect have been addressed in §4 of [Ref.1], through the Interoperability requirements, to ensure that exchanged data and information are indeed mutually consistent between airborne and ground views over the full range of

conditions to which the system is expected to be subjected in its operational environment. In the case of surveillance, this range of conditions mainly relates to traffic conditions and to GNSS constellation.

Data Items broadcast from the Airborne Domain to the Ground Domain can be split into two categories that are addressed in the following sections:

- a) Data Items for which the provision can be directly compared to the reference radar service (Pressure-Altitude, Emergency codes and SPI) and therefore where the Safety Criteria Cr001 will apply.
- b) Data Items for which the provision is specific to ADS-B (Identity, 24 bit address, Horizontal Position and Position Quality Indicator) and therefore where Safety Criteria Cr003 will apply.

#### **6.5.1 Data Items for which the provision can be directly compared to those of the reference radar service**

The following is only an example of interoperability requirements obtained for ADS-B-NRA concerning ground reception and airborne transmission, as an illustration of how appropriate interpretation of the data is ensured by comparison to the reference radar service (the entire list is available in §4 and annex §D.3 of [Ref.1]):

- **IR-11:** The Transmit Aircraft Domain shall formulate altitude measurements as barometric altitude relative to a standard pressure of 1013.25 hectopascals (29.92 in Hg).
- **IR-13:** The Ground Domain shall interpret barometric altitude as altitude relative to a standard pressure of 1013.25 hectopascals (29.92 in Hg).[...]

ED126/DO303 [Ref.1] includes interoperability requirements for all data items for which the provision can be directly compared to the reference radar service, and then it can be concluded that both airborne and ground domains in the system are operating in a consistent manner, based on consistent data and consistent data interpretation.

#### **6.5.2 Data Items for which the provision is specific to ADS-B**

The following are only examples of interoperability requirements obtained for ADS-B-NRA concerning ground reception and airborne transmission, as an illustration of how appropriate interpretation of the data is ensured (the entire list is available in §4 of [Ref.1]):

- **IR-6:** The Transmit Aircraft Domain shall provide an ADS-B message containing the aircraft identification (OR-1 ASSUMP-11 from [Ref.1] ).  
**Note:** The ATC Processing System may use the aircraft identification to

associate ADS-B Surveillance reports to internal flight information (e.g., to a surveillance track).

- **IR-7:** As per ICAO Doc. 4444, PANS/ATM the following definitions shall be applied by the Transmit Aircraft Domain:
  - (Chapter 1, Definitions) Aircraft Identification is 'A group of letters, figures or a combination thereof which is either identical to, or the coded equivalent of, the aircraft call sign to be used in air-ground communications, and which is used to identify the aircraft in ground-ground air traffic services communications',
  - (Appendix 2, 2.2) one of the following aircraft identifications, not exceeding 7 characters:
    - the registration marking of the aircraft (e.g. EIAKO, 4XBCD, N2567GA), or
    - the ICAO designator for the aircraft operating agency followed by the flight identification (e.g. KLM511, NGA213, JTR25) when in radiotelephony the call sign to be used by the aircraft will consist of the ICAO telephony designator for the operating agency followed by the flight identification (e.g. KLM511, NIGERIA 213, HERBIE 25).
  
- **IR-5:** The Transmit Aircraft Domain shall provide the 24 bit aircraft address within each ADS-B message. Note 1: ICAO Doc.4444 PANS/ATM (Chapter 1, Definitions) defines the aircraft address as “a unique combination of 24 bits available for assignment to an aircraft for the purpose of air-ground communications, navigation and surveillance”.[...]

ED126/DO303 [Ref.1] includes interoperability requirements for all data items for which the provision is specific to ADS-B, and then it can be concluded that both airborne and ground domains in the system are operating in a consistent manner, based on consistent data and consistent data interpretation.

## **6.6 ABSENCE OF UNDEFINED STATES IN ADS-B-NRA (ARG1.1.3.4)**

Table 6 in this document is an extract from Figure 9 of [Ref.1] that aims at identifying all the various control phases for the use of ADS-B surveillance to support the provision of ATC/separation tasks and alerting services.

Due to the fact that all these phases (Initiation, Provision of service and Termination phases of the ADS-B based services) together with expected and unexpected cases have been covered, it can be concluded that there is an absence of undefined states. These phases have been documented based on similar reference radar service phases, applying Safety Criteria Cr001.

## **6.7 CONCLUSIONS ON ARG1.1.3 - DESIGN CORRECTNESS**

This section has provided adequate Argument and supporting Evidence that the ADS-B-NRA design functions correctly and coherently under all normal environmental conditions.

Coherency of the procedure, human actions and data items have been discussed either by direct comparison with the reference radar service, thus applying Safety Criteria Cr001, or by showing in the case of specific ADS-B data items how coherency is provided, thus applying Safety Criteria Cr003. This shows the ADS-B-NRA design correctness.

Next, section 7 considers the reaction of the system to abnormal events in its operational environment.



## 7 DESIGN ROBUSTNESS (ARG1.1.4)

The objectives of this section are to show that the Application system design is robust against external abnormalities in the operational environment.

### 7.1 SAFETY CRITERIA

The Safety Criteria considered for this argument Arg1.1.4 are the same as for Arg1.1.1, i.e. the combination of main Safety Criterion Cr001 and Cr003 (*Success Case*), i.e.:

Cr001 No higher than the equivalent risk associated with “reference service” – i.e. radar-based surveillance, including separation service provided by ATS (for the given set of separation minima).

Cr003 Reduced as far as reasonably practicable.

### 7.2 STRATEGY

The reaction of the system to abnormal events in its operational environment was considered from the following perspectives:

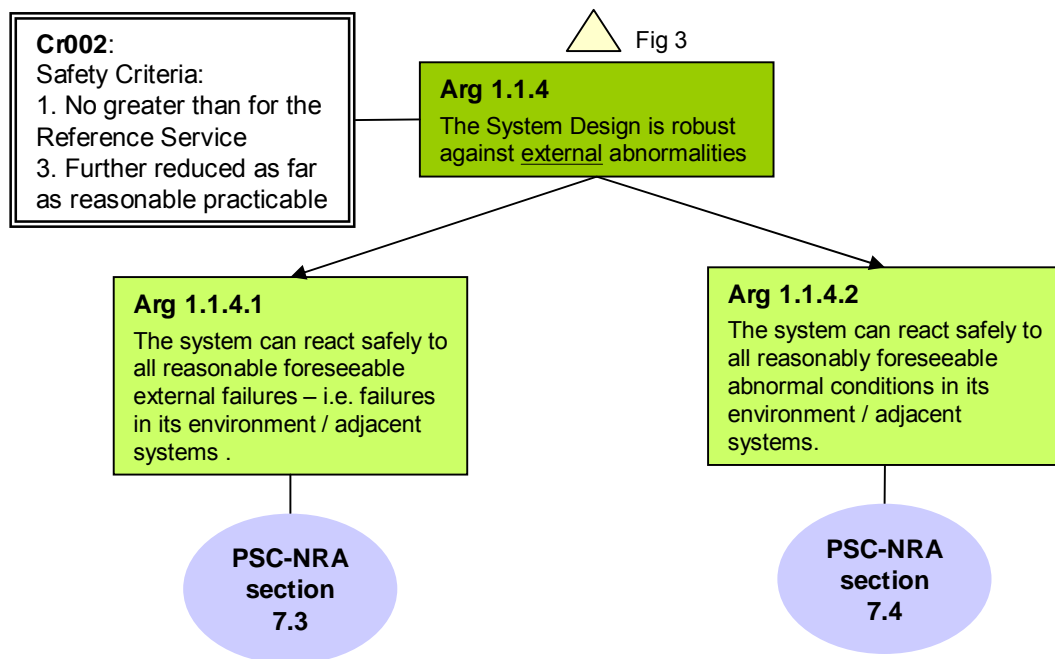
- Can the system continue to operate?
- Could such conditions cause the system to behave in a way that introduces additional risk?

The strategy for satisfying Arg1.1.4 is to provide Evidence that both of the following lower-level Arguments are true:

- a) **Arg 1.1.4.1.** The system can react safely to all reasonably foreseeable external failures<sup>33</sup>.
- b) **Arg 1.1.4.2.** The system can react safely to all other reasonably foreseeable abnormal external conditions.

---

<sup>33</sup> Failures internal to the system are addressed under Arg1.1.5, in section 8 below.



**Figure 8: Decomposition of Argument on Design Robustness (Arg1.1.4)**

These are addressed in turn, in sections 7.3 and 7.4 below. Conclusions regarding Arg1.1.4 are then drawn, in section 7.5.

### 7.3 REACTION TO EXTERNAL FAILURES (ARG1.1.4.1)

The failures external to the application have been identified, either through direct comparison with those having the same impact as for the reference radar service case, or by considering those having an impact on the ADS-B system only:

- a) External failures having the same impact as for the reference radar service case are Voice Communication failures and Aircraft failures.
- b) External failure having an impact on the ADS-B system only are those relating to GNSS.

**GM030.** The failures related to the specific external elements related to local characteristics identified by implementer (see GM023) shall also be taken into account and assessed here.

### 7.3.1 Voice Communication and Aircraft failures

#### Voice communication failure

Concerning this external failure, it has been asserted that:

**A007.** Because voice communication is entirely independent of the ADS-B application, then it is assumed that the likelihood of voice-communication failure would be no greater than for the reference radar-based ATS case (see Table-8 from [Ref.1] and [Ref.12]).

Further, in case of voice communication failure, the following safety requirements have been defined to be applied:

**SAF040.** Concerning procedures in case of voice communication failure, the same contingency procedure as for reference radar services shall apply (PANS ATM).

**SAF041.** In the event of complete failure of the ground radio equipment used for communication, the controller shall, unless able to continue to provide the ATS surveillance service by means of other available communication channels, proceed as follows (PANS-ATM 8.8.6.1.):

- a) Without delay inform all adjacent control positions or ATC units, as applicable, of the failure;
- b) Appraise such positions or units of the current traffic situation;
- c) Request their assistance, in respect of aircraft which may establish communications with those positions or units, in establishing and maintaining separation between and maintaining control of such aircraft; and
- d) Instruct adjacent control positions or ATC units to hold or reroute all controlled flights outside the area of responsibility of the position or ATC unit that has experienced the failure until such time that the provision of normal services can be resumed.

Therefore, the system is no less robust against voice-communications failure than is the reference radar service situation.

**GM031.** In order to reduce the impact of complete ground radio equipment failure on the safety of air traffic, the appropriate ATS authority should establish contingency procedures to be followed by control positions and ATC units in the event of such failures. Where feasible and practicable, such contingency procedures should provide for the delegation of control to an adjacent control position or ATC unit in order to permit a minimum level of services to be provided as soon as possible, following the ground radio failure and until normal operations can be resumed (PANS-ATM 8.8.6.1)

### **Aircraft failure**

In case of aircraft failure (e.g. engine failure), this would involve application of the same procedures as today's reference radar-based operations. As for previous external failure, it has been asserted that:

**A008.** Because the aircraft failures are independent of ADS-B operations, then the likelihood of such failures would be no greater than for the reference radar-based ATS case.

**Note:** This statement excludes common mode of failure (related to positioning) between navigation and surveillance that is addressed in section 8.6 as hazard cause.

Therefore, the system is no less robust against aircraft failures than is the reference situation.

### **7.3.2 Satellite constellation (GNSS) failures**

This section lists the assumptions related to the performance / failure of the GNSS system. The reaction of the system to these external failures is addressed in section 8 (Mitigation of Internal Failures (Arg1.1.5)) as GNSS, although an external system is also a failure cause considered in the safety assessment.

In case of GNSS detected failure impacting ADS-B-NRA application, ATS can continue to be provided by applying procedural control (as indicated by Safety Requirement SAF046 in section 8.4.3) in this failure situation, and as stated by ASSUMP-7 in ED126/DO303 [Ref.1]:

**A009.** The navigation capability of the aircraft is assumed to be sufficient to enable the pilot to comply with a basic procedural separation service (e.g. DME, VOR, NDB, pressure-altitude) thus allowing time, vertical and some lateral distance separation standards to be applied.

For more detail, see navigation infrastructure description in Table-8 of [Ref.1], as well as explanations provided in §A.3.7, in §A.3.8 and in §C.3.2 of [Ref.1].

It is however assumed that the likelihood for this GNSS failure is rare:

**A010.** It is assumed that the integrity failure rate where multiple a/c are affected, for any GNSS system used as position source is no more than 10<sup>-5</sup> per hour (ASSUMP-28 in [Ref.1]).

**A011.** It is assumed that the integrity failure rate of the horizontal position source impacting one aircraft is no more than 10<sup>-4</sup> per user (ASSUMP-29 in [Ref.1]).

## 7.4 REACTION TO ABNORMAL EXTERNAL CONDITIONS (ARG1.1.4.2)

The following possible abnormal conditions have been identified:

- ▶ Aircraft Emergencies
- ▶ Adjacent sector(s) failure
- ▶ Capacity overload
- ▶ Extreme Weather
- ▶ Satellite Constellation

The corresponding assumptions and requirements that apply for each case are presented in the following subsections (from 7.4.1 to 7.4.5).

### 7.4.1 Aircraft Emergencies

The same emergency conditions are expected to occur for ADS-B-based ATS as for the reference radar-based ATS, and also displayed to controller in the same way – i.e. emergency status, as indicated in §A.3.4.2.7 of [Ref.1]. A set of operational requirements (listed in §A.3.9.10 of [Ref.1]) have been determined related to this issue:

**SAF042.** Whenever the capability for the pilot to select discrete emergency code is available the ADS-B system shall transmit the appropriate discrete emergency and/or urgency modes. These discrete emergency and/or urgency modes are (OR-5 in [Ref.1]):

- a) Emergency modes:
  - ▶ Emergency
  - ▶ Communication failure
  - ▶ Unlawful interference
- b) Urgency modes:
  - ▶ Minimum fuel
  - ▶ Medical

**SAF043.** Indication that an aircraft is transmitting an emergency and/or urgency mode shall be displayed to the controller in a clear and expeditious manner (OR-6 in [Ref.1]).

### 7.4.2 Adjacent sectors failures

The abnormal environmental condition related to adjacent sectors failure may occur, in the same way as for the reference radar-based service.

Then, in case of a more severe failure occurs (e.g. ACC failure) resulting in a significantly reduced operational availability of an alternate procedure (e.g. evacuation of the adjacent centre) contingency procedures in the adjacent sector will apply. EC2096/2005 [Ref.12] relates to Contingency Plans for all

services provided in adjacent sectors in the case of events which result in significant degradation or interruption of its services.

#### **7.4.3 Capacity Overload**

This case corresponds to the situation where traffic demand exceeds ATC sector capacity. The following statement applies:

**A012.** It is assumed that the management of demand versus capacity (e.g. Flow Management Function) is implemented for the ADS-B-NRA sector as it would be implemented in the reference radar-based ATS (see Guidance for the Provision of Air Traffic Services Using ADS-B in Non Radar Area [Ref.11]).

ADS-B-NRA is considered to be applicable to areas of low density traffic, but implementation is assumed to be able to accommodate higher levels of traffic (see section 2.1), and provisions have been made in the assessment of this application to ensure this. The defining factor is then more related to operational aspects than to technical limitations.

#### **7.4.4 Extreme Weather**

In terms of the high level design, there is nothing to indicate that the system will be any less robust to extreme weather conditions than the reference radar system.

**GM032.** Robustness of the physical system (against e.g. lightning, extreme temperature phenomena) will have to be considered at local specification level as it is closely related to the environment in which the application is going to be used.

#### **7.4.5 Abnormal Satellite Constellation Condition**

Beyond the satellite constellation failure which is described in section 7.3.2, one additional abnormal external condition relates to the degradation of the satellite constellation.

Contingency procedures are required to cover this case.

**GM033.** In order to reduce the impact of a degradation of aircraft position source data, the appropriate ATS authority shall establish contingency procedures to be followed by controlled positions and ATC units in the event of data degradation.

## 7.5 CONCLUSIONS ON ARG1.1.4 - DESIGN ROBUSTNESS

This section addresses the reaction of the system to abnormal events when both external failures and other abnormal environmental conditions have been considered.

Adequate Evidence that the ADS-B-NRA application design is as robust against external failures as reference radar system has been provided when direct comparison with radar situation is appropriate

Adequate Evidence that the ADS-B-NRA application design is robust against external failures which are unique to the ADS-B-NRA case has also been provided.

Similarly robustness on other abnormal external conditions has been demonstrated in principle, subject to confirmation at the physical implementation stage.

Next, section 8 considers the risks associated with internal failure of the system.

Page intentionally left blank



## 8 MITIGATION OF INTERNAL FAILURES (ARG1.1.5)

The objectives of this section are to show that all risks from internal system failure have been mitigated sufficiently.

### 8.1 SAFETY CRITERIA

The Safety Criteria considered for this argument Arg1.1.5 are the combination of main Safety Criterion Cr001, Cr002 and Cr003, i.e:

Cr001 No higher than the equivalent risk associated with “reference service” – i.e. radar-based surveillance, including separation service provided by ATS (for the given set of separation minima).

Cr002 Within an appropriate portion of the relevant Target Levels of Safety.

Cr003 Reduced as far as reasonably practicable.

### 8.2 STRATEGY

Internal failure of the system has been assessed from the perspective of how anomalous behaviour of the system could induce risks that might otherwise not occur. Common<sup>34</sup> mode failures have also been assessed.

The strategy is to focus on separation service (**St001**), assuming that:

**A013.** Separation service (airspace classes A - E) provides the most demanding requirements, compared to flight information and other services provided by ADS-B-NRA (ASSUMP-34 in ED126 [Ref.1]).

**GM034.** The implementer has to decide at local level whether services other than separation (e.g. FIS and Alerting) have to be considered for providing additional or more demanding requirements at a local level

Based on conclusions presented in section 4, the data items identified as being specific to ADS-B are mainly the horizontal position, its associated quality indicator, and the aircraft identification information. The other data items (pressure-altitude, SPI, Emergency modes) are quite similar to those used in the reference radar environment.

Then, and based also on previous assumption A013, internal system failure in this Arg1.1.5 will mainly focus on horizontal position and associated quality indicator items, as they are the main parameters to be considered for ADS-B-NRA separation services. In this case the absolute strategy will be considered

---

<sup>34</sup> Common with one or more non ADS-B functions

in the analysis (i.e. safety Criteria Cr002) as this is a specific ADS-B parameter.

Quality indicator parameter will then also be considered, except for those aspects relating to the QI management (not related to the position itself, but to the provision, or not, of the information on the ATCo interface as specified by SAF006 and SAF007) and to the potential associated failures (e.g. oscillation of QI value) as this aspect is very dependent upon the local implementation of the application. Thus, no further analysis is developed here; it needs to be considered at local level.

**GM035.** Implementers shall then address those aspects relating to the QI management (e.g. the provision or not of the information on the controller interface) and to the potential associated failures (e.g. oscillation of QI value) which have not been considered in this generic Preliminary Safety Case as they are very dependent upon the local implementation of the application.

Concerning the other data items (pressure-altitude, Identification, emergency modes, 24bit address), they have been considered as being less related to horizontal separation services. Besides, potential hazards related to these parameters have been assumed to be similar to those already encountered in the reference radar environment and have therefore been analysed in comparison to the reference radar-based situation (and Mode S for the identity). More explanation on these hazards is presented in §C.7.6 and in §Table 57 of ED-126/DO-303 [Ref.1] and detailed corresponding specification is presented in [Ref.14].<sup>35</sup>

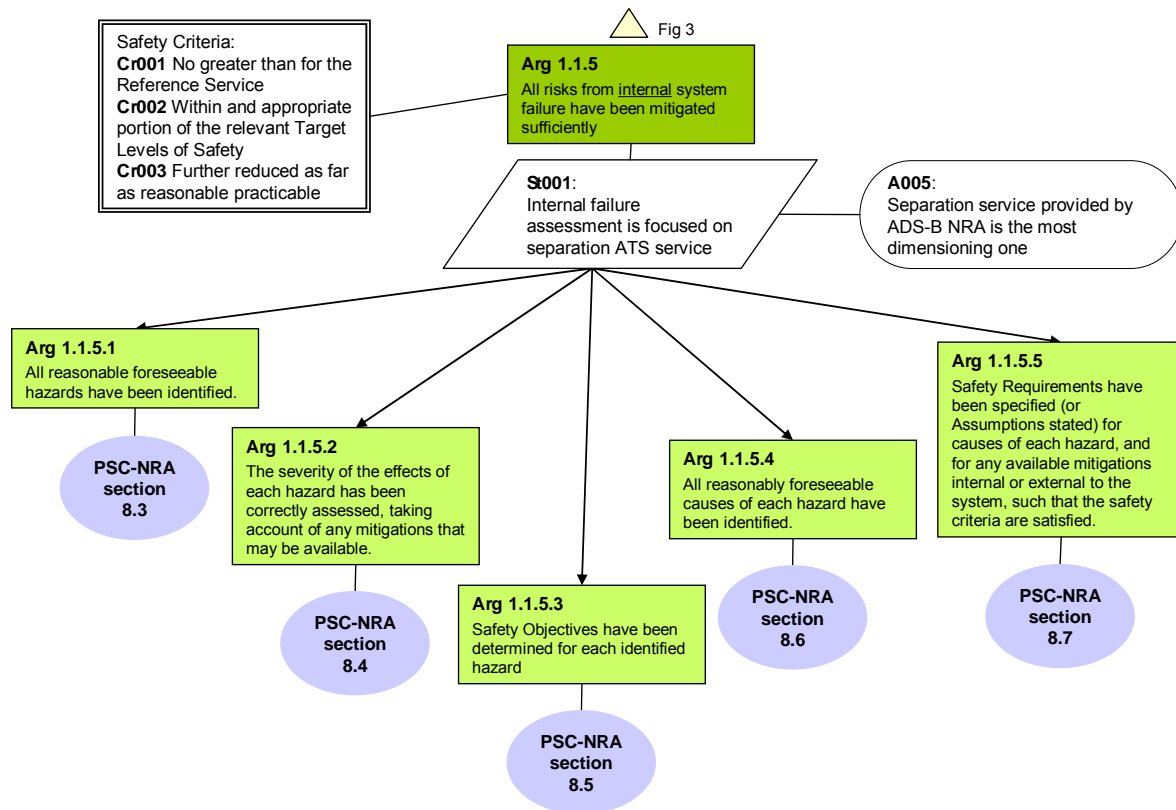
Based on that the above, what is proposed to satisfy Arg1.1.5 is to provide Evidence that the following lower-level Arguments are true, in line with previous assumption A013 and strategy presented above (i.e. mainly addressing horizontal position parameter in separation services provided by ADS-B-NRA):

- a) **Arg 1.1.5.1.** All reasonably foreseeable hazards have been identified.
- b) **Arg 1.1.5.2.** The severity of the effects of each hazard has been correctly assessed, taking account of any mitigation that may be available (external mitigation means and environmental conditions).
- c) **Arg 1.1.5.3** Safety Objectives have been determined for each identified and assessed hazard.
- d) **Arg 1.1.5.4.** All reasonably foreseeable causes of each hazard have been identified, including common mode of failure, together with internal mitigation means.

---

<sup>35</sup> Required integrity performance for individual ADS-B data item (airborne domain) is detailed in the [Ref.14] (EASA Acceptable Means of Compliance (AMC) 20-24)

- e) **Arg 1.1.5.5.** Safety Requirements have been specified (or Assumptions stated) for the causes of each hazard, such that the safety criteria (Cr002 & Cr003) are satisfied.



**Figure 9: Decomposition of Argument on Internal Failures Mitigation (Arg1.1.5)**

These Arguments presented above are addressed in turn, in sections 8.3 to 8.7 below.

Conclusions regarding Arg1.5 are then drawn, in section 8.8.

### 8.3 HAZARDS IDENTIFICATION (ARG1.1.5.1)

Potential hazards have been identified based on brainstorming sessions in which operational and safety experts participated. See ED-126/DO-303 §C.3.1 [Ref.1]. These hazards are defined at Controller Working Position (CWP) level and apply for both En-route and TMA.

The Hazards identified during these sessions are as follows:

OH #	OH description
OH1	Sudden and unexpected loss of position information for a <u>single aircraft</u> previously identified in the sector.
OH1-d	Detected by the ATCo
OH1-u	Undetected by the ATCo
OH2	Sudden and unexpected loss of position information for <u>multiple aircraft</u> previously identified in the sector.
OH2- d	Detected by the ATCo
OH3	Incorrect position information for <u>multiple aircraft</u> in a wide area is presented on the CWP
OH3-1d	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Detected by the ATCo
OH3-1u	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Undetected by the ATCo
OH3-2d	Horizontal position error resulting from a corruption of the position information. Detected by the ATCo
OH3-2u	Horizontal position error resulting from a corruption of the position information. Undetected by the ATCo
OH3-3d	Incorrect horizontal position error as a result of a corrupted quality indicator. Detected by the ATCo
OH3-3u	Incorrect horizontal position error as a result of a corrupted quality indicator. Undetected by the ATCo
OH4	Incorrect position information for <u>single aircraft</u> is presented on the CWP
OH4-1d	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Detected by the ATCo
OH4-1u	Horizontal position error resulting from a GNSS position source

OH #	OH description
	error not detected by the aircraft integrity monitoring. Undetected by the ATCo
OH4-2d	Horizontal position error resulting from a corruption of the position information. Detected by the ATCo
OH4-2u	Horizontal position error resulting from a corruption of the position information. Undetected by the ATCo
OH4-3d	Incorrect horizontal position error as a result of a corrupted quality indicator. Detected by the ATCo
OH4-3u	Incorrect horizontal position error as a result of a corrupted quality indicator. Undetected by the ATCo

**Table 14 : ADS-B-NRA Hazards list**

Note: hazards detected “too late” have been conservatively considered as being undetected

During cause identification and assessment of these hazards, common modes of failure have also been considered, especially for OH3 and OH4. Although sustained error affecting independently either Surveillance or Navigation capability could help as detection mechanism for pilot and ATCo, Appendix C1.3.1.3 in [Ref.1] assumes the most pessimistic assumption which is that the incorrect position will always affect both navigation and surveillance and, as such, is unable to be detected by pilot or ATCo (see Case 1 below).

For OH3 and OH4, different cases have been identified, leading to considering them as different hazards as presented here-after:

**Case 1:** In this case, incorrect position is due to a failure in the horizontal position source (e.g. GNSS), which produces an incorrect position combined to a failure by the on-board position integrity monitoring function (e.g. RAIM) to detect the loss of integrity in the position source.

**Case 2:** This case concerns the corruption of the (good) horizontal navigation position by either the on-board avionics or the ADS-B ground processing system, i.e. the position is corrupted by a software or hardware fault on board the aircraft or in the ground processing system.

**Case 3:** This fault concerns the corruption of the quality indicator by either the on-board avionics or the ADS-B ground processing system (system integrity failure).

A detailed description of each hazard is available in sections §C.7.2 to §C.7.6 of ED-126/DO-303 [Ref.1], dedicating a specific sub-section for detected and undetected cases when relevant (e.g. section §C.7.4.4 describes the OH3u2: Undetected case of incorrect position information for multiple aircraft in a wide-area is provided to controller - scenario 2 (corruption of the position)).

**GM036.** The ED126/DO303 operational hazard assessment has relied heavily on the involvement of qualified operational staff (mainly ATCOs) supported by Safety experts. Local implementers may nevertheless identify new – local – hazards which have not been considered in the generic case or may even reconsider the severity of the potential effects of identified hazards (e.g. because of significant differences in traffic conditions) or the consideration in the specific local case of the exposure time (in this document hazards being detected “too late” have conservatively been considered as being undetected hazards which may result in making the safety argument more difficult than necessary in some case, where exposure is limited).

**GM037.** Additional hazards resulting from the partial equipage issue (see also GM003) will have to be equally considered. Assuming that the ED126/DO303 safety approach is followed (see section 3.4.2 above), the inclusion of such new operational hazards or severities in the OSA would have to be performed consistently with the methodology adopted (see [Ref.1] particularly sections 2 and 3 of Annex C).

## 8.4 HAZARDS ASSESSMENT AND SEVERITY ASSIGNMENT (ARG1.1.5.2)

Hazards OH1 to OH4 from Table 14 above are directly related to ADS-B specific functions part of ADS-B-NRA for separation services, in particular those dealing with the provision of aircraft position by the aircraft itself and have therefore been thoroughly analysed, from severity assignment up to the derivation of the corresponding ADS-B specific requirements.

### 8.4.1 Hazard Assessment

Concerning hazards OH1 to OH4 (addressing loss or corruption of aircraft position), a thorough assessment has been performed as explained in section §C.2.1 of [Ref.1], by identifying all the potential effects of each hazard, based on operational and safety expertise judgement. The worst credible effects identified for each hazard are summarised in Table 17 below.

Hazards have been assessed based on the following assumption:

A019: ATCo is assumed to be applying the minimum surveillance separation standard applicable for the airspace (e.g. 5Nm) (EC-4 of [Ref.1]).

This assumption has been considered in the assessment of all the operational hazards, and constitutes a worst case situation.

Mitigation means (including procedural and environmental factors) having an impact on the severity of the effects of hazards have been identified and taken into account. The list of these External Mitigation Means and Environmental Conditions is provided in next section 8.4.3.

### 8.4.2 Severity Assignment

Each hazard is then classified according to the severity of their operational “worst credible effect” as per a common classification scheme (from severity 1, accident, to severity 5, no safety impact). This scheme is presented in Annex A , and it is compliant with ESARR4. Severity classes finally assigned for each hazard are included in Table 17 below.

The “worst credible effect” has been determined taking into account various components of the environmental characteristics, in particular traffic numbers, assuming that they are at their “worst” at the time of the failure. Hence, the following statement has been considered:

**A014.** For the severity classification it has been assumed that the ATCo is managing a high number of aircraft peaking at 15 for en-route and 7 for TMA (see EC-3<sup>36</sup> of [Ref.1])

---

<sup>36</sup> EC-3 is also presented in Table 16 : Safety Requirements and Assumptions relating to External Mitigation Means  
of PSC-NRA document.

Note: Implementing guidance concerning this item is available in GM040.

The effects assessment of each hazard (for detected and undetected cases when relevant), as well as the severity assigned as a result of this assessment are presented in a specific sub-section of the corresponding hazard assessment section in ED126/DO303 [Ref.1] (e.g. §C.7.5.3.2 provides the description of the effects of the OH4 detected case scenario 2 and its severity).

**GM038.** [Ref.1] analysis has been considering the “worst credible effect” approach. It is however recommended, when considering the updated hazard identification (as per GM036 and GM037) to expand the analysis to cover in addition to the worst credible effect all possible other effects and demonstrate that way in the local environment the worse hazard-effect pairs

### 8.4.3 Mitigation Means identification: EMM and EC

As mentioned before, *Environmental Conditions (EC)* and *External Mitigation Means (EMM)* are identified during the assessment of the hazards effects and taken into account for the severity assignment and Safety Objective allocation process (this latest process is explained in section 8.5.2).

These mitigation means are listed in the following tables. They are expressed in the form of a requirement or an assumption depending on the nature of the mitigation means:

Environmental Conditions	
<b>SAF044.</b>	Direct Controller Pilot Communication (VHF) shall be available in order to ensure that the ATCo has means to advise the pilot and issue instructions for the establishment of alternate separation standard (EC-1 of [Ref.1]).
<b>SAF045.</b>	System segregation of route structure (e.g. SID/STAR separation, one way routes, and level assignment in accordance with the Table of Cruising Levels as specified in ICAO Annex 2 Appendix 3 and where applicable as provided for in ICAO Doc 9574 for RVSM implementations between FL290 and FL410 inclusive) shall exist. <u>Note</u> : Although it is difficult to measure, these can have a significant impact on the hazard if implemented into the environment concerned (EC-2 of [Ref.1]).
	Traffic conditions for the NRA airspace have been assumed to be (EC-3 of [Ref.1]):
<b>A015.</b>	The average duration of a flight within a single ATC sector is assumed to be 20 minutes for en-route and 6 minutes for TMA.
<b>A016.</b>	The average number of aircraft assumed to be managed per ATSU.hour is 30 for en-route and 10 for TMA (resulting in the following



equivalences: 1 ATSU.h = 10 flight.h for en-route and 1 ATSU.h = 1 flight.h for TMA).

**A017.** The maximum instantaneous count of traffic is assumed to be at any one time 15 aircraft for en-route and 7 aircraft for TMA.

**A018.** 100% of these aircraft are under ADS-B surveillance.

(For A018 see guidance box GM037).

**A019.** ATCo is assumed to be applying the minimum surveillance separation standard applicable for the airspace (e.g. 5Nm) (EC-4 of [Ref.1])

**Table 15 : Safety Requirements and Assumptions relating to Environmental Conditions**

Note: the environmental conditions presented in assumptions from A015 to A017 are used for the assessment of the hazards effects as described in previous sections but they are also used for the unit conversion between flight.hours and ATSU.hours units (as described in section 8.5.1).

#### **External Mitigation Means**

**SAF046.** ATCo shall apply alternate separation (e.g. procedural time or distance separation standards) after detection of loss of position for a single aircraft (OH1d) or multiple aircraft (OH2d), and incorrect position for a single aircraft (OH4d1, OH4d2, OH4d3) or multiple aircraft (OH3d1, OH3d2, OH3d3) (EMM-1 of [Ref.1]).

This mitigation means is based on the following statement (already presented in section 7.3.2):

**A009.** The navigation capability of the aircraft is assumed to be sufficient to enable the pilot to comply with a basic procedural separation service (e.g. DME, VOR, NDB, pressure-altitude) thus allowing time, vertical and some lateral distance separation standards to be applied.

**Table 16 : Safety Requirements and Assumptions relating to External Mitigation Means**

Note that Environmental Conditions (EC) relates to specific characteristics of the environment in which ADS-B-NRA is expected to operate: available CNS means, traffic density, airspace configuration, etc. These elements have an impact on the hazards, either by mitigating or aggravating their effects.

Concerning the External Mitigation Means SAF046, it has been defined in order to mitigate hazards' effects (for detected cases of OH3 and OH4) once the ADS-B based ATS can no more be provided (because traffic position information available on CWP is incorrect). Thus, for this degraded mode, a similar level of service is maintained during the ADS-B-NRA failure using an

alternate procedural system (e.g. whereas system supported coordination fails, an ATCo may use direct voice communication system (SAF044) to perform the same operation as a back-up).

**GM039.** More generally, implementers have to establish degraded mode procedure applicable to ADS-B-NRA (see Guidance for the Provision of Air Traffic Services Using ADS-B in Non Radar Area [Ref.11])

Environmental Conditions (EC) and External Mitigation Means (EMM) taken into account during the assessment are provided for each hazard in Table 17 below.

The detailed list of mitigation means considered for each individual hazard is presented in a specific sub-section of the corresponding hazard assessment section in ED126/DO303 [Ref.1] (e.g. §C.7.4.5.1 provides the ECs and EMMs used through the assessment of the hazard OH3 detected case scenario 3).

**GM040.** The operational safety assessment performed for the generic case is based on a traffic level assumed (A015, A016 and A017) to be typical of areas where ADS-B-NRA could be implemented. Implementers will have to check whether these figures are appropriate for their local environment

**GM041.** The **order of magnitude** of these traffic conditions was used for the severities determination, Implementers will have to check whether these severity figures remain appropriate for their local environment

#### 8.4.4 Determination of Pe values

Pe value is the probability that the occurrence of a hazard will result in a given severity of operational effect. In order words, this probability tries to quantify the effectiveness of the Environmental Conditions (ECs) and the External Mitigation Means (EMM) identified during the hazards assessment.

As explained in section 8.4.1 the determination of Pe values has been done assuming (A019) that ATCo is assumed to be applying the minimum surveillance separation standard applicable for the airspace (e.g. 5Nm) (EC-4 of [Ref.1]). This assumption has been considered in the assessment of all the operational hazards, and constitutes a worst case situation<sup>37</sup>.

All Pe values presented here after are summarised in Table 17 below.

---

<sup>37</sup> This does not mean that larger minimum separations would automatically lead to different Pe values in all cases. But Pe values determination might have to be reviewed in light of the different situation if larger minimum separations are applied

### **Detected cases of hazards OH1 to OH4**

For these detected hazards, Pe values have been determined following an extremely conservative approach, which assumes that every failure event will in all cases lead to the corresponding severity effect (i.e.  $Pe = 1$ ). This is based on the idea that worst credible conditions apply for every failure event.

Only Pe values for hazards OH1-d, OH2-d and OH3-2d are not equal to 1 (Pe values are respectively 0.5, 0.1 and 0.1). The reason is that for these hazards it was considered that worst conditions only apply in some cases, resulting then in lesser frequencies for Pe values.

More explanations are provided on these values are provided in §C.4 of [Ref.1].

### **Undetected case of hazard OH1**

The Pe value used in this case is 0.1 as indicated in §C.5 of [Ref.1], assuming that the loss of one aircraft on ADS-B-NRA traffic conditions does not lead each time to an accident.

As indicated in section C.7.2.2. of [Ref.1]: *“In the current radar environment, when a case hazard involving the loss of position data for an aircraft has been detected, the ground system is required to present a distinct symbol (e.g. ‘radar coasting’) to the ATCo to indicate that the displayed position data is a predicted position rather than one that has been updated with surveillance data. This system detection is required to ensure that the ATCo can detect the loss. If the ground system does not provide the ATCo with a distinct symbol, and subsequently removes the track from the ATCo display, it is assumed that the loss will not be detected by the ATCo. This assumes that the ATCo is managing a large number of aircraft, making detection of a loss unlikely. It is assumed that the ATCo is separating the concerned aircraft in close proximity (at the minimum separation standard) to other aircraft. Once the track has been removed from the display, if a distinct symbol has not been displayed long enough for the ATCo to detect it (e.g. three refresh cycles), only providence can prevent a breakdown of separation. In an undetected case, a breakdown of separation equates to a risk of collision”*

Conservatively, very little credit for providence ( $Pe=0.1$ ) has been used for this hazard. It should also be noted that conservatively, no credit for ACAS and pilot visual avoidance have been used in the Pe determination.

### **Undetected cases of hazards OH3 and OH4**

For these undetected hazards the following corresponding Pe have been obtained in the various cases as described in section 8.3 (more information is provided in §AppendixC.1 of [Ref.1]):

**Case 1.** In case of the horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring, the  $P_e$  value used is  $1e-07^{38}$ . This value has been obtained based on Close Approach Probability (CAP) results (presented in §Annex E of [Ref.1]) and cross-validated through Monte-Carlo simulations (detailed in §AppendixC.1.2 of [Ref.1]). A summary of the Monte Carlo analysis is provided in 0. See also note below relating to  $P_e$  values in respect to the possible common mode of failure affecting both surveillance and navigation.

**Case 2.** In the case of the horizontal position error resulting from a corruption of the position information, the  $P_e$  value used is  $5e-03$ . This value has been determined based on “CAP footprints” analysis (detailed in §AppendixC.1.3 of [Ref.1]). The CAP footprints are established through the relative speed of the candidate close-approach aircraft in relation to the problem aircraft, the size of the “CAP” aircraft (including additional margin) and the length of time the error persists.

**Case 3.** In the case of an incorrect horizontal position error as a result of a corrupted quality indicator, the  $P_e$  value used is  $5e-03$ . The same approach as for Case 2 has been applied here (detailed in §AppendixC.1.3 of [Ref.1]), but in this case, for the hazard to occur, it requires prior to the corruption of the quality indicator, to have an incorrect position (modelled as a continuous drift). The resulting value for Case 3 is smaller than for Case 2 but for further conservatism,  $P_e$  has been set equal in both cases.

These 3 cases above are different nature of errors, therefore leading to different track error behaviours on the ATCo screen and having therefore different operational impacts and also  $P_e$  values. For example, when comparing case 2 (corruption of the horizontal position resulting in a “jump” of the position – undetected by the ATCo) and case 1 (GNSS position error not detected by the aircraft integrity monitoring resulting in a “drift” of the position – undetected by the ATCo), the analysis referred to above to ED-126 show that the corruption error can result in a higher probability of collision than the GNSS drift as illustrated in Table 17 below when considering related  $P_e$  values.

Note: the uncoupled case (only surveillance is affected by the error) is modelled to not result in the aircraft deviating from the intended course/track (only the corresponding track on the ATCo screen is deviating, not in the air). The coupled case (both NAV + SUR are affected by the same GNSS measurement fault) is modelled to lead to aircraft actually deviating off course

---

<sup>38</sup> Although in the multiple aircraft case,  $P_e$  should be reduced by a factor to account for the number of pairs which are potentially losing separation, a single  $P_e$  value has been selected for both, focusing on one pair scenario. The reason of this choice is that such a scenario involving only two aircraft results conservatively in a worst case situation for the related fault trees (see Table 23 : Safety Objectives versus Top event results) which would not be the case in more than 2 aircraft would be considered (as in that case accounting for all the coincidental simultaneous RAIM failures would result at the top of the OH3 fault tree in probability extremely low value compared to the 2 aircraft only scenario) .

due to navigation “compensating” for the apparent deviation in an attempt to bring the aircraft “back on course” (hence, on the ATCo screen, the aircraft is modelled to be displayed on course). This second case (coupled NAV + SUR error) is consequently modelled as the situation where a positioning error immediately moves the aircraft physically off-course which is the situation that has been assessed in the CAP (physical close approach risk) as being the most pessimistic situation.

It should be noted that conservatively, no credit for ACAS and pilot visual avoidance have been used in the Pe determination.

**GM042.** In case traffic conditions differ largely from the generic ones (A015, A016, A017 & A019), and/or in case that separation minima locally considered differs from 5 and 3 NM, implementers will have to check that Pe values are still valid in their local environment.

**GM043.** Pe values changes would generally lead to significant OSA modifications that will have to be taken into account by local implementers

#### 8.4.5 Hazard Assessment Summary

The following table provides a summary of identified hazards, their effects, severities assigned, Environmental Conditions (EC) and External Mitigation Means (EMM) taken into account, and the corresponding calculated Pe.

OH #	OH description	Effects	Sev	Pe	EMM / EC
<b>OH1</b>	<b>Sudden and unexpected loss of position information for a <u>single aircraft</u> previously identified in the sector.</b>				
OH1-d	Detected by the ATCo	Controller's Workload increase due to the application of an adequate procedural standard.	4	0.5	SAF045, A015, A016 A017, A018 A019
OH1-u	Undetected by the ATCo	Loss of separation leading to collision risk.	1	0.1	SAF045, A015, A016 A017, A018 A019
<b>OH2</b>	<b>Sudden and unexpected loss of position information for <u>multiple aircraft</u> previously identified in the sector.</b>				
OH2-d	Detected by the ATCo	Significant reduction in air traffic control capability. Additionally, until adequate alternate standards are established, significant reduction in safety margins exist.	3	0.1	SAF045, A015, A016 A017, A018 A019
<b>OH3</b>	<b>Incorrect position information for <u>multiple aircraft</u> in a wide area is presented on the CWP</b>				
OH3-1d	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Detected by the ATCo	Controller's Workload increase (higher than for OH4 as multiple aircraft are involved) due to the application of an adequate procedural standard.	3	1	SAF044, SAF046 A015, A016 A017, A018 A019

OH #	OH description	Effects	Sev	Pe	EMM / EC
OH3-1u	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Undetected by the ATCo	Multiple loss of separation. 2 examples of this effect: * conflict situation not detected: as a consequence, corrective action was not applied when it should have been * controller makes decisions which brings AC into proximity below the approved standard, without being identified by the controller.	1	1e-7	A015, A016 A017, A018 A019
OH3-2d	Horizontal position error resulting from a corruption of the position information. Detected by the ATCo	Controller's Workload increase (higher than for OH4 as multiple aircraft are involved) due to the application of an adequate procedural standard.	3	0.1	SAF044, SAF046 A015, A016 A017, A018 A019
OH3-2u	Horizontal position error resulting from a corruption of the position information. Undetected by the ATCo	Multiple loss of separation. 2 examples of this effects: * conflict situation not detected: as a consequence, corrective action was not applied when it should have been * controller makes decisions which brings AC into proximity below the approved standard, without being identified by the controller.	1	5e-3	A015, A016 A017, A018 A019
OH3-3d	Incorrect horizontal position error as a result of a corrupted quality indicator. Detected by the ATCo	Controller's Workload increase (higher than for OH4 as multiple aircraft are involved) due to the application of an adequate procedural standard.	3	1	SAF044, SAF046 A015, A016 A017, A018 A019

OH #	OH description	Effects	Sev	Pe	EMM / EC
OH3-3u	Incorrect horizontal position error as a result of a corrupted quality indicator. Undetected by the ATCo	Multiple loss of separation. 2 examples of this effect: * conflict situation not detected: as a consequence, corrective action was not applied when it should have been * controller makes decisions which brings AC into proximity below the approved standard, without being identified by the controller.	1	5e-3	A015, A016 A017, A018 A019
<b>OH4</b>	<b>Incorrect position information for <u>single aircraft</u> is presented on the CWP</b>				
OH4-1d	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Detected by the ATCo	Controller's Workload increase due to the application of an adequate procedural standard.	4	1	SAF044, SAF046 A015, A016 A017, A018 A019
OH4-1u	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Undetected by the ATCo	Multiple loss of separation. 2 examples of this effect: * conflict situation not detected: as a consequence, corrective action was not applied when it should have been * controller makes decisions which brings AC into proximity below the approved standard, without being identified by the controller.	1	1e-7	A015, A016 A017, A018 A019
OH4-2d	Horizontal position error resulting from a corruption of the position information. Detected by the ATCo	Controller's Workload increase due to the application of an adequate procedural standard.	4	1	SAF044, SAF046 A015, A016 A017, A018 A019



OH #	OH description	Effects	Sev	Pe	EMM / EC
OH4-2u	Horizontal position error resulting from a corruption of the position information. Undetected by the ATCo	Multiple loss of separation. 2 examples of this effect: * conflict situation not detected: as a consequence, corrective action was not applied when it should have been * controller makes decisions which brings AC into proximity below the approved standard, without being identified by the controller.	1	5e-3	A015, A016 A017, A018 A019
OH4-3d	Incorrect horizontal position error as a result of a corrupted quality indicator. Detected by the ATCo	Controller's Workload increase due to the application of an adequate procedural standard.	4	1	SAF044, SAF046 A015, A016 A017, A018 A019
OH4-3u	Incorrect horizontal position error as a result of a corrupted quality indicator. Undetected by the ATCo	Multiple loss of separation. 2 examples of this effect: * conflict situation not detected: as a consequence, corrective action was not applied when it should have been * controller makes decisions which brings AC into proximity below the approved standard, without being identified by the controller.	1	5e-3	A015, A016 A017, A018 A019

**Table 17 : ADS-B-NRA Hazards Effects, Severity, Pe and EMM & EC**

## 8.5 DETERMINATION OF SAFETY OBJECTIVES (ARG1.1.5.3)

The determination of Safety Objectives for identified ADS-B-NRA hazards has been performed based on ED78A/DO264 [Ref.7] process and using SAM methodology [Ref.4]. This process has been described in sections §C.2.1.3.3 and §C.2.1.3.4 of [Ref.1] and summarised in the following steps:

- Apportionment of the ATM Safety Targets (section 8.5.1)
- Safety Objective calculation (section 8.5.2)

### 8.5.1 Apportionment of the ATM Safety Targets

Apportionment of the ATM Safety Targets<sup>39</sup> for ADS-B-NRA application specifies the overall maximum frequency of occurrence of effects for the concerned application.

The Risk Classification Scheme used (including ATM Safety Targets Values) has been obtained based on ESARR4 values, and processes proposed in ED-125 [Ref.13] and SAM [Ref.4].

The first set of ATM Safety Targets has been directly obtained from ED125. In this standard, an ambition factor of 1.55 is proposed to be applied on ESARR4 value for ST1. For Safety Targets from severity class 2 to 4, values *“are set by ED-125 through consideration of data and expert judgment”* (as per §2.3 in ED-125 [Ref.13]). These values are presented in Table 18.

As indicated in §C3.3 of ED-126 [Ref.1], an Ambition Factor of 1 has been applied for ADS-B-NRA to these ATM Safety Targets, *“as the level of safety for NRA is expected to be at least the same as for current radar environment”*. However a quite conservative safety assessment has been made, typically by not using human elements (ATCo or pilot) as detection and/or mitigation mechanism.

This first set of values has been expressed in [flight.h] units. Then, different Safety Targets have been determined depending on the characteristics of the considered NRA environment (i.e. for En-route and for TMA), expressing them in [ATSU.h] units. This conversion has been based on traffic conditions as indicated in A016:

The average number of aircraft assumed to be managed per ATSU.hour is 30 for en-route and 10 for TMA (resulting in the following equivalences: 1 ATSU.h = 10 flight.h for en-route and 1 ATSU.h = 1 flight.h for TMA).

Finally, a certain percentage for each of these Safety Targets has been determined, in order to define the part of the total ATM Safety Targets to be

---

<sup>39</sup> Applicable to the overall ATM system

guaranteed by ADS-B-NRA application for ATS separation services. The percentages stated are captured in the following assumption:

**A020.** It is assumed that ADS-B-NRA for ATS separation services participates to the ATM Safety Targets at the following levels: 35% for severity class 1, 11% for severity class 3, and 9% for severity class 4. Percentages corresponding to severity class 2 have not been defined as no NRA hazard has been identified for this severity class.

These percentages are justified by the fact a typical ADS-B-NRA implementation is assumed to take place in an area which is today a procedural environment with limited infrastructure (voice reporting, no radar, no tracking, no display, very basic or no FDPS, etc.), in low density airspace, with low route structure complexity, etc.

Note that these safety budgets are then allocated to the corresponding NRA hazards having the same Worst Credible Case, assuming an even distribution of the risk (as proposed in ED-125 [Ref.13]).

The following table shows all these Safety Targets, as well as the percentage of each safety budget assigned to ADS-B-NRA application:

ATM Safety Targets				NRA	
Severity	per [flight.h]	per [ATSU.h]		% of ATM Safety Targets	N° Hazards
		ER	TMA		
Severity 1	1e-08	1e-07	1e-08	35%	7
Severity 2	1e-05	1e-04	1e-05	n/a <sup>40</sup>	0
Severity 3	1e-04	1e-03	1e-04	11%	4
Severity 4	1e-02	1e-01	1e-02	9%	4

**Table 18 : Risk Classification Scheme and apportionment for ADS-B-NRA**

**GM044.** The impact of a change in the ratio between the numbers of NRA and overall ATM hazards (for each severity) would also have to be reviewed by implementers as apportionment of the safety objectives in a local environment will depend on the complexity of the local implementation and such values will have to be adapted. Note that ED125 [Ref.13] was not established<sup>41</sup> at the time of the edition of the ED126/DO303 [Ref.1] standard, It is recommended to implementers to use the ED125 document as input for determining the level of granularity at which hazards have to be defined, and for determining the number of ATM hazards to be considered based on the airspace complexity definitions included in ED-125.

<sup>40</sup> Any hazard class 2 has been identified for ADS-B-NRA application.

<sup>41</sup> At the time of the edition of this document, ED-125 is still pending approval.

## 8.5.2 Determination of Safety Objectives

Based on information presented in previous sections, the Safety Objectives have been assigned to each hazard as explained in §C3.3 of [Ref.1]. I.e. by knowing the probability of a hazard to lead to an effect (Pe), and the maximum frequency of occurrence tolerable for this effect (Safety Target), the Safety Objective can be determined.

As explained in section 8.5.1, Safety Targets for NRA have been obtained by applying the percentage determined for each corresponding severity class, and then distributing these safety budgets into the different related hazards. For example, for severity class 1 NRA hazards, the Safety Target to be considered for En-Route is calculated as follows:

$$ST_{1,NRA} = \frac{ST_{1,ATM} * \%_{1,NRA}}{N^{\circ} Hazards_{NRA}} \quad ST_{1,NRA} = \frac{1e^{-08} * 35\%}{7} = 5.0e^{-09} [ATSU.h]$$

And then, the calculation of the Safety Objective for en-route airspace for example for hazard OH1u, for which Pe is 0.1, is done as follows:

$$SO_{OH1u} = \frac{ST_{1,NRA}}{Pe_{OH1u}} \quad SO_{OH1u} = \frac{5.0e^{-09} [ATSU.h]}{0.1} = 5.0e^{-08} [ATSU.h]$$

The Safety Objectives for ADS-B-NRA hazards calculated based on above explanations for OH1 to OH4 are the following ones:

OH #	OH description	Sev.	Airsp.	Safety Target [ATSU.h]	Pe	Safety Objective [ATSU.h]
<b>OH1</b>	<b>Sudden and unexpected loss of position information for a <u>single</u> aircraft previously identified in the sector.</b>					
OH1-d	Detected by the ATCo	4	ER	2.2e-03	0.5	4.5e-03
			TMA	2.2e-04		4.5e-04
OH1-u	Undetected by the ATCo	1	ER	5.0e-09	0.1	5.0e-08
			TMA	5.0e-10		5.0e-09
<b>OH2</b>	<b>Sudden and unexpected loss of position information for <u>multiple</u> aircraft previously identified in the sector.</b>					
OH2-d	Detected by the ATCo	3	ER	2.9e-05	0.1	2.9e-04
			TMA	2.9e-06		2.9e-05
<b>OH3</b>	<b>Incorrect position information for multiple aircraft in a wide area is presented on the CWP</b>					

OH #	OH description	Sev.	Airsp.	Safety Target [ATSU.h]	Pe	Safety Objective [ATSU.h]
OH3-1d	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Detected by the ATCo	3	ER	2.9e-05	1	2.9e-05
			TMA	2.9e-06		2.9e-06
OH3-1u	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Undetected by the ATCo	1	ER	5.0e-09	1e-7	5.0e-02
			TMA	5.0e-10		5.0e-03
OH3-2d	Horizontal position error resulting from a corruption of the position information. Detected by the ATCo	3	ER	2.9e-05	0.1	2.9e-04
			TMA	2.9e-06		2.9e-05
OH3-2u	Horizontal position error resulting from a corruption of the position information. Undetected by the ATCo	1	ER	5.0e-09	5e-3	1.0e-06
			TMA	5.0e-10		1.0e-07
OH3-3d	Incorrect horizontal position error as a result of a corrupted quality indicator. Detected by the ATCo	3	ER	2.9e-05	1	2.9e-05
			TMA	2.9e-06		2.9e-06
OH3-3u	Incorrect horizontal position error as a result of a corrupted quality indicator. Undetected by the ATCo	1	ER	5.0e-09	5e-3	1.0e-06
			TMA	5.0e-10		1.0e-07
<b>OH4</b>	<b>Incorrect position information for single aircraft is presented on the CWP</b>					
OH4-1d	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Detected by the ATCo	4	ER	2.2e-03	1	2.2e-03
			TMA	2.2e-04		2.2e-04
OH4-1u	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Undetected by the ATCo	1	ER	5.0e-09	1e-7	5.0e-02
			TMA	5.0e-10		5.0e-03
OH4-2d	Horizontal position error resulting from a corruption of the position information. Detected by the ATCo	4	ER	2.2e-03	1	2.2e-03
			TMA	2.2e-04		2.2e-04

OH #	OH description	Sev.	Airsp.	Safety Target [ATSU.h]	Pe	Safety Objective [ATSU.h]
OH4-2u	Horizontal position error resulting from a corruption of the position information. Undetected by the ATCo	1	ER	5.0e-09	5e-3	1.0e-06
			TMA	5.0e-10		1.0e-07
OH4-3d	Incorrect horizontal position error as a result of a corrupted quality indicator. Detected by the ATCo	4	ER	2.2e-03	1	2.2e-03
			TMA	2.2e-04		2.2e-04
OH4-3u	Incorrect horizontal position error as a result of a corrupted quality indicator. Undetected by the ATCo	1	ER	5.0e-09	5e-3	1.0e-06
			TMA	5.0e-10		1.0e-07

**Table 19 : SO for hazards OH1 to OH4**

**GM045.** Conversion between "ATSU.hour" and "flight.hour (A016)" is widely used in the OSA, particularly when deriving Safety Objectives, expressed per ATSU.h, from Safety Targets, expressed in flight.h. If local traffic conditions result in a different conversion rule, it would then be necessary to review whether Safety Objectives values need to be modified.

## 8.6 HAZARDS CAUSES IDENTIFICATION AND INTERNAL MITIGATION MEANS (ARG1.1.5.4)

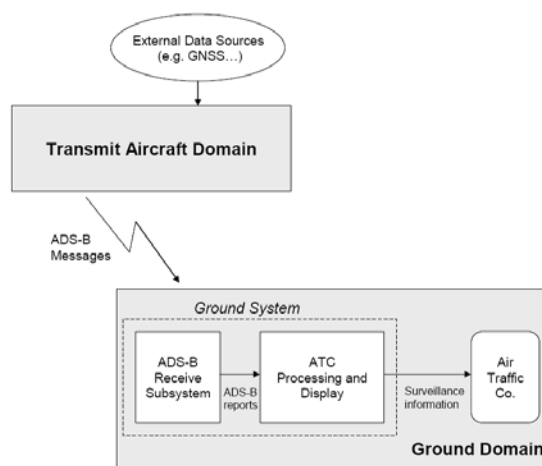
Once the Safety Objective has been determined for each hazard, further analysis has been performed to identify all the potential causes leading to these hazards, in order to be able to allocate the SO over the different elements having an impact upon the hazard occurrence.

### 8.6.1 Hazard Causes

The ED-126/DO-303 [Ref.1] (ASOR in § Annex C) used Fault Tree Analysis to identify the possible causes (called Basic Causes - BC) and their interactions for each of the hazards mentioned in previous sections. Common mode failures have also been considered during this process.

A fault tree for each individual hazard is presented in a specific sub-section of the corresponding hazard assessment section in [Ref.1] (e.g. §C.7.2.2.4 for OH1 undetected case fault tree). Another specific sub-section lists the basic causes included in the corresponding fault tree (e.g. §C.7.2.2.5 for the same hazard example).

These basic causes have been determined at functional CNS/ATM system components level, i.e. ground domain, airborne domain, and some subsystems as presented in following figure (obtained from §Figure 25 of [Ref.1] and derived from Figure 1):



**Figure 10: Functional System description for ADS-B-NRA**

More explanation concerning these functions has already been provided in sections 2.2 and 4.3.3.

Some typical examples of basic causes are listed below (the complete list is available in the various subsections of §C.7 in [Ref.1]):

**AC-L01:** Aircraft ceases to provide ADS-B position.

**GND-L03:** ADS-B Receive Subsystem loses an aircraft information entirely.

**GND-E09:** ATC Processing and Display subsystem corrupts position information (multiple aircraft).

### 8.6.2 Internal Mitigation Means

Apart from these basic causes, mitigation means allowing hazards detection (called Internal Mitigation Means - IMM) have also been identified. Failures related to these IMM have been included in the fault trees too (for undetected cases of hazards mainly).

The internal mitigation means identified for ADS-B-NRA and the corresponding hazards for which they apply are presented in the following table:

Internal Mitigation Means	Related Hazards
<p><b>SAF047.</b> Ground system function shall detect that no position information is available for one track which leads to the presentation of a distinct symbol on the ATCo display highlighting that the position data is predicted (e.g. track coasting function). The relevant ground function must detect the loss of data at least within a time similar to one display refresh cycle as for current radar, i.e. 10 sec. for en-route airspace and 5 sec. for TMA airspace (IMM-1 in [Ref.1]).</p> <p><b>Note:</b> The efficiency of this barrier is described by SAF052</p>	OH1d
<p><b>A021.</b> It is assumed that controller will always detect the loss of all tracks on the CWP (as in current radar system) (IMM-2. in [Ref.1])</p>	OH2d
<p><b>A022.</b> It is assumed that the probability of a corrupted position<sup>42</sup> being undetected by the ground processing system is 2.5E-4 (per event) (IMM-3 and IMM-5 in [Ref.1]).</p>	OH3u2 OH4u2
<p><b>A023.</b> It is assumed that all position errors (characterised by</p>	OH3u3

---

<sup>42</sup> This relates to the case 2 described in section 8.4.4, for a random “jump” of the position as a result of a corruption.



Internal Mitigation Means	Related Hazards
quality indicator information corruption) being inside a circle with a radius of 50 NM are not detected by ATCo or ground processing system whereas errors outside this radius are detected by either the ground processing or the controller (IMM-4 and IMM-6 in [Ref.1]).	OH4u3

**Table 20 : Internal Mitigation Means list**

The detailed list of internal mitigation means considered for each individual hazard is presented in the specific sub-section in [Ref.1] as the Environmental Conditions and the External Mitigation Means. Another specific sub-section lists the IMM failures included in each corresponding fault tree (e.g. §C.7.2.2.5 for the same hazard example).

## 8.7 SAFETY REQUIREMENTS AND ASSUMPTIONS (ARG1.1.5.5)

After the identification of hazards causes, the next step consisted of allocating the Safety Objectives and in deriving the corresponding Safety Requirements.

Each Safety Objective has then been apportioned to causes leading to the corresponding hazard through the dedicated fault trees. This allocation has been performed based on discussions involving operational, technical and safety experts (as described in §C.2.2.3.2 of [Ref.1]).

Specific Safety Requirements have been determined for each cause (Basic Cause or Internal Mitigation Means failure) based on this apportionment (as described in §C.2.2.3.3 of [Ref.1]). At the end and based on this apportionment, the top level result for each fault tree has been recalculated to be sure that the corresponding Safety Objective is met, in order to validate this allocation.

It is important to note that in any case, corresponding Safety Requirements have been derived based on the following statement:

**A024.** It is assumed that failure rates are independent of traffic numbers (ASSUMP-24 of [Ref.1]).

The results of this allocation are provided in the following Table 21:

Safety Requirement	Related OH
<b>SAF048.</b> The likelihood that the aircraft domain corrupts ADS-B position information or associated quality indicators shall be no more than 1e-05 per flight.hour <sup>43</sup> (SR-1 & SPR-10 in [Ref.1]).	OH1d OH1u
<b>SAF049.</b> The likelihood that the aircraft transmit domain is unavailable during an operation, given that it was available at the start of the operation, shall be no more than 2e-04 per flight.hour (SR-2 and SPR-9 in [Ref.1]).	OH1d OH1u
<b>SAF050.</b> The likelihood that the ADS-B receive sub-system corrupts ADS-B position information or associated quality indicator for a single aircraft track shall be no more than 5e-06 per ATSU.hour (SR-3 & SPR-13 in [Ref.1]).	OH1d OH1u
<b>SAF051.</b> The likelihood that ADS-B receive subsystem does not provide updated ADS-B surveillance reports for one aircraft from which ADS-B messages are being received shall be no more than 1e-04 per ATSU.hour (SR-4 & SPR-15 in [Ref.1]).	OH1d OH1u
<b>SAF052.</b> The likelihood that ATC processing system does not notify the controller of the loss of a track (e.g. through coasting) shall be no more than 1e-05 per ATSU.hour (SR-5 in [Ref.1])	OH1u
<b>SAF053.</b> The likelihood that ADS-B receive subsystem does not provide update ADS-B surveillance reports for more than one aircraft from which ADS-B messages are being received shall be no more than 5e-06 per ATSU.hour (SR-6 & SPR-14 in [Ref.1])	OH2d
<b>SAF054.</b> The likelihood that ATC processing and display system lose all information for more than one aircraft shall be no more than 5e-06 per ATSU.hour (SR-7 in [Ref.1])	OH2d
<b>SAF055.</b> The likelihood that the ADS-B receive subsystem corrupts ADS-B position information or associated quality indicator for more than one track shall be no more than 5e-06 per ATSU.hour (SR-8 & SPR-13 in [Ref.1])	OH2d
<b>SAF056.</b> The likelihood that ATC processing and display system corrupts ADS-B quality indicator or position for more than one aircraft shall be no more than 5e-06 per ATSU.hour (SR-9 in [Ref.1])	OH2d
<b>SAF057.</b> The likelihood that aircraft horizontal position integrity monitoring fails to detect errors in the horizontal position shall be no more than 1e-03 per flight.hour (SR-10 in [Ref.1])	OH3d1

<sup>43</sup> The SIL value is established to SIL<sub>≥2</sub> in line with this system integrity value

Safety Requirement	Related OH
<b>SAF058.</b> The likelihood that the aircraft domain corrupts position information shall be no more than 1e-05 per flight.hour (SR-11 & SPR-10 in [Ref.1])	OH3d2 OH4d2
<b>SAF059.</b> The likelihood that ATC processing and display system corrupts position information for more than one aircraft shall be no more than 5e-06 per ATSU.hour (SR-12 in [Ref.1])	OH3d2 OH3u2
<b>SAF060.</b> The likelihood that the ADS-B receive subsystem provides incorrect information or no information at all for multiple aircraft tracks due to the corruption of position information shall be no more than 5e-06 per ATSU.hour (SR-13 & SPR-13 in [Ref.1])	OH3d2
<b>SAF061.</b> The likelihood that the aircraft domain corrupts ADS-B quality indicators shall be no more than 1e-05 per flight.hour (SR-14 & SPR-10 in [Ref.1])	OH3d3
<b>SAF062.</b> The likelihood that the ADS-B receive subsystem provides incorrect information at all for one or more tracks due to the corruption of quality indicators shall be no more than 5e-06 per ATSU.hour (SR-15 & SPR-13 in [Ref.1])	OH3d3 OH3u3 OH4d3 OH4u3
<b>SAF063.</b> The likelihood that the ATC processing and display system corrupts quality indicators for aircraft shall be no more than 5e-06 per ATSU.hour (SR-16 in [Ref.1])	OH4d3 OH4u3 OH3d3 OH3u3
<b>SAF064.</b> The likelihood that ATC processing and display subsystem corrupts position information for a single aircraft should be no more than 5e-06 per ATSU.hour (SR-17 in [Ref.1])	OH4d2 OH4u2
<b>SAF065.</b> The likelihood that ADS-B receive subsystem provides incorrect information or no information at all for a single aircraft track due to the corruption of either position information or associated quality indicators shall be no more than 5e-06 per ATSU.hour (SR-18 & SPR-13 in [Ref.1])	OH4d2 OH4u2

**Table 21 : Safety Requirements related to hazards causes**

**GM046.** (see also GM018) Implementers shall ultimately consider the most demanding requirements regarding update rate / loss of track information between SAF018 and SAF021 presented in Table 12 (for the success case) on the one hand and SAF051 presented in previous Table 21 (for the failure case) on the other hand.

**GM047.** Implementers shall complete the list of quantitative safety requirements with qualitative safety requirements (e.g. controllers training, extra procedural mitigations, etc.) based on own local characteristics.

For some specific causes in the fault trees, some assumptions were determined instead of safety requirements due to the nature of these causes (e.g. failure of external elements or technical system design). These assumptions are listed here after:

Assumption	Related OH
<b>A025.</b> It is assumed that while being under ADS-B-NRA ATS, the probability that an aircraft temporarily loses positioning or surveillance coverage (e.g. due to a steep bank angle), is not greater than 1e-04 per flight.hour (ASSUMP-25 in [Ref.1])	OH1d OH1u
<b>A026.</b> It is assumed that there is no detection means on-board concerning either the failure to transmit ADS-B data (FC is not alerted if the ADS-B data is not broadcast) or the transmission or incorrect quality indicators or corrupted ADS-B data (ASSUMP-27 in [Ref.1])	OH1d OH1u
<b>A010</b> It is assumed that the integrity failure rate where multiple a/c are affected, for any GNSS system used as position source is no more than 10-5 per hour (ASSUMP-28 in [Ref.1]) .	OH2d OH3d3 OH3u3
<b>A011</b> It is assumed that the integrity failure rate of the horizontal position source impacting one aircraft is no more than 10-4 per user (ASSUMP-29 in [Ref.1]).	OH3d1 OH3u1 Oh4d1 OH4u1

**Table 22 : Assumptions related to hazards causes**

The detailed list of safety requirements and assumptions considered for each individual hazard is presented in [Ref.1] in the same sub-section in which the basic causes and IMM failures are listed (e.g. §C.7.2.2.5 for the same previous hazard example).

**GM048.** In case Safety Objectives values need to be modified in the local environment, implementers will have to check the fault trees so as to ensure that the Safety Objectives are still met with the ED126 Safety Requirements or otherwise that the appropriate related requirements are derived

**GM049.** Conversion of flight-hours to ATSU-hours using traffic conditions less dense than the generic ED126 one results in deriving stricter requirements (in ATSU.h) on the ground system functions. Therefore, implementers will have to perform a detailed review if this situation occurs.

Note that due to the nature of the ADS-B-NRA application itself and its dependability upon external elements, the assessment performed and

requirements obtained for ADS-B-NRA are based on agreed performance and characteristics of GNSS system (L001).

The SR presented here before satisfies the Safety Criteria as the result from Fault trees taking into account these safety requirements and the assumptions previously presented show that the Safety Objectives are met in all the cases:

OH #	OH description	Airsp.	Safety Objective [ATSU.h]	Top event Result [ATSU.h]	SO achieved
OH1	Sudden and unexpected loss of position information for a <u>single aircraft</u> previously identified in the sector.				
OH1-d	Detected by the ATCo	ER	4.5e-03	2.3e-03	OK
		TMA	4.5e-04	3.3e-04	OK
OH1-u	Undetected by the ATCo	ER	5.0e-08	2.3e-08	OK
		TMA	5.0e-09	3.3e-09	OK
OH2	Sudden and unexpected loss of position information for <u>multiple</u> aircraft previously identified in the sector.				
OH2-d	Detected by the ATCo	ER	2.9e-04	3.0e-05	OK
		TMA	2.9e-05	3.0e-05	OK <sup>44</sup>
OH3	Incorrect position information for multiple aircraft in a wide area is presented on the CWP				
OH3-1d	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Detected by the ATCo	ER	2.9e-05	9.9e-09	OK
		TMA	2.9e-06	1.0e-10	OK
OH3-1u	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Undetected by the ATCo	ER	5.0e-02	9.9e-09	OK
		TMA	5.0e-03	1.0e-10	OK
OH3-2d	Horizontal position error resulting from a corruption of the position information. Detected by the ATCo	ER	2.9e-04	1.0e-05	OK
		TMA	2.9e-05	1.0e-05	OK

<sup>44</sup> Safety Objective is considered as achieved even in TMA case as the difference with the result at the top event of the fault tree is marginal

OH #	OH description	Airsp.	Safety Objective [ATSU.h]	Top event Result [ATSU.h]	SO achieved
OH3-2u	Horizontal position error resulting from a corruption of the position information. Undetected by the ATCo	ER	1.0e-06	2.5e-09	OK
		TMA	1.0e-07	2.5e-09	OK
OH3-3d	Incorrect horizontal position error as a result of a corrupted quality indicator. Detected by the ATCo	ER	2.9e-05	1.0e-10	OK
		TMA	2.9e-06	1.0e-10	OK
OH3-3u	Incorrect horizontal position error as a result of a corrupted quality indicator. Undetected by the ATCo	ER	1.0e-06	1.0e-10	OK
		TMA	1.0e-07	1.0e-10	OK
OH4	Incorrect position information for single aircraft is presented on the CWP				
OH4-1d	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Detected by the ATCo	ER	2.2e-03	9.9e-07	OK
		TMA	2.2e-04	9.9e-08	OK
OH4-1u	Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring. Undetected by the ATCo	ER	5.0e-02	9.9e-07	OK
		TMA	5.0e-03	9.9e-08	OK
OH4-2d	Horizontal position error resulting from a corruption of the position information. Detected by the ATCo	ER	2.2e-03	1.1e-04	OK
		TMA	2.2e-04	2.0e-05	OK
OH4-2u	Horizontal position error resulting from a corruption of the position information. Undetected by the ATCo	ER	1.0e-06	2.7e-08	OK
		TMA	1.0e-07	5.0e-09	OK
OH4-3d	Incorrect horizontal position error as a result of a corrupted quality indicator. Detected by the ATCo	ER	2.2e-03	1.1e-08	OK
		TMA	2.2e-04	2.0e-09	OK
OH4-3u	Incorrect horizontal position error as a result of a corrupted quality indicator. Undetected by the ATCo	ER	1.0e-06	1.1e-08	OK
		TMA	1.0e-07	2.0e-09	OK

**Table 23 : Safety Objectives versus Top event results**

It has to be noted that for a large number of Operational Hazards, the top event result meet the Safety Objective with a large margin (e.g. a factor 1000).

## 8.8 CONCLUSIONS ON ARG1.1.5 - INTERNAL FAILURES

This section has provided adequate Argument and supporting Evidence that the ADS-B-NRA application for ATS separation service is robust against internal failures, by:

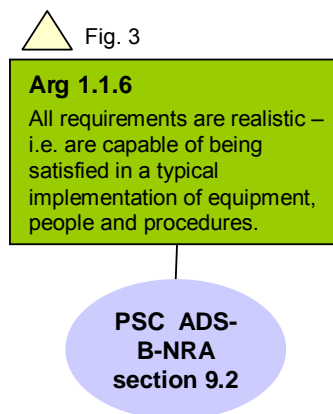
- Identifying all hazards at the boundary of the system (at Controller Working Position level) related to ADS-B-NRA ATS separation service.
- Assessing the severity of the effects from each hazard, taking account of any external mitigation means and environmental condition.
- Determining, for each external mitigation means and environmental condition, specific Safety Requirements or Assumptions concerning their functionality. The associated performance and probability that the mitigation will be successful have been quantified via the  $P_e$ . The  $P_e$  value indicates the probability that the occurrence of a hazard will result in a given operational effect taking into account all the applicable external mitigation means and environmental conditions for this hazard.
- Deriving Safety Objectives such that the aggregate risk, from all hazards, is within the Safety Criteria for the “failure case”.
- Identifying all potential causes of each hazard (deductive analysis) as well as any internal mitigation means that would reduce the probability that those causes would actually lead to the corresponding hazard(s).
- Specifying, for each internal mitigation means, the corresponding Safety Requirement or Assumption concerning its functionality, performance and probability that the mitigation will be successful.
- Deriving Safety Requirements (or Assumptions when appropriate) for each of the causes of each hazard such that the Safety Objective for that hazard is satisfied, taking account of any internal mitigation means.
- Summarizing how the set of Safety Requirements satisfies the Safety Criteria.



## 9 REALISM OF ALL REQUIREMENTS AND ASSUMPTIONS (ARG1.1.6)

The objectives of this section is to show that all requirements allocated to each domain or sub-system and assumptions stated are realistic, i.e. capable of being satisfied in a typical implementation of equipment, people and procedures.

Note that for generic aspects of ADS-B-NRA, equipment has been specified at functional level only. Local full Safety Case will address the physical part of the equipment as per GM019.



**Figure 11: Realism of requirements and assumptions (Arg1.1.6)**

### 9.1 STRATEGY

The strategy for satisfying Arg1.1.6 is to provide evidence demonstrating that:

- › Working process used to obtain and validate results addresses all the elements of the application system
- › Information on existing equivalent systems is used when relevant

### 9.2 VALIDATION OF SPECIFICATION REQUIREMENTS

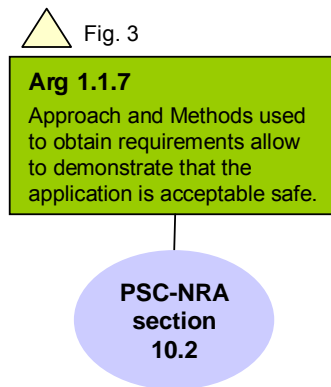
The results presented in previous sections (requirements and assumptions) are obtained and validated, at least for this generic level, following the RFG working approach: working groups including technical and operational experts formalising their activities as per ED78A [Ref.7] process and EUROCONTROL SAM methodology [Ref.4]. Participants to these working groups represent a large number of perspectives, in particular from industry (e.g. EUROCAE, RTCA).

Furthermore, and concerning procedures and operational results, as most of those results have been obtained by comparison with reference radar operations, they are in general capable of being satisfied as radar is.

**Page intentionally left blank**

## 10 APPROACH USED FOR THE SPECIFICATION (ARG1.1.7)

The objective of this section is to show that the approach and methodology used to obtain all requirements specifying ADS-B-NRA demonstrate that the application is acceptable safe.



**Figure 12: Approach and Methodology used (Arg1.1.7)**

### 10.1 STRATEGY

The strategy for satisfying Arg1.1.7 is to provide evidence demonstrating that:

- Approach and methods applied during the specification of the application are well recognised, and specific adaptations of the methods for surveillance have been done and documented when necessary.
- These approaches and methods were applied by competent personnel.
- Concerning safety aspects, these methods and approaches are compliant with regulatory requirements (i.e. ESARR).

### 10.2 APPROACH AND METHODS FOR SPECIFICATION

All the requirements and assumptions related to ADS-B specification have been obtained based on ED-78A [Ref.7] process and SAM [Ref.4] methodology. Main Assumptions related to methodology applied are included in §3.3 from [Ref.1].

The list of organisations involved in the specification process of ADS-B-NRA is provided in Annex B . The large number of RFG participants, the variety of perspectives (US, Europe, etc), the involvement of operational people (ATCo & Pilots), the number of ANSP including future European implementers, all these elements contribute to demonstrate that the RFG brought key competence to apply the mentioned methodologies and approaches.

Concerning regulatory requirements, the following table summarises compliance with ESARR-4 [Ref.5] requirements concerning hazard assessment process (section 5 of [Ref.5]):

ESARR4 section	Compliance
<b>5.1:HAZARD ASSESSMENT ADDRESSES:</b>	
5.1a) complete life-cycle	NO, only specification part is addressed in PSC; other Arguments will address the other aspects.
5.1b) air and ground aspects	OK
5.1c) ATM elements (procedures, human, equipment)	OK <sup>45</sup>
<b>5.2: HAZARD ASSESSMENT INCLUDES:</b>	
5.2a) system description	OK
5.2b) safety objectives determination	OK
5.2c) risk mitigation strategy (requirements, EC, etc.)	OK
5.2d) verify that SO and SR are met (prior implementation, during transition, during operation, until decommission.)	NO (as this is the responsibility of the ANSP)
<b>5.3: RESULTS</b>	
5.3a) demonstrate that is and will remain tolerably safe (monitoring tools):	NO (as this is the responsibility of the ANSP)
5.3b) traceability	OK

**Table 24 : Compliance with ESARR4 section 5**

**GM050.** As shown in previous table, almost all relevant parts of ESARR4 have been followed in this generic Preliminary Safety Case. A local safety assessment and safety case is then required to be done by the implementers in order to fill in the 3 remaining parts [i.e. 5.1a), 5.1c), 5.2d) and 5.3a)].

---

<sup>45</sup> For generic aspects of ADS-B-NRA, “equipment” has been specified at functional level only. Local full Safety Case will have to address the physical architecture supporting the local implementation.

## 11 ASSUMPTIONS, ISSUES AND LIMITATIONS

The following caveats apply to this Preliminary Safety Case and need to be considered in the context of the overall conclusions presented in section 12:

### 11.1 ASSUMPTIONS

Ref	Assumption	Source	Validation
A001	Reference service (i.e. radar-based surveillance as defined in ICAO PANS-ATM Doc4444 [Ref.2] - (C001)) is tolerably safe.	PSC ADS-B-NRA section 3.2	This is based on years of experience using radar based ATS. However as no ESARR4 compliant Safety Assessment has been conducted for radar-based ATS, it cannot be claimed for the reference radar service to be "acceptably safe"
A002	100% of aircraft are equipped and certified for ADS-B-NRA	PSC ADS-B-NRA section 3.4.1	ED126/DO303 section 1.1.1
A003	The horizontal plane error distribution for a GNSS positioning source is represented by a radial Rayleigh probability density function (ASSUMPT-70 in [Ref.1]).	PSC ADS-B-NRA section 4.5.1	ED126/DO303 ASSUMPT-70
A004	It is assumed that the GNSS constellation is sufficient to assure the availability of ADS-B integrity monitoring or equivalent capabilities confirming the integrity of the surveillance position data (ASSUMP-13 [Ref.1]).	PSC ADS-B-NRA section 5.6.3	ED126/DO303 ASSUMP-13

Ref	Assumption	Source	Validation
A005	With the exception of quality indicator (QI) management, it is assumed that there is no major change regarding ATCo actions for ADS-B-NRA compared to those performed in the reference radar-based ATS.	PSC ADS-B-NRA section 6.4	The validity of this assumption has been confirmed through the RFG process that involved lots of industry, operational people (ATCo, pilots), service providers (NATS, DNSA, LFV, etc.), and other organisations as FAA, AirService Australia and EUROCONTROL.
A006	With the exception of the aircraft identification (see FC manual [Ref.10] section §6), it is assumed that there is no change regarding pilot action for ADS-B-NRA and the same functionality is applied regarding emergency situation, Mode A code change <sup>14</sup> , SPI or deselecting of the Pressure-Altitude.	PSC ADS-B-NRA section 6.4	The validity of this assumption has been confirmed through the RFG process that involved lots of industry, operational people (ATCo, pilots), service providers (NATS, DNSA, LFV, etc.), and other organisations as FAA, AirService Australia and EUROCONTROL.
A007	Because voice communication is entirely independent of the ADS-B application, then it is assumed that the likelihood of voice-communication failure would be no greater than for the reference radar-based ATS case (see Table-8 from [Ref.1] and [Ref.12])	PSC ADS-B-NRA section 7.3.1	ED126/DO303 Table-8
A008	Because the aircraft failures are independent of ADS-B operations, then the likelihood of such failures would be no greater than for the reference radar-based ATS case.	PSC ADS-B-NRA section 7.3.1	The validity of this assumption has been confirmed through the RFG process that involved lots of industry, operational people (ATCo, pilots), service providers (NATS, DNSA, LFV, etc.), and other organisations as FAA, AirService Australia and EUROCONTROL.

Ref	Assumption	Source	Validation
A009	The navigation capability of the aircraft is assumed to be sufficient to enable the pilot to comply with a basic procedural separation service (e.g. DME, VOR, NDB, pressure-altitude) thus allowing time, vertical and some lateral distance separation standards to be applied.	PSC ADS-B NRA section 7.3.2 section 8.4.3	ED126/DO303 EMM-1
A010	It is assumed that the integrity failure rate where multiple a/c are affected, for any GNSS system used as position source is no more than 10 <sup>-5</sup> per hour (ASSUMP-28 in [Ref.1]) .	PSC ADS-B-NRA section 7.3.2 section 8.7	This assumption is based on conservative GNSS required performances and not on the current observed performances in operation, which are probably much better.
A011	It is assumed that the integrity failure rate of the horizontal position source impacting one aircraft is no more than 10 <sup>-4</sup> per user (ASSUMP-29 in [Ref.1]).	PSC ADS-B-NRA section 7.3.2 section 8.7	This assumption is based on conservative GNSS required performances and not on the current observed performances in operation, which are probably much better
A012	It is assumed that the management of demand versus capacity (e.g. Flow Management Function) is implemented for the ADS-B-NRA sector as it would be implemented in the reference radar-based ATS (see Guidance for the Provision of Air Traffic Services Using ADS-B in Non Radar Area [Ref.11]).	PSC ADS-B-NRA section 7.4.3	The validity of this assumption has been confirmed through the RFG process that involved lots of industry, operational people (ATCo, pilots), service providers (NATS, DNSA, LFV, etc.), and other organisations as FAA, AirService Australia and EUROCONTROL.
A013	Separation service (airspace classes A - E) provides the most demanding requirements, compared to flight information and other services provided by ADS-B-NRA (ASSUMP-34 in ED126 [Ref.1]).	PSC ADS-B-NRA section 8.2	ED126/DO303 ASSUMP-34

Ref	Assumption	Source	Validation
A014	For the severity classification it has been assumed that the ATCo is managing a high number of aircraft peaking at 15 for en-route and 7 for TMA (see EC-3 of [Ref.1])	PSC ADS-B-NRA section 8.4.2	ED126/DO303 EC-3
A015	The average duration of a flight within a single ATC sector is assumed to be 20 minutes for en-route and 6 minutes for TMA.	PSC ADS-B-NRA section 8.4.3	ED126/DO303 EC-3
A016	The average number of aircraft assumed to be managed per ATSU.hour is 30 for en-route and 10 for TMA (resulting in the following equivalences: 1 ATSU.h = 10 flight.h for en-route and 1 ATSU.h = 1 flight.h for TMA).	PSC ADS-B-NRA section 8.4.3	ED126/DO303 EC-3
A017	The maximum instantaneous count of traffic is assumed to be at any one time 15 aircraft for en-route and 7 aircraft for TMA.	PSC ADS-B-NRA section 8.4.3	ED126/DO303 EC-3
A018	100% of these aircraft are under ADS-B surveillance.	PSC ADS-B-NRA section 8.4.3	ED126/DO303 EC-3
A019	ATCo is assumed to be applying the minimum surveillance separation standard applicable for the airspace (e.g. 5Nm) (EC-4 of [Ref.1])	PSC ADS-B-NRA section 8.4.3	ED126/DO303 EC-4



Ref	Assumption	Source	Validation
A020	It is assumed that ADS-B-NRA for ATS separation services participates to the ATM Safety Targets at the following levels: 35% for severity class 1, 11% for severity class 3, and 9% for severity class 4. Percentages corresponding to severity class 2 have not been defined as no NRA hazard has been identified for this severity class.	PSC ADS-B-NRA section 8.5.1	These percentages are justified by the fact a typical ADS-B-NRA implementation is assumed to take place in an area which is today a procedural environment with limited infrastructure (voice reporting, no radar, no tracking, no display, very basic or no FDPS, etc.), in low density airspace, with low route structure complexity, etc.
A021	It is assumed that controller will always detect the loss of all tracks on the CWP (as in current radar system) (IMM-2. in [Ref.1])	PSC ADS-B-NRA section 8.6.2	ED126/DO303 IMM-2
A022	It is assumed that the probability of a corrupted position being undetected by the ground processing system is 2.5E-4 (per event) (IMM-3 and IMM-5 in [Ref.1]).	PSC ADS-B-NRA section 8.6.2	ED126/DO303 IMM-3 and IMM-5
A023	It is assumed that all position errors (characterised by quality indicator information corruption) being inside a circle with a radius of 50 NM are not detected by ATCo or ground processing system whereas errors outside this radius are detected by either the ground processing or the controller (IMM-4 and IMM-6 in [Ref.1]).	PSC ADS-B-NRA section 8.6.2	ED126/DO303 IMM-4 and IMM-6
A024	It is assumed that failure rates are independent of traffic numbers (ASSUMP-24 of [Ref.1]).	PSC ADS-B-NRA section 8.7	ED126/DO303 ASSUMP-24

Ref	Assumption	Source	Validation
A025	It is assumed that while being under ADS-B-NRA ATS, the probability that an aircraft temporarily loses positioning or surveillance coverage (e.g. due to a steep bank angle), is not greater than 1e-04 per flight.hour (ASSUMP-25 in [Ref.1])	PSC ADS-B-NRA section 8.7	ED126/DO303 ASSUMP-25
A026	It is assumed that there is no detection means on-board concerning either the failure to transmit ADS-B data (FC is not alerted if the ADS-B data is not broadcast) or the transmission or incorrect quality indicators or corrupted ADS-B data (ASSUMP-27 in [Ref.1])	PSC ADS-B-NRA section 8.7	ED126/DO303 ASSUMP-27

## 11.2 OUTSTANDING SAFETY ISSUES

Ref	Safety Issue	Source	Action Required
I001	This PSC is limited to the generic aspects of the ADS-B-NRA specification and does not include local specification	PSC ADS-B-NRA section 1.4	ANSPs to review the contents of the PSC in light of the local operational environment etc
I002	This Safety Case is <i>preliminary</i> in that it addresses only the specification stage of the Application. It does <u>not</u> address implementation issues, although the structure of the Safety Argument presented herein does include a high-level framework for the development of assurance relating to the implementation, transition and in-service stages of the safety lifecycle	PSC ADS-B-NRA section 1.4	ANSPs to address other safety-lifecycle stages
I003	This document does not supersede all assumptions made in the reference documents and in particular those from ED-126/DO 303.	PSC ADS-B-NRA section 5.5	ANSPs to review the contents of the of ED-126 requirements and assumptions in light of the local operational environment.

## 11.3 LIMITATIONS

Ref	Limitation	Source	Implications
L001	The assessment performed and requirements obtained are based on agreed performance and characteristics of GNSS system.	PSC ADS-B-NRA section 8.7	For alternative position sources a dedicated safety and performance assessment is required to demonstrate compliance with the ED-126/DO-303 requirements <sup>46</sup> and assumptions

---

<sup>46</sup> As per paragraph 8.4.7. of [Ref.14].

Page intentionally left blankj

## 12 CONCLUSIONS

This Preliminary Safety Case set out with the aim of showing that the use of ADS-B surveillance in Non Radar Areas by Air Traffic is acceptably safe, subject to satisfaction of the Safety Requirements specified herein<sup>47</sup>. In the context of this document, “acceptably safe” is defined principally against the two following safety criteria: a) the comparison with a radar-based ATS operation in the nominal mode of operation and b) relevant target level of safety (compliant with ESARR4) in the non nominal mode of operation (failure case).

The principal Argument addressed herein is that use of ADS-B surveillance in NRA Application has been specified to be *acceptably safe*. In addressing this Argument, supporting Evidence has been presented to show that:

1. The ADS-B Application underlying surveillance in NRA is intrinsically safe.
2. The design of the system which underlies the Application is complete and correct.
3. The system design functions correctly and coherently under all normal environmental conditions.
4. The system design is robust against external abnormalities in the operational environment.
5. All risks from internal system failure have been mitigated sufficiently,
6. All requirements allocated to each domain or sub-system (and assumptions) are realistic,
7. The approach and methodology used on the safety assessment are adequate to show that the application is acceptably safe, and were applied by competent personnel.

Thus, subject to the caveats presented in section 11 above it is concluded overall that ADS-B-NRA application has been specified to be *acceptably safe*.

Local specification and implementation issues have not been addressed (except in outline) in this Preliminary Safety Case. However, it has been shown that all the Requirements which form the specification of the Application are achievable in a generic implementation.

---

<sup>47</sup> The caveat “subject to satisfaction of the Safety Requirements specified herein” is necessary because this is only a Preliminary Safety Case and therefore doesn't not address implementation issues (except in outline)

**Page intentionally left blank**

**13 REFERENCES:**

- [Ref.1]** EUROCAE ED-126/RTCA DO-303 - "Safety Performance and Interoperability Requirements Document for ADS-B-NRA Application". December 2006
- "This standard provides the minimum operational, safety and performance requirements (SPR) and interoperability requirements (INTEROP) for the implementation of the Automatic Dependent Surveillance - Broadcast (ADS-B) application "Enhanced Air Traffic Services in Non-Radar Areas using ADS-B surveillance" (ADS-B-NRA). This document provides the minimum ADS-B-NRA requirements and allocation of these requirements to both air and ground domains. This standard has been developed by the "ADS-B Requirements Focus Group" (RFG). The RFG was established through the EUROCONTROL / FAA Memorandum of Cooperation. It operates as a joint EUROCAE/RTCA activity assuming the responsibility for the SPR and INTEROP standard material contained in this document."*
- [Ref.2]** ICAO PANS ATM - "Procedures for Air Navigation Services - Air Traffic Management", Document 4444, Fifteen edition 2007, including ADS-B procedures in Chapter 8 "ATS Surveillance Services"
- [Ref.3]** EUROCONTROL - "Safety Case development Manual", DAP/SSH/091, Edition 2.2. Nov 2006
- [Ref.4]** EUROCONTROL - "ANS Safety Assessment Methodology (SAM)" v2.1. Nov 2006
- [Ref.5]** EUROCONTROL - Safety Regulatory Requirement 4 (ESARR4), "Risk Assessment and Mitigation in ATM"
- [Ref.6]** EUROCONTROL - Safety Regulatory Requirement 3 (ESARR3), "Safety Management Systems by ATM Service Providers"
- [Ref.7]** EUROCAE ED-78A / RTCA DO-264 - "Guidelines for approval of the provision and use of Air Traffic Services supported by data communications". December 2000.
- [Ref.8]** ICAO PANS-OPS - "Procedures for Air Navigation Services - Aircraft operations", Document 8168.
- [Ref.9]** ICAO Annex 10 - Aeronautical Telecommunications, Volume IV "Surveillance Radar and Collision Avoidance Systems", Edition 3.

- [Ref.10]** The NRA Flight Crew Manual
- [Ref.11]** Guidance for the Provision of Air Traffic Services Using ADS-B in Non Radar Area
- [Ref.12]** EC 2096/2005 Common Requirements Annex 1 – 8: Contingency Plans for all services it (the ANSP) provides in the case of events which result in significant degradation or interruption of its services.
- [Ref.13]** ED-125 – Guidance to specify an ATM Risk Classification Scheme
- [Ref.14]** EASA Acceptable Means of Compliance (AMC) 20-24
- [Ref.15]** EUROCAE ED-129 Technical Specification for 1090MHz Extended Squitter Ground Station (draft November 2007)
- [Ref.16]** RTCA/DO-229D : Minimum Operational Performance Standards for Global Positioning System/Wide Area Augmentation System Airborne Equipment (dated 13 December 2006)



ACAS	Airborne Collision Avoidance Systems
ADS-B	Automatic Dependent Surveillance - Broadcast
ANSP	Air Navigation Service Provider
ASOR	Allocation of Safety Objectives and Requirements
ATC	Air Traffic Control
ATS	Air Traffic Services
CAP	Close Approach Probability
EASA	European Aviation Safety Agency
ESARR	EUROCONTROL Safety Regulatory Requirement
FC	Flight Crew
GNSS	Global Navigation Satellite System
GSN	Goal Structuring Notation
ICAO	International Civil Aviation Organisation
LOA	Letter Of Agreement
MSAW	Minimum Safe Altitude Warning
MSSR	Monopulse Secondary Surveillance Radar
NAC	Navigation Integrity Category
NACp	Navigation Integrity Category Position
NIC	Navigation Accuracy Category
NUC	Navigation Uncertainty Category
NUCp	Navigation Uncertainty Category Position
NRA	Non Radar Area
OH	Operational Hazard
OHA	Operational Hazard Assessment
OPA	Operational Performance Assessment
OSA	Operational Safety Assessment
OSED	Operational Service and Environment Definition
PR	Performance Requirement
PSC	Preliminary Safety Case
RFG	Requirement Focus Group
SIL	Surveillance Integrity Level
SPI	Special Position Ident
SPR	Safety and Performance Requirement
SR	Safety Requirement

SSR	Secondary Surveillance Radar
STCA	Short Term Conflict Alert
SWSSR	Sliding Window Secondary Surveillance Radar
TMA	Terminal Manoeuvring Area
VHF	Very High Frequency

## Annex A HAZARD CLASSIFICATION MATRIX

This Matrix is directly obtained from §Table 30 of [Ref.1].

Hazard Class	1 (most severe)	2	3	4	5 (least severe)
<b>Effect on Operations</b>	Normally with hull loss. Total loss of flight control, mid-air collision, flight into terrain or high speed surface movement collision.	Large reduction in safety margins or aircraft functional capabilities.	Significant reduction in safety margins or aircraft functional capabilities.	Slight reduction in safety margins or aircraft functional capabilities.	No effect on operational capabilities or safety
<b>Effect on Occupants</b>	Multiple fatalities.	Serious or fatal injury to a small number of passengers or cabin crew.	Physical distress, possibly including injuries.	Physical discomfort.	Inconvenience.
<b>Effect on Air crew</b>	Fatalities or incapacitation.	Physical distress or excessive workload impairs ability to perform tasks.	Physical discomfort, possibly including injuries or significant increase in workload.	Slight increase in workload.	No effect on flight crew.
<b>Effect on Air Traffic Service</b>	Total loss of separation.	Large reduction in separation or a total loss of air traffic control for a significant period of time.	Significant reduction in separation or significant reduction in air traffic control capability.	Slight reduction in separation or in ATC capability. Significant increase in air traffic controller workload.	Slight increase in air traffic controller workload.
<b>Example of ASAS operational effects</b>	<ul style="list-style-type: none"> <li>• <i>Mid-air collision</i></li> <li>• <i>Controlled flight into terrain</i></li> <li>• <i>Total loss of flight control</i></li> <li>• <i>High speed surface movement collision (i.e. collision in runway)</i></li> <li>• <i>Leaving a prepared surface at high speed.</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Large reduction in separation or safety margins</i></li> <li>• <i>Loss of separation resulting in wake vortex encounter at low altitude.</i></li> <li>• <i>Large reduction in safety margins like abrupt maneuver is required to avoid mid-air collision or CFIT (e.g. one or more aircraft deviating from their intended clearance)</i></li> <li>• <i>Large reduction in aircraft functional capabilities</i></li> <li>• <i>Total loss of air traffic control for a significant period of time</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Significant reduction in separation or safety margins</i></li> <li>• <i>Loss of separation resulting in wake vortex encounter at high altitude.</i></li> <li>• <i>Low speed surface movement collision (i.e. collision in taxiway)</i></li> <li>• <i>Leaving a prepared surface at low speed</i></li> <li>• <i>Significant reduction in aircraft functional capabilities</i></li> <li>• <i>Significant reduction in air traffic control capability</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Slight reduction in separation or safety margins</i></li> <li>• <i>Significant increase in air traffic controller workload</i></li> <li>• <i>Slight increase in flight crew workload</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>No effect on operations /traffic</i></li> <li>• <i>Slight increase in air traffic controller workload</i></li> <li>• <i>No effect on flight crew</i></li> </ul>

Page intentionally left blank

## **Annex B ORGANISATIONS INVOLVED IN SPECIFICATION OF ADS-B-NRA**

The organisations involved in the specification of ADS-B-NRA in the framework of the Requirements Focus Group (RFG) are:

Airbus	Johns Hopkins University
Airservices Australia	LFV Group
ALPA	LFV Luftfartsverket
Alticode	LFV Stockholm-Arlanda Airport
BAE SYSTEMS	MITRE/CAASD
Boeing	MLIT Japan
Boeing Air Traffic Management	National Air Traffic Services Ltd - LACC
CNS Support HB	QinetiQ
DGAC	Rockwell Collins
DoD	RTCA
DSNA	SAIC (FAA)
EUROCAE	Egis Avia - Sofreavia
EUROCONTROL	Thales Air Defence SA
FAA	Thales ATM
FAA Flight Standards	Thales Avionics Limited
FAA WJH Technical Centre	United Airlines
United Airlines	

More detail about people from involved in this process can be found in ED-126/DO303 document [Ref.1].

### Annex C COMPARISON BETWEEN ADS-B-NRA AND RADAR CASES W.R.T. COORDINATION AND TRANSFER

FROM AN ADJACENT SECTOR TO ADS-B-NRA			Difference between SSR sector case and ADS-B-NRA case	
TRANSFERRING SECTOR		RECEIVING SECTOR	w.r.t. transfer of identification ?	w.r.t. separation ?
Transferring sector type	Methods used for transfer of identification			
Procedural	n.a.	ADS-B-NRA	<b>No difference</b>	<b>No difference</b> , aircraft transferred in conformance with procedural based minima (e.g. 10 minutes longitudinally) as per agreed LOA's.
SSR sector	Mode A code based		<b>No difference</b> if Mode A code transmitted by the aircraft and managed by the ground system	<b>No difference</b> , transferring and receiving sector would be able to establish an LOA to enable the inter-sector transfer of aircraft separated by surveillance based minima such as 5Nm or other defined agreed distance.
	Other than Mode A code based		<b>Different</b> (for transferring and receiving sectors) compared to the SSR sector if Mode A code not transmitted by the aircraft or not managed by the ground system. Existing alternate ICAO procedures have to be used	
			<b>No difference</b>	


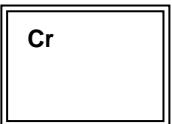

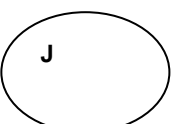
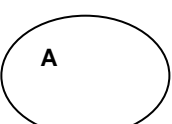
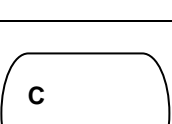

**FROM ADS-B-NRA TO AN ADJACENT SECTOR**

TRANSFERRING SECTOR		RECEIVING SECTOR	Difference between SSR sector case and ADS-B-NRA case	
Transferring sector type	Methods used for transfer of identification		w.r.t. transfer of identification ?	w.r.t. separation ?
ADS-B-NRA	Mode A code based if Mode A code transmitted by the aircraft and managed by the ground system	SSR sector	No difference	No difference, transferring and receiving sector would be able to establish an LOA to enable the inter-sector transfer of aircraft separated by surveillance based minima such as 5Nm or other defined agreed distance.
	Mode A code based si not possible if Mode A code not transmitted by the aircraft or not managed by the ground system		Different (for transferring and receiving sectors) as method based on Mode A code is not possible in that case. Existing alternate ICAO procedures have to be used	
	Other than Mode A code based		No difference	
	n.a.	Procedural	No difference	





## Annex D GOAL STRUCTURING NOTATION LEGEND

	<b>Goal</b>	<p>A goal is a requirement or target to be met or shown to be true.</p> <p>In this document, goals are called arguments.</p>
	<b>Criteria</b>	<p>Criteria are the means by which satisfaction of particular goals, strategies, choices and solutions can be assessed or checked.</p>
	<b>Strategy</b>	<p>A goal or set of goals can be solved by a strategy, which breaks those goals down into a number of sub-goals. The interpretation is that the solution of the sub-goals ensures the solution of the parent goals.</p>
	<b>Justification</b>	<p>The various elements of the GSN can all be given justifications for their use. Justifications are most frequently associated with strategies.</p>
	<b>Assumption</b>	<p>An assumption is an assertion that some element of the goal structure (e.g. Goal or Strategy) has to rely on, in order for it to be satisfiable. An assumption is some fact that has to be assumed about the environment, system, theories, etc., for the goal structuring element to be valid.</p>
	<b>Context</b>	<p>Context provides the inputs or background information that a goal or other goal structuring element requires for it to be understood or satisfied. It will include analysis results, hazard logs, etc. in some senses models and assumptions could be regarded as special cases of context, but are treated as separate entities because of their importance in defining goal structures.</p>
	<b>Solution</b>	<p>Solutions provide the evidence for satisfaction of goals. They may be individual pieces of analysis, evidence, results of audit reports, references to design material, etc.</p>



## **Annex E SUMMARY OF THE MONTE-CARLO ANALYSIS SUPPORTING THE CALCULATION OF THE PE VALUES FOR HAZARDS OH3 AND OH4 – UNDETECTED CASES**

This annex is a summary extracted from [Ref.1], appendix C.1.2.2.4.

A Monte-Carlo analysis was used to help assess the likelihood of collision given an error in the position information that affects both the navigation and surveillance functions.

The analysis was performed by examining several stressing scenarios in which it is assumed that because it is unknown to the controllers and flight crews that the data is in error, they continue to act as they normally would with correct information. That is, since the flight crews and controllers are both unaware that the data is erroneous, it is assumed that the erroneous observed positions of the aircraft would be treated as if they were correct positions. The controller would request the aircraft to follow a perceived normal path and the flight crews would follow the perceived normal path. The true positions of the aircraft, unbeknownst to the flight crew and the controller, are somewhere else. The question that the Monte-Carlo analysis attempts to answer is: given the appearance of a normal situation, what is the likelihood of collision when there is an undetected integrity failure, i.e., the data is actually in error?

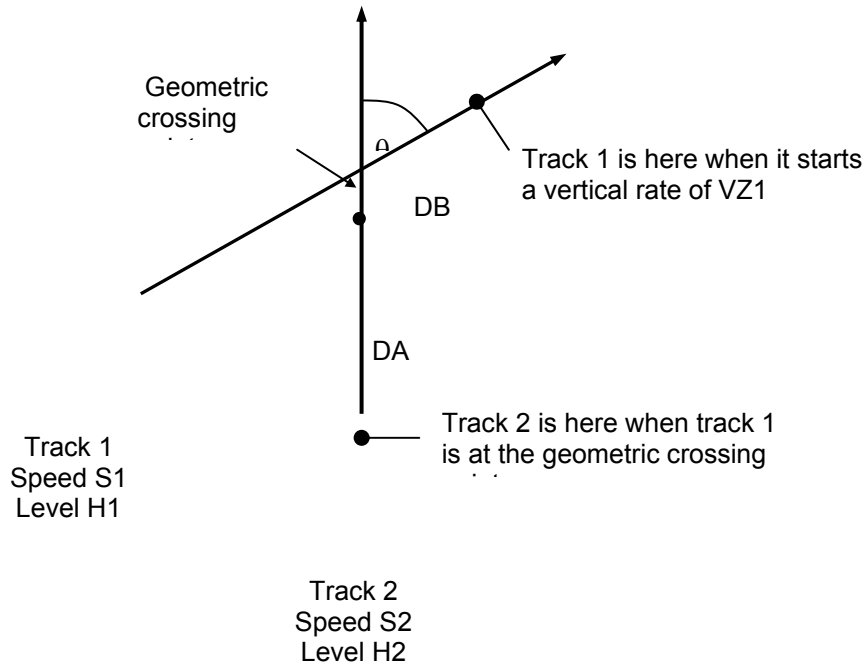
### Scenarios

A number of aircraft track pair scenarios (in line with CAP), involving the reliance on the horizontal surveillance separation minimum, were described by operational experts. The scenarios essentially involved two types of situations:

- Crossing tracks, at different crossing angles, some at the same level and some involving a vertical change after crossing with 1000ft vertical separation.
- Parallel / in-trail tracks, separated in either the across-track or along-track directions by the separation minimum.

The required track scenarios were then described mathematically for modelling according to the parameters defined in the Figure 13 below.

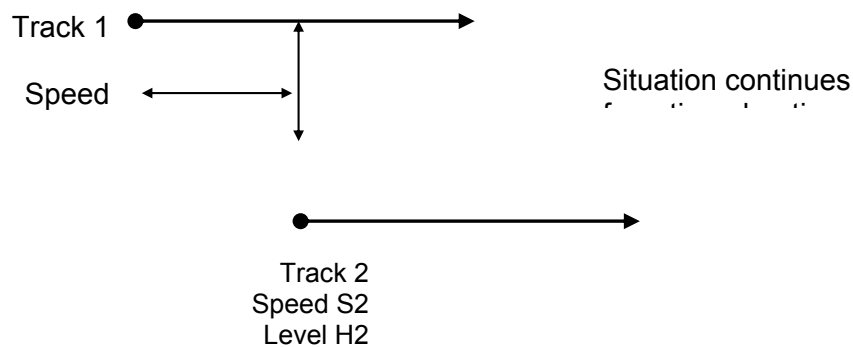
### Crossing track parameters



### Crossing track scenarios

Scen	S1 (kt)	S2 (kt)	H1 (ft)	H2 (ft)	$\theta$ (deg)	DA (NM)	DB (NM)	VZ1 (ft/min)
C-1	300	300	8000	9000	90	2	2	2000
C-2	300	300	8000	8000	90	5	0	0
C-3	300	300	8000	8000	45	5	0	0
C-4	540	540	33000	34000	80	5	-9	1000
C-5	540	540	33000	34000	60	-5	-9	1000

### Parallel track parameters



### Parallel track scenarios

Scen	S1 (kt)	S2 (kt)	H1 (ft)	H2 (ft)	Sx (NM)	Sy (NM)	VZ1 (ft/min)	Td (min)
P-1	300	300	10000	10000	5	0	0	5
P-2	300	300	10000	10000	0	5	0	5
P-3	540	540	33000	34000	5	0	500	3

### Figure 13: Monte Carlo Scenario Definitions

#### Analysis Method

In general, Monte-Carlo techniques simulate scenarios with random perturbations based on error models. Many runs are done based on the error models, and then statistics are gathered on measures of interest. Conclusions are drawn from this modelled statistical characterization.

Each scenario described in the preceding sections was repeated many times with different errors in the actual position. Specifically, the true positions of the aircraft were displaced from the positions that the controllers and flight crews “observed” in the model. The position errors were assumed to have a fixed bias for each simulation run (in line with CAP). Based on the error model, the errors might be such that the aircraft appear to be farther apart than they actually are, which might potentially cause a collision. Figure 14 illustrates the idea.

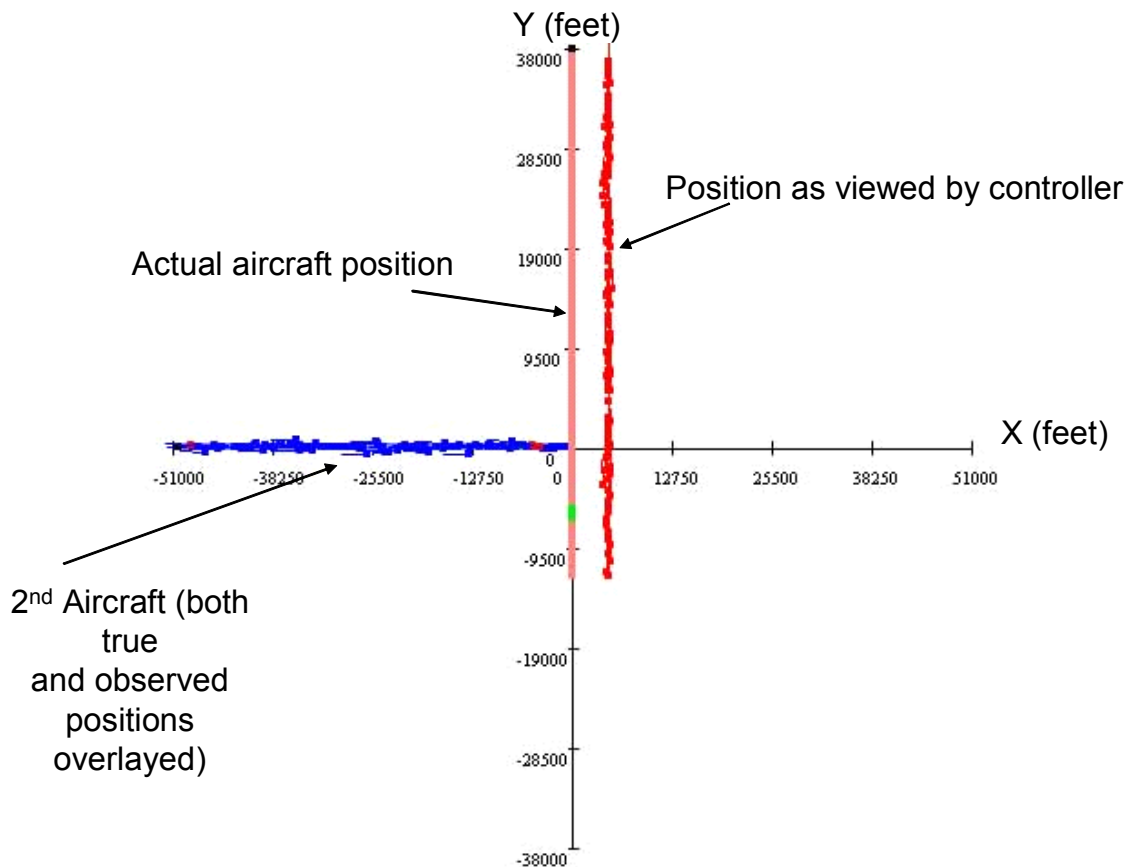


Figure 14 Example Trajectory for Monte-Carlo Model (Based on Scenario C-1)

In our case the statistic of interest is the distribution of the actual point of closest approach, and what the probability is of the closest point of approach being a critical near mid-air collision, with the center-of-mass to center-of-mass distance being less than 500 ft. The critical near-mid-air collision criterion is used as a surrogate for an actual collision.

In [Ref.1], appendix C.1.2.2.4., figure 48 shows the distribution of results for scenarios C1 through C4, and figure 49 shows the distribution of results for scenarios P1, P2, and P3. The closest point of approach through all runs was 1500 ft.

It is noted that through the course of 1,500,000 runs of what are considered to be stressful scenarios, there was not a single critical near-mid-air collision. Therefore based on this analysis, we consider the  $Pe_{pca}$  estimate of  $1 \times 10^{-7}$  to be conservative.