Safety Assessment for 15.04.05b Prototype Second Iteration

Document information	
Project Title	Surveillance Ground System Enhancements for ADS-B (Prototype Development)
Project Number	15.04.05b
Project Manager	Thales
Deliverable Name	Safety Assessment for 15.04.05b Prototype Second Iteration
Deliverable ID	Del 15
Edition	00.01.01
Template Version	03.00.00
Task contributors	
EUROCONTROL;INDRA;NATS;NORACON;SELEX;THALES	

Abstract

SESAR WP15.4.5 will implement security and other enhancements into selected elements of the ADS-B ground surveillance system. Elements for enhancements are the ADS-B groundstation, SDPD system (EUROCONTROL ARTAS), performance assessment tool i.e. SASS-C and ASTERIX interfaces between these units.

WP15.4.5 is organised into 3 Prototype Iterations, with each iteration aligned to a different SESAR CONOPS. Prototype 2nd Iteration is aligned to SESAR Trajectory Based Operations CONOPS [1]. WP15.4.5a provides the system design, interface and test specifications and WP15.4.5b develops prototype ADS-B ground systems from these documents.

Strategic project aims and requirements for the ADS-B ground system 2nd Iteration Prototype are defined within various WP15.4.5a System [2] and ADS-B GS specification [3] and are summarised in the 2nd Iteration Baseline Matrix Report [4].

This report builds on the foundations described within the 1st Iteration Safety Report, Deliverable 08 [5]. It details operational hazards ascribed to ADS-B NRA [6], ADS-B RAD [7] and ADS-B APT [8] ATM applications and their Safety Objectives and Requirements and can be considered within the update to the ADS-B Groundstation Technical Specification, ED-129 [9] and GEN SUR SPR work being conducted in EUROCAE WG51 SG4.

Authoring & Approval

Prepared By		
Name & Company	Position & Title	Date
[redacted]	NATS [redacted]	30/10/2013

Reviewed By		
Name & Company	Position & Title	Date
[redacted] THALES	[redacted]	04/11/2013
[redacted] INDRA		04/11/2013
[redacted] THALES		04/11/2013
[redacted] SELEX		04/11/2013
[redacted] NORACON		04/11/2013
[redacted] EUROCONTROL		04/11/2013

Reviewed By – *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date

Approved for submission to the SJU		
Name & Company	Position & Title	Date
[redacted] THALES	[redacted]	11/11/2013
[redacted] INDRA		11/11/2013
[redacted] NATS		11/11/2013
[redacted] EUROCONTROL		11/11/2013
[redacted] SELEX		11/11/2013

Rejected By		
Name & Company	Position & Title	Date
None		

Rational for rejection
None.

Document History

Edition	Date	Status	Author	Justification
00.00.01	24/07/2013	Draft	[redacted]	First Draft
00.01.00	28/08/2013	Issued		Issued document
00.01.01	11/11/2013	Issued		Amended in line with SJU Assessment comments

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

List of tables

List of figures

Executive summary

SESAR WP15.4.5 has the stated objective of implementing technological enhancements into ADS-B ground based surveillance, termed the enhanced ADS-B ground system. The enhanced ADS-B ground system is defined to comprise 1090 ADS-B groundstations, connected to Surveillance Data Processing and Distribution (SDPD) systems via suitability modified ASTERIX interfaces [1].

The objective of the implemented enhancements is to mitigate security concerns within ADS-B surveillance services, so they can augment radar services within High Density (HD) controlled airspace and offer standalone services in lower density operating environments [1]. In-addition, it will enable ADS-B surveillance of mobile units i.e. aircraft and ground vehicles on the airport surface [1,4].

ATM applications have been defined for these ADS-B modes of operation. The ground based ADS-B surveillance applications are termed ADS-B RAD (Radar airspace) for high density operational environments and ADS-B NRA (Non-Radar Airspace) for lower density operational environments. They are defined in EUROCAE Safety, Performance and Interoperability Requirements (SPR) ADS-B application documents, termed ED-161 [7] and ED-126 [6] respectively. The airport ground surveillance application is termed ADS-B APT and is defined in EUROCAE SPR document ED-163 [8].

WP15.4.5b Prototype 2nd Iteration is aligned with SESAR Trajectory Based Operations CONOPS and has been defined to support ADS-B RAD and ADS-B APT applications explicitly, in-addition to the implicit ADS-B NRA application [1]. Each ADS-B ATM application is defined within its Safety and Performance and Interoperability Requirements Document. This report describes the structure of a EUROCAE SPR document, comprising i) Operational Service and Environment Description (OSED), ii) Operational Performance Assessment (OPA), iii) Operational Safety Assessment (OSA) and iv) Interoperability Assessment (IA).

Safety Requirements and Performance Requirements generated within the OSA and OPA respectively are combined into Safety and Performance Requirements (SPR) within the SPR summary section. The SPR summary section also contains the ADS-B application Functional Model, for the purpose of allocation of Operational, Performance and Safety Requirements within the Airborne and Ground domains in the performed assessments.

The report presents a summary of the ADS-B NRA, RAD and APT SPR documents, comprising:

SPR Functional Model for each application and salient points from each OSED

Detailed summary of the Operational Safety Assessment comprising

- Operational Hazard list
- ATM Safety Target and ADS-B application Safety Target determination,
- Safety Objectives and Probability of Effect values,
- Safety Requirements for each application and
- Safety and Performance Requirements derived from the Safety Requirements

The final section draws all elements into a proposed enhanced ADS-B ground system functional model and combined NRA, RAD and APT SPR requirements set for consideration in the design of the enhanced ADS-B ground system developed within WP15.4.5.

This report is aimed at Air Navigation Service Providers who are unfamiliar with the format and content of the available ADS-B applications standards and are considering integrating the enhanced ADS-B ground system into their surveillance infrastructure, to increase capability and reduced equipment costs. The report presents a summary of the available ADS-B applications and hence aims to help the ANSP to select a ADS-B operating environment which matches their needs and informs them of the relevant Safety Requirements which they should consider within a procurement activity.

It is further planned that the identified Safety Requirements will be validated against the three manufacturers ADS-B ground system elements within the 3rd Iteration Safety Assessment report, document D22 as this prototype will comprise the fully developed enhanced ADS-B ground system within the WP15.4.5 project. The validation approach will be identified and agreed within the 3rd Iteration Kick Off Activity through consultation with EUROCONTROL and SJU Safety Subject Matter Experts and is expected to feature use of relevant Safety Guidance Material generated in SESAR WP16.06.01 and EUROCAE ED-109/ED-153.

1 Introduction

1.1 Purpose of the document

This document gives an overview of the enhanced ADS-B ground system specified within SESAR 15.4.5b Prototype Second Iteration and a summary of supported ADS-B ATM applications within the Prototype Second Iteration [1]. It details the Safety Requirements allocated to each ADS-B ATM Applications and proposes a new ADS-B Functional Model for the enhanced ADS-B Ground System elements.

1.2 Intended readership

The audience of this document includes:

Projects 15.04.05.a and b,

SJU projects that may require ADS-B Surveillance Systems for their validation activities.

SESAR ANSP's planning to implement basic ADS-B systems into their ATM surveillance infrastructure.

1.3 Inputs from other projects

Input documents in the form of system specifications, interface specifications and test specifications for the enhanced ADS-B ground system from 15.4.5a.

1.4 Structure of the document

Executive Summary

Chapter 1: Introduction

Chapter 2: Safety and Security

Chapter 3: ADS-B NRA ATM Application

Chapter 4: ADS-B RAD ATM Application

Chapter 5: ADS-B APT ATM Application

Chapter 6: Enhanced ADS-B Ground System

Chapter 7: Conclusions

Chapter 8: Assumptions

Chapter 9: References

1.5 Functional block Purpose

1.5.1 Enhanced ADS-B ground system overview

WP15.4.5b is tasked with taking the system design, system test and interface specifications from WP15.4.5a and developing enhanced ADS-B ground system prototypes. These were termed Prototype First, Second and Third Iteration and this document is concerned with Prototype Second Iteration of the enhanced ADS-B ground system [1].

The enhanced ADS-B ground system comprises the following system elements [2];

Enhanced ADS-B groundstation(s) [3]

Enhanced Surveillance Data Processing and Distribution system [10]

Modified ASTERIX Category interfaces; comprising ADS-B target reports in CAT 021 and ADS-B service and status messages in CAT 023 and System Track target reports in CAT 062 and System service and status messages in CAT 063 [11]

A schematic representation of the enhanced ADS-B ground system is highlighted within the dashed blue line region in Figure 1 [2]:

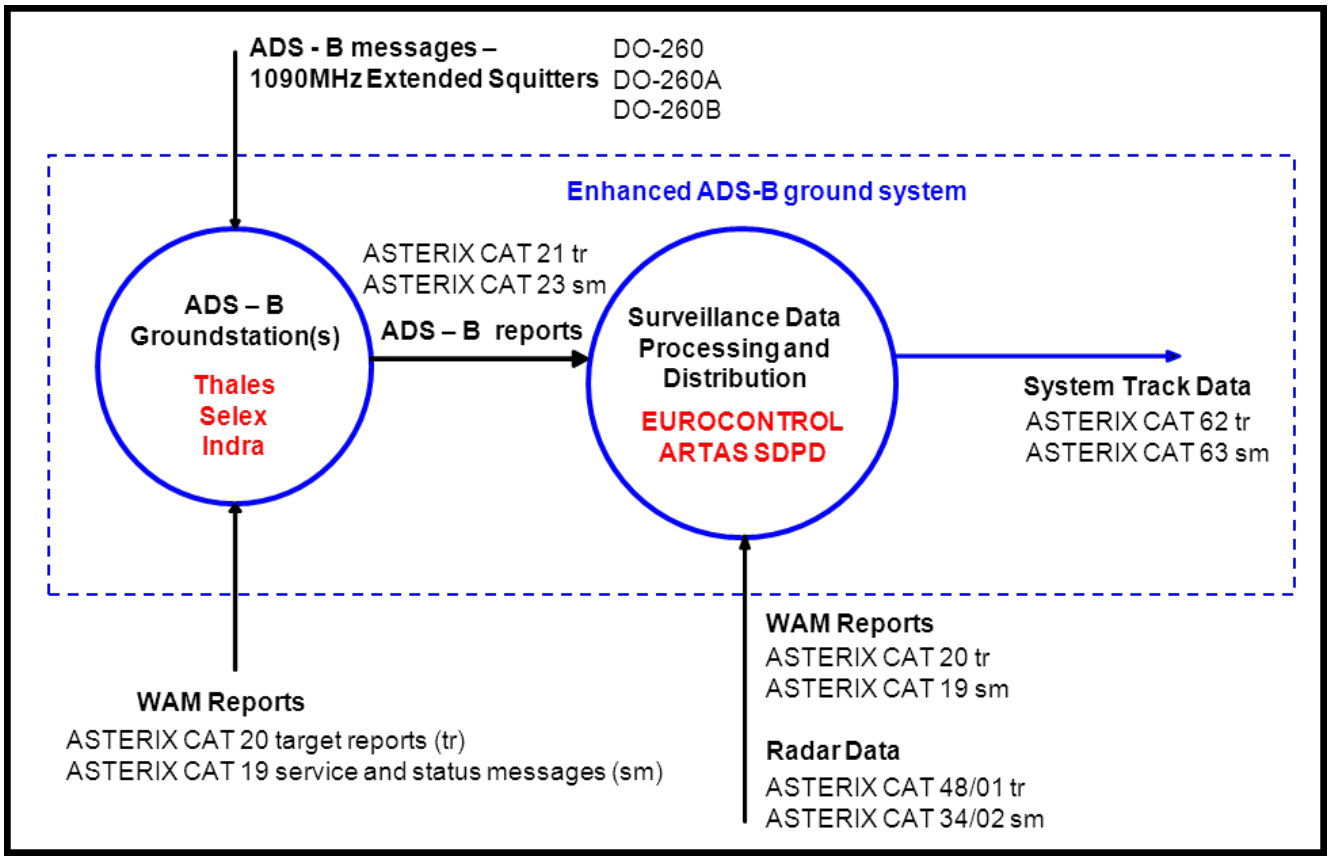

Figure 1 - Enhanced ADS-B ground system schematic

1.6 Functional Block Overview

1.6.1 Enhanced ADS-B groundstation overview

The primary functions of the enhanced 1090 ADS-B Groundstation (GS) are [2]:

Receive 1090 MHz RF input on the Air Interface

Extract message payload data from 1090MHz Extended Squitter ADS-B messages

Timestamp the decoded ADS-B messages using the UTC Time Sync function

Assemble the ADS-B message data into ASTERIX Category 021 target reports

Dispatch ASTERIX CAT 021 ADS-B target reports and ASTERIX CAT 023 service and status messages to client systems over the Ground Interface [11]

Interacts with the Remote Control and Monitoring system through the Management Interface, using SNMP messaging protocols

Determines the internal status of the groundstation equipment through BITE

A functional block diagram of the 1090 GS is shown in Figure 2:

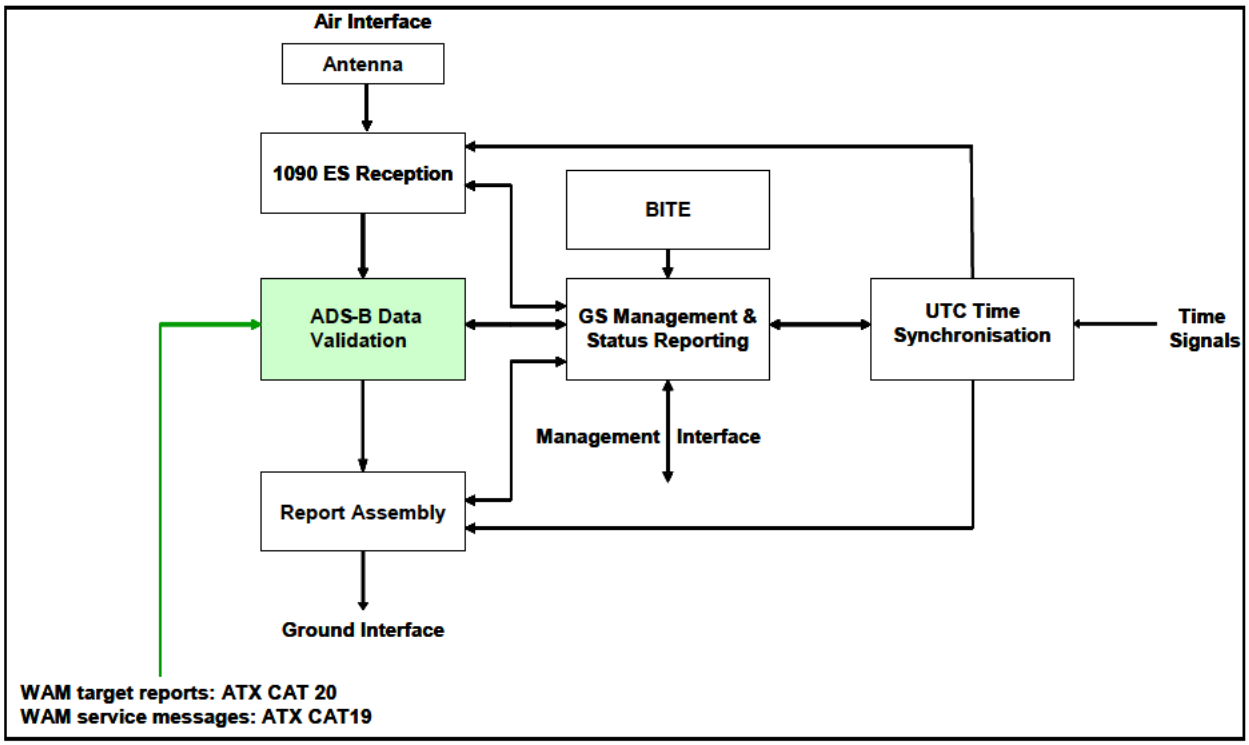

Figure 2 - 1090 GS Component Overview[1]

In comparison with the functional blocks specified against the basic ADS-B-RAD groundstation in ED-129 [9], it is noted that the ADS-B Data Validation functional block (shown in green in Figure 2) has been added incorporating the additional security enhancement functionality required by the enhanced ADS-B ground system [2].

[1] The partitioning shown is for the purpose of describing the high level behaviour of the Ground Station and is not intended to convey an implementation requirement or the physical architecture of the equipment

1.6.2 SDPD system overview

The Surveillance Data Processing & Distribution system (SDPD) receives aircraft data from individual surveillance sensors, including ADS-B 1090 MHz Extended Squitter Ground Station, and serves fused surveillance track updates to client systems such as Controller Working Positions (CWP). Aircraft data updates contain measured or reported 2-D horizontal position, reported altimeter altitude, velocity, status and other information extracted from aircraft onboard systems and received by ground based surveillance sensors [10].

The primary function of the SDPD is to present an accurate and complete air situation picture in ASTERIX Category 062 to its client systems. The CAT 062 picture is composed of input surveillance target report data received in ASTERIX Categories 048/001 (radar), 020 (WAM) and 021 (ADS-B) target messages and fused into a composite air picture [3].

The SDPD uses the input service and status messages in ASTERIX Categories 034/002 (radar), 019 (WAM) and 023 (ADS-B) to determine the validity of the separate surveillance system supplied target data stream and hence to discard or include each particular surveillance target data stream.

The EUROCONTROL ARTAS product was selected as the SDPD element within the enhanced ADS-B system and is designed around four main functions [10];

The TRACKER processes the input surveillance information (from the surveillance sensors) and maintains the Track Data Base,

The SERVER performs the Track Information Service i.e. the management of all requests from Users and the transmission of the relevant sets of track data to these Users. It will also execute the so-called inter-ARTAS cooperation functions.

The SYSTEM MANAGER performs the functions related to the supervision and management of the ARTAS Unit,

The RECORDING function will record selected data related to the operational use of ARTAS.

A functional block diagram of the ARTAS SDPD system is shown in Figure 4 [10]:

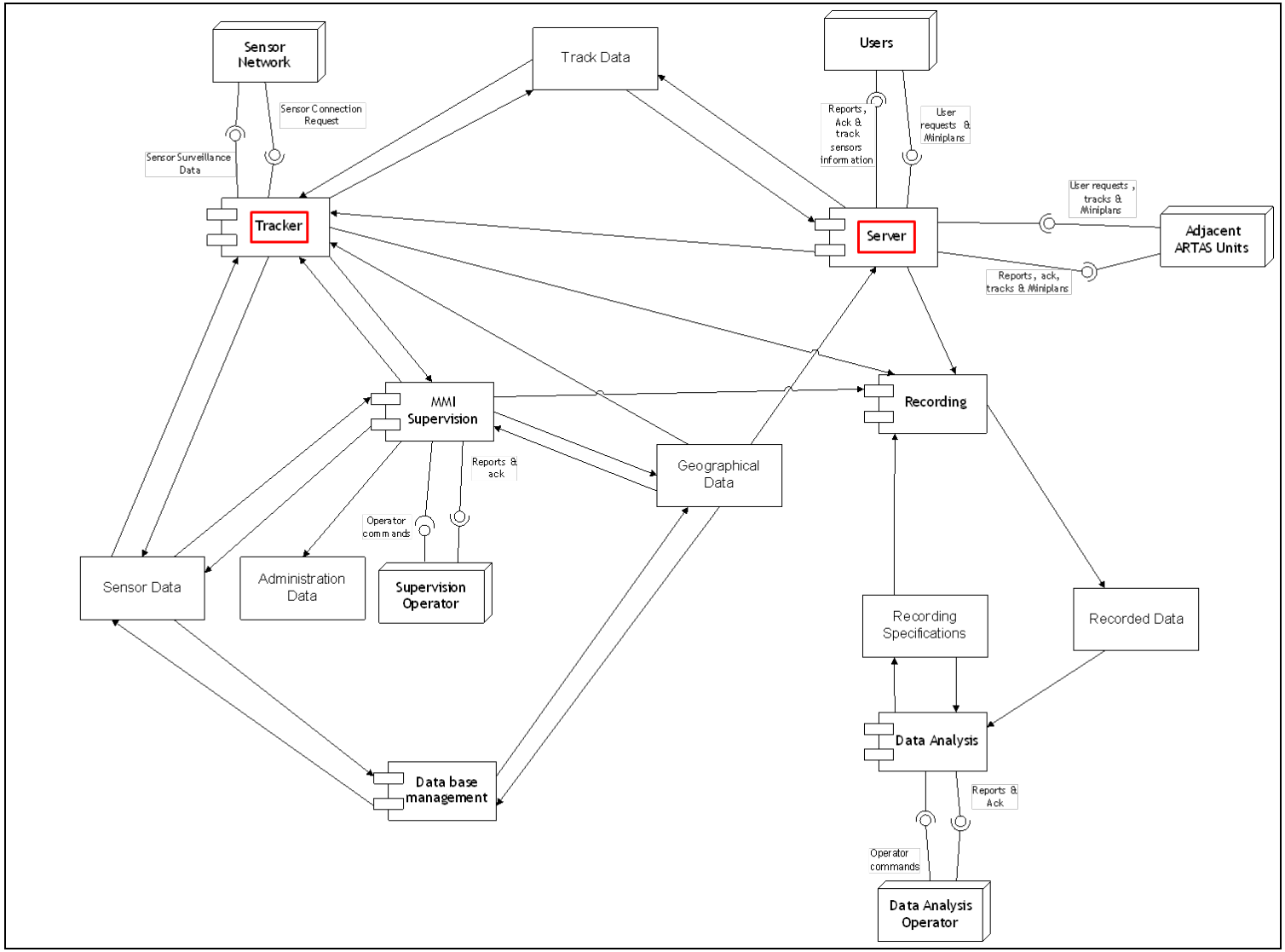
Sensor Network
Track Data
Users
Sensor Connection Request
Sensor Surveillance Data
Reports, Ack & track sensors information
User requests & Miniplans
User requests, tracks & Miniplans
Tracker
Server
Adjacent ARTAS Units
Reports, ack, tracks & Miniplans
MMI Supervision
Recording
Reports & ack
Geographical Data
Operator commands
Sensor Data
Administration Data
Supervision Operator
Recording Specifications
Recorded Data
Data Analysis
Data base management
Reports & Ack
Operator commands
Data Analysis Operator

Figure 3. ARTAS functional overview

1.7 Glossary of terms

None

1.8 Acronyms and Terminology

Term	Definition
A-SMGCS	Advanced Surface Movement and Ground Control System
ACC	Area Control Centre
Ack	Acknowledgement
AD	Airport/Aerodrome
ADS-B	Automatic Dependent Surveillance – Broadcast
ADS-B NRA	Enhanced ATS in Non Radar Areas (“ADS-B out” application)
ADS-B RAD	Enhanced ATS in Radar Areas (“ADS-B out” application)
AoA	Angle of Arrival
APT	AirPorT
ARTAS	ATM suRveillance Tracker And Server
ASAS	Airborne Separation Assistance System
ASOR	Allocation of Safety Requirements
ASTERIX	All-purpose Structured EUROCONTROL Surveillance Information Exchange
ATC	Air Traffic Control
ATCO	Air Traffic Control Officer
ATM	Air Traffic Management
ATSAW	Airborne Traffic Situational Awareness
ATSU	Air Traffic Service Unit
ATX	ASTERIX
B	Barrier
BC	Basic Cause
BITE	Built-in Test System
C	Corruption

Term	Definition
CAT	Category
CONOPS	Concept of Operations
CWP	Controller Working Position
DO	RTCA Document
EC	Environmental Condition
ED	EUROCAE Document
EMM	External Mitigation Means
ES	Extended Squitter
ESSAR	EUROCONTROL Safety Regulatory Requirement
EUROCAE	European Organisation for Civil Aviation Equipment
FIS	Flight Information Service
G	Gate
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GS	Ground Station
HD	High Density
IA	Interoperability Assessment
ICAO	International Civil Aviation Organization
ID	Identity
IMM	Internal Mitigation Means
INTEROP	Interoperability
IR	Interoperability Requirements
L	Loss
MM	Mitigation Means
MMI	Man Machine Interface
Mode S	Mode Select
MOPS	Minimum Operational Performance Standards

Term	Definition
MST	Multi-sensor Tracking
NM	Nautical Mile
Nmax	Maximum Number
NRA	Non Radar Airspace
OE	Operational Effect
OH	Operational Hazard
OHA	Operational Hazard Assessment
OPA	Operational Performance Assessment
OR	Operational Requirement
OSA	Operational Safety Assessment
OSED	Operational Service and Environment Description
OSEIC	Operational Services and Environment Information Capture
Pe	Probability of Effect
PR	Performance Requirement
PSR	Primary Surveillance Radar
RAD	Radar
RCS	Risk Classification Scheme
RF	Radio Frequency
RTCA	Radio Technical Commission for Aeronautics
SC	Severity Class
SDPD	Surveillance Data Processing and Distribution
SES	Single European Skys
SESAR	Single European Sky ATM Research (Programme)
SJU	SESAR Joint Undertaking
SO	Safety Objective
SM	Service and status Messages
SMNP	Simple Network Management Protocol

Term	Definition
SMR	Surface Movement Radar
SPR	Safety and Performance Requirements
SR	Safety Requirements
SSR	Secondary Surveillance Radar
ST	Safety Target
TOA	Time of Arrival
TDOA	Time Difference Of Arrival
TMA	Terminal Manoeuvring Area
UTC	Universal Time Constant
TR	Target Reports
VC	Visibility Conditions
WAM	Wide Area Multilateration
WG	Working Group
WP	Work Package

Table 1 - Acronyms and Terminology

2 Safety & Security

Security aspects of the 2nd Prototype Iteration ADS-B ground system are covered within the D16 Security Assessment report [12].

This report will focus on the safety aspects of the 2nd Iteration supported ADS-B applications and their respective SPR documents as the reference for the Logical Functional Models, Operational Hazards, Safety Objectives and derived Safety Requirements.

It follows the OSA process described within the First Prototype Iteration Safety Report and further developed within this report [5].

2.1 2nd Iteration Supported ADS-B ATM Applications

All currently defined ADS-B ATM applications share a common logical ADS-B system airborne and ground environment functional architecture diagram, shown in Figure 4 [6]:

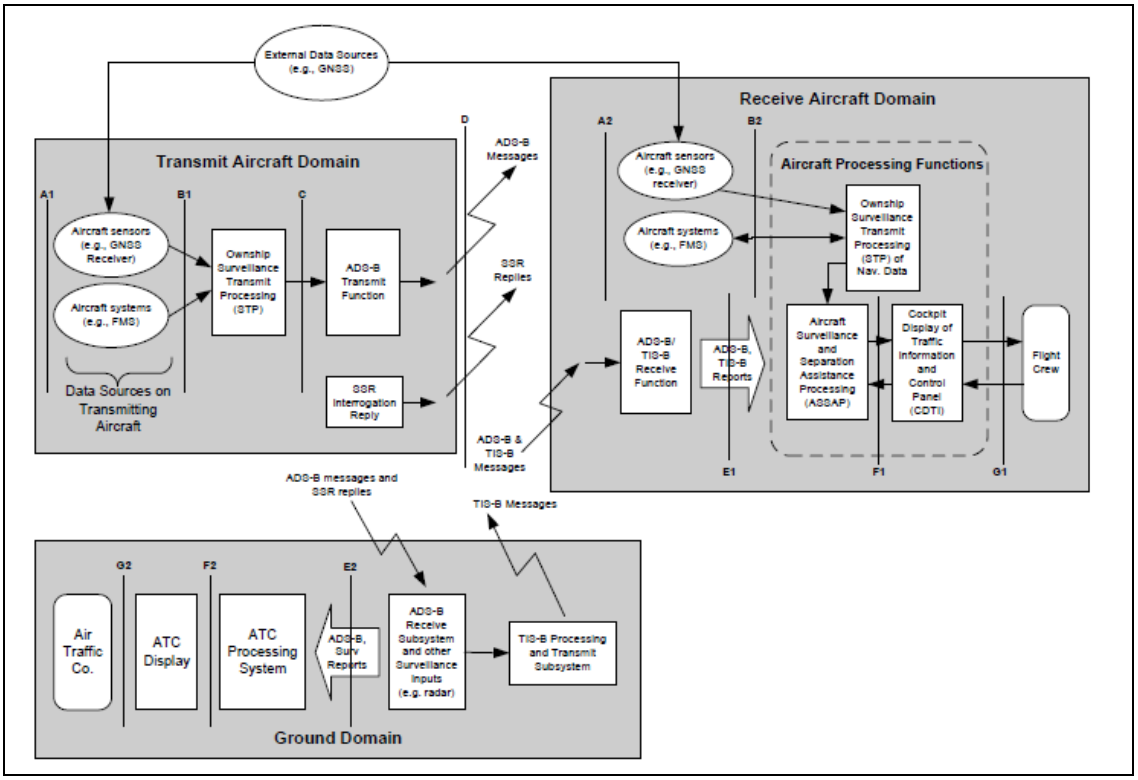

Figure 4. Generic Airborne and Ground Domain ADS-B Functional Model

Each ADS-B application sub-divides the generic ADS-B system functional model into the relevant elements to the application in question.

Airborne applications, such as ATSAW and ASAS applications using 'ADS-B in' techniques which reside in the Transmit Aircraft and Receive Aircraft domains [6]

ADS-B out applications involving ground surveillance applications, including ADS-B NRA, RAD and APT which reside in the Transmit Aircraft and Ground Domains

WP15.4.5b Prototype Iteration Two is defined explicitly to support:

ADS-B RAD ATM application, ED-161, enabling the ADS-B surveillance service to be used in-conjunction with existing radar services in busy, ATC controlled airspace [7]

ADS-B APT ATM application, ED-163, which enables ADS-B surveillance of Mobiles units i.e. aircraft and surface vehicles on airport Manoeuvring areas [8].

This definition is initially made in the Specification Baseline Document for WP15.4.5a [1] and further elaborated in the Prototype Second Iteration Baseline Report/Matrix produced in WP15.4.5b [4].

The Baseline Report [4] also states that the ADS-B Ground Surveillance System shall support standalone operation in lower density operating environments and that this airspace could be a Non-Radar Airspace type environment. Therefore, it is assessed that the Second Iteration Prototype should also support the **ADS-B NRA** ATM application, as defined in ED-126 [6].

A review of the ADS-B NRA, RAD and APT SPR documents was undertaken to determine if Ground Domain Safety Requirements from the three applications could be normalised and hence form input conditions into the proposed enhanced ADS-B ground system OSA activity.

2.2 EUROCAE SPR Document Overview

Each EUROCAE Safety and Performance Requirements document for an ATM application is organised into four assessment activities, in the manner proposed within ED-78A [19] and described within the 1st Iteration Safety Assessment report [5].

In summary, these comprise:

1. Operational Services and Environment Information Capture (OSEIC) activity, resulting in an Operational Services and Environment Description or **OSED** [19]. The OSED defines the operational objectives, services, intended functions and associated procedures of the developed application and assumptions regarding its operating environment [8].

   Operational objectives apply to aircraft operators and ATS providers through the implementation of ATM supported by data communications [19]. In the context of this study, data communications taken to be the provision of surveillance services. The OSED output is a set of Operational Requirements, **OR#**, characterising the developed application.

   The OSED contain the application logical functional architecture, representing the interconnected elements of the application located within either the airborne or ground domain which enable the application to deliver the required surveillance service. The functional architecture defines the interfaces between the domains and functional elements within each domain.

2. Interoperability Assessment or **IA**. The IA identifies the minimum interface requirements, **IR#**, enable all elements of the implemented CNS/ATM system to function correctly together in the end-to-end functional architecture, linking the various airborne and ground domain elements into a whole system [19].

3. Operational Performance Assessment or **OPA**. The OPA derives a set of Performance Requirements, **PR#**, by examining the all of the OR set and assumptions defined within the OSED and establishing the minimum performance requirements which the application must meet to satisfy these conditions under nominal conditions [8].

4. Operational Safety Assessment or **OSA**. The OSA derives Safety Requirements, **SR#**, through the consideration of Operational Hazards introduced by the developed application or modification of existing ATM Operational Hazards which the application may adversely affect. The OSA process is described in more detail within the following section, given the safety focus of this report [19].

The most stringent requirement values from the OPA and OSA activities are combined into Safety and Performance Requirements or SPR and presented within the Safety and Performance Requirements summary at the start of each SPR document [8].

The SPR section also contains the ADS-B application Functional Model, which for the purpose and allocation of requirements tailors the generic Airborne and Ground Domain ADS-B Functional Model shown in Figure 4 to the specifics of the ADS-B application in question.

Given the safety focus of this report, the OSA process is described in detail in the following section.

2.3 Operational Safety Assessment

Operational Safety Assessment process comprises an Operational Hazard Assessment, **OHA**, followed by an Allocation of Safety Requirements, **ASOR** process [8].

2.3.1 Operational Hazard Assessment

Operational Hazard Assessment process is organised into the following steps:

2.3.1.1 Operational Hazard Identification and Classification

The first step in the OHA is the identification and assessment of Operational Hazards (OH) relevant to the application OSED. Detected and undetected conditions of each Operational Hazard are assessed, except in cases where the undetected condition of the hazard was assessed to not be a creditable failure mechanism [5].

Detected and undetected OH conditions are sub-divided into risk Severity Classes using the Risk Classification Scheme (RCS) proposed within ED-78A and repeated in Table 2 [19]:

Hazard Class	1 (most severe)	2	3	4	5 (least severe)
Effect on Operations	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
Effect on Occupants	Multiple fatalities.	Serious or fatal injury to a small number of passengers or cabin crew.	Physical distress, possibly including injuries.	Physical discomfort.	Inconvenience.
Effect on Air crew	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.
Effect on Air Traffic Service	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 slight reduction in air traffic control capability. Significant increase in air traffic controller workload.	Slight increase in air traffic controller workload.

Table 2. ED-78A Risk Classification Scheme – Severity Class 1 -5 definitions

5 ATM risk Severity Classes are defined, with Severity Class 1 the most severe in terms of effect on the aircraft and ATM operation, decreasing to Severity Class 5, which is defined to have no impact on either aircraft or ATM operations

2.3.1.2 Overall ATM Safety Targets for Severity Classes 1-4

Safety Targets (ST) for all Operational Hazard test cases assessed to be Severity Classes 1-4 are then calculated. SC5 are not assessed, as they are deemed to not affect the ATM operation. A Safety Target specifies the overall maximum frequency of occurrence of effects of any type having a Severity Class (SC_i) whatever the ATM cause [8].

Overall ATM Safety Target values are taken from ESARR 4 [17] or ED-125 [19] and these values are apportioned to the different Severity Classes using ATM Operational Hazard Distribution, termed $Nmax_i$, where 'i' is the index of the Severity Class. ED-125 defines multiple ATM Operational Hazard distributions containing up to 125 Operational Hazards judged to be relevant to the ATM System (airborne and ground elements) in all situations [19].

Different distribution models are defined within ED-125 for service provision within an Air Traffic Service Units (ATSU), comprising 4 ATM OH Distribution Models applied to three operational environments; Area Control Centre (ACC) ATSU encompassing Enroute and TMA operations, Approach (APP) ATSU and Airport (AD) ATSU.

Selection of the appropriate ATSU OH Distribution Model allows the calculation of the ATM Safety Target apportioned to each Severity Classes 1 to 4 using Equation (1):

$$\text{ATM apportioned Safety Target per } SC_i = \frac{\text{Overall ATM Safety Target}_i}{\text{Nmax}_i} \quad (1)$$

where 'i' is the index of the Severity Class.
T

2.3.1.3 Safety Targets for the developed application

The ATM apportioned ST values for SC 1-4 are now modified for the ATM application in-question through comparison between the number of ATM application Operational Hazards in each SC against the overall ATM apportioned value. If the values are comparable i.e. ATM OH = 3 for SC1, application OH = 3 for SC 1, then the ATM application ST is equally divided between the assessment OH.

If the ATM application Nmax number is significantly less than the overall ATM OH number per SC then the ATM application Safety Target value is set to be equal to the overall ATM ST value [8].

2.3.1.4 Probability of Effect evaluation using Event Trees

Each OH must now have its Probability of Effect, **Pe** values assessed. A Probability of Effect gives the probability of the Operational Hazard propagating through an event tree to cause an Operational Effect of assessed Severity Class to occur [5]. An Event Tree is a graphical representation of a logic model that identifies and quantifies the possible outcomes following an initiating event, i.e. the Operational Hazard yielding an Operational Effect, as shown in Figure 5:

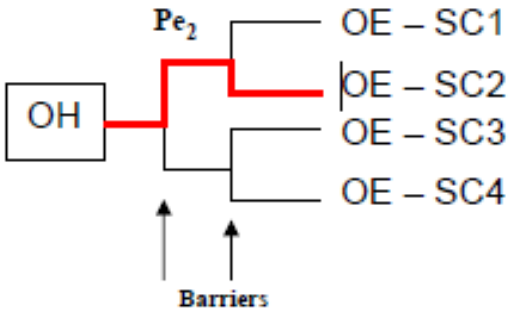

Figure 5. Event tree model for Pe

The conservative approach to determining Pe is to assume that each time the Operational Hazard occurs its Operational Effect - Severity Class will also occur. This sets Pe to a value of 1. However, this approach discounts any form of 'Mitigation Means' present within the ATM system or application preventing this one-to-one relationship between operational hazard and operational effect [19].

Mitigation Means are procedures, alerts, or other aspects that are implemented to help reduce the frequency of exposure to hazards and/or to alleviate the consequences of hazards when encountered. Two types of mitigation means are defined within the OHA process [6]:

External Mitigation Means (EMM). Fall back ATM procedures or capabilities of the ATM system, outside of the considered application. These mitigations help to reduce the impact of the OH after it has happened. All identified EMMs are defined within the application OSED if used within the assessment event trees to mitigate the effect of the identified OH's.

Internal Mitigation Means (IMM). Features internal to the considered application or systems, which act to reduce the Operational Hazards probability of occurrence. IMM's are defined to constitute application specific Safety Requirements in ED-126 for ADS-B NRA and ED-161 for ADS-B RAD.

Event tree analysis provides an inductive approach to reliability assessment as they are constructed using forward logic featuring branch levels [7]. Inductive systems analysis proposes the Operational Hazard as the starting condition and attempts to ascertain the effect of the hazard on the ATM system operation [20]. Each branch level describes either an Environmental Condition or a Mitigation Means and these are labelled as 'Barriers'. Each barrier features either binary accounting (yes, no) or probabilistic determination of the "success" or "failure" of the barriers. At the end of the branches, the effects of the OH on the ATM system are described giving the rationale behind the assigned Severity Class and the Pe value for each event tree branch [7].

Probability effect values for each branch of the event tree are calculated through the multiplication of the individual barrier probability values to give a total Pe for each SC-OE branch. The binary accounting, Yes, No branches can be defined to either have a probability associated with them e.g. ED-163 ADS-B APT OSA (Figure 6) or not e.g. ED-161 ADS-B RAD OSA (Figure 7).

Figures 6 & 7 show different approaches taken in ED-163 for APT application and ED-161 for the RAD application for the event tree compositions:

- RAD splits the event tree presentation into two halves, with the upper one describing the 'success' cases for the each operational hazard assessed for the four reference environments (e.g. 9 OE-SC pairs) and the lower one the 'failure' case for each reference scenario (e.g. 8 OE-SC pairs) [7].

- APT combined both 'success' and 'failure' into a single, more complicated tree per OH (e.g. 29 OE-SC cases) [8].

OH07: Loss of Specific ADS-B Emergency Mode after Selected by Pilot.	**BARRIER-V**: Ground radar is available and displayed to the ATCo. Note: It is assumed radar is performing correctly if available.	**BARRIER-XVII**: Ground system cross checks radar and ADS-B emergency data (i.e. Mode A code) and notifies ATCo of any inconsistency.	**BARRIER-XVIII**: Pilot able to report emergency to ATCO given that emergency does not entail a radio communication failure or unlawful interference.	**BARRIER-XIX**: ATCO able to detect the type of emergency, either due to sudden aircraft maneuvers (e.g., emergency descent) or other observable cue given Barrier V.	**BARRIER-XX**: Lack ATCo of assistance contributed to severity of the emergency.	Scenario No.	Hazard Detected?	Probability of Effect (Pe)	Severity	Severity Rationale
OH07 occurs (From Fault Tree)	RAD 1 environment used only for severity assessment; radar availability is N/A	N/A given PSR	Success [0.99]	N/A	N/A	I	Y	9.77E-01	5	Pilot informs ATCO of exact emergency. *NOTE: Scenario is equivalent to existing system today, where SSR (in a combined SSR / PSR environment) may fail to provide emergency mode.*
			Failure [0.01]	YES	N/A	II	Y	9.87E-03	3	Significant reduction in safety margin and ATC capability, given that ATCO unable to prepare for possible change in aircraft trajectory. *NOTE: Scenario is equivalent to existing system today, where SSR (in a combined SSR / PSR environment) may fail to provide emergency mode.*
				NO	YES	III	N	9.87E-03	1	Hazard not detected; possible collision or flight into terrain. Lack of ATCO assistance due to ADS-B failure contributes to severity. *NOTE: Scenario is equivalent to existing system today, where SSR (in a combined SSR / PSR environment) may fail to provide emergency mode.*
					NO	IV	N	9.87E-03	5	Severity based on ATCo's impact on the event and not the emergency itself. In this case, ATCo has no impact on the outcome of the emergency.
	RAD 2A / 2B / 3 Success [0.9999]	Success [0.99]	Success [0.99]	N/A	N/A	V	Y	9.80E-01	5	Same as scenario I
				YES	N/A	VI	Y	9.90E-03	3	Same as scenario II
			Failure [0.01]		YES	VII	N	9.90E-03	1	Same as scenario III
				NO	NO	VIII	N	9.90E-03	5	Same as scenario IV
		Failure [0.01]				IX	N	1.00E-02	1	Same as scenario III
	Ground radar unavailability scenarios									
	RAD 2A / 2B / 3 Failure [0.0001]	N/A - Barrier needs SSR	Failure [0.01]	YES	N/A	X	N	1E-06	3	Same as scenario II
	RAD 2A / 2B / 3 Failure [0.0001]	N/A - Barrier needs SSR	Failure [0.01]	NO	YES	XI	N	1E-06	1	Same as scenario III

FIGURE C-29: OH07 EVENT TREE

Figure 6. Event tree model used in ADS-B RAD application OHA

FIGURE C.17: OH03u-A EVENT TREE: NON THREAT SEEN AS A THREAT

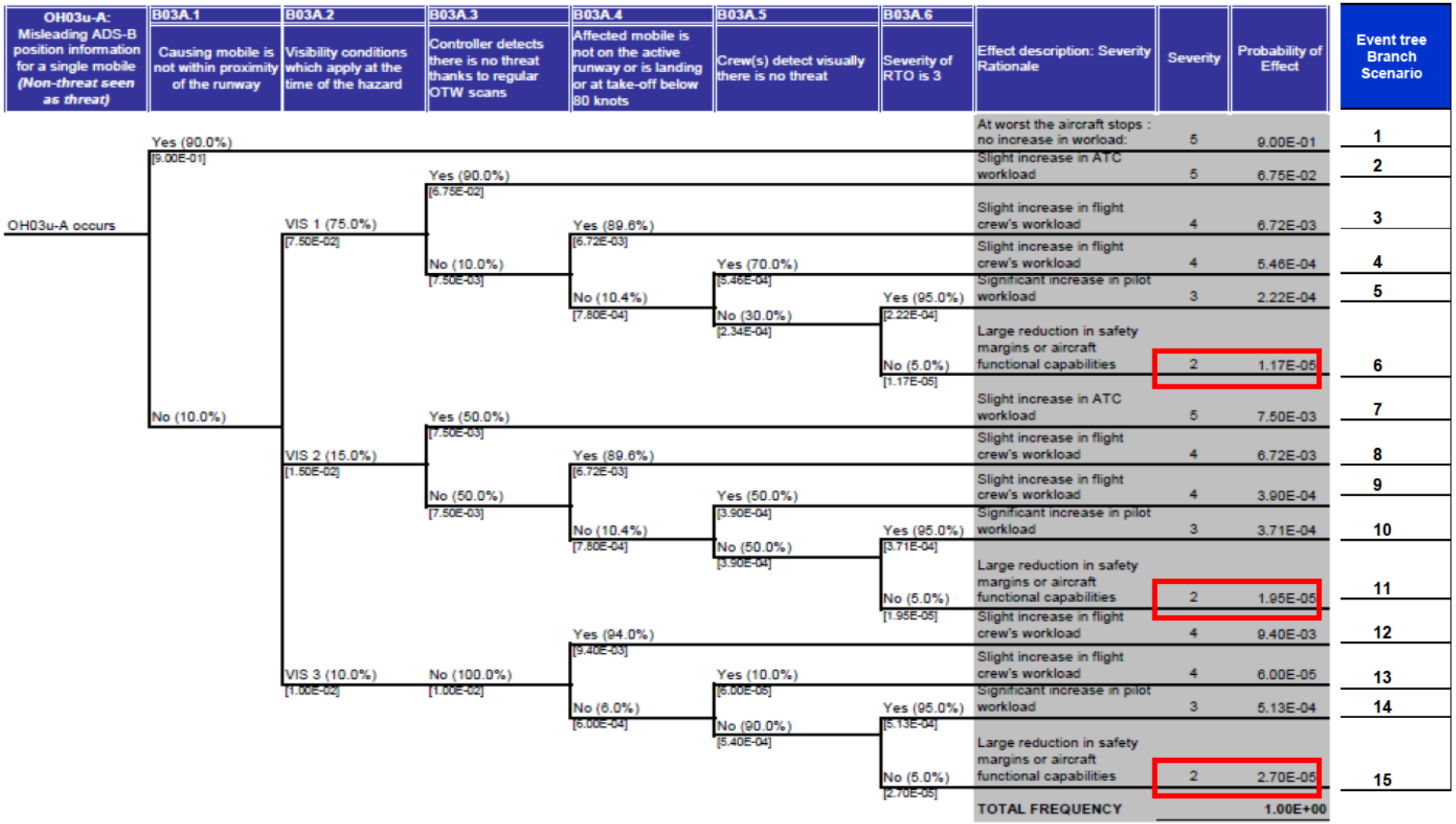

Figure 7. Event tree model used in ADS-B APT application OHA

Within the APT standard the final step of the Pe assessment is to sum all of the OH Pe values assessed per Severity Class from the different event tree branches into a common value for SC1 to SC4. For example, OH 01u Severity Class 2 Pe value in Figure 6 equals 5.82E-05, which is a summation of the SC2 branch scenario **6**, **11** and **15** highlighted in red in the figure. This common Pe value per SC was used within the determination of each OH Safety Objective within the APT OHA [8].

ADS-B RAD retained each Pe value for each event tree assessment scenario, for use in the calculation of the OH Safety Objective and did not sum them into a common value per SC.

2.3.1.5 Safety Objectives assignment

The Pe and Safety Targets are now used to derive the Safety Objective for each OH through the use of equation (2) [8]:

$$\text{Safety Objective } \mathbf{SO} = \frac{\text{ATM apportioned } \mathbf{ST} \text{ per Severity Class}}{\mathbf{Pe} \text{ per Severity Class}} \quad (2)$$

The above process generates a table of Safety Objective values against the Event Tree branch scenarios for each Operational Hazard. For example, ADS-RAD OH07 shown in Figure 7 develops 11 event tree branches and hence realises 11 SO values, as shown below [7]:

TABLE C-57: OH07 SAFETY OBJECTIVES

Scenario	Probability of Effect (Pe)	Severity	FAA SMS Safety Target	FAA SMS Safety Objective	ESARR-4 Safety Target	ESARR-4 Safety Objective
I	9.77E-01	5	N/A	N/A	N/A	N/A
II	9.87E-03	3	1.00E-05	1.01E-03	4.00E-07	4.05E-05
III	9.87E-03	1	1.00E-09	1.01E-07	5.00E-10	2.54E-08[11]
IV	9.87E-03	5	N/A	N/A	N/A	N/A
V	9.80E-01	5	N/A	N/A	N/A	N/A
VI	9.90E-03	3	1.00E-05	1.01E-03	4.00E-07	4.04E-05
VII	9.90E-05	1	1.00E-09	1.01E-07	5.00E-10	5.05E-08
VIII	9.90E-05	5	N/A	N/A	N/A	N/A
IX	1.00E-02	1	1.00E-09	**1.00E-07**	5.00E-10	5.00E-08
X	1E-06	3	1.00E-05	1.00E+01	4.00E-07	4.00E-01
XI	1E-06	1	1.00E-09	1.00E-03	5.00E-10	**2.50E-08**[12]

The most demanding safety objectives are shaded.

Table 3. ADS-B RAD OH07 Safety Objectives

In the case of ADS-B APT, the summed Pe values for the assessed Event Tree scenarios are used to calculate the SO for each Severity Class, shown for OH03u-A in Table 3 [8]:

TABLE C.33: OH03u-A DERIVATION OF SAFETY OBJECTIVES

Severity Class	$ST_{SMS\ FAA}$ [per flight hour]	$SO_{SMS\ FAA}$ [per flight hour]	ST_{ESARR4} [per flight hour]	SO_{ESARR4} [per flight hour]
1	1E-09	N/A.	3.33E-10	N/A.
2	1E-07	1.72E-03	6.67E-08	1.15E-03.
3	1E-05	9.04E-03	3.33E-07	3.01E-04
4	1E-03	4.20E-02	1.30E-05	5.45E-04

Table 4. ADS-B RAD OH07 Safety Objectives

The most demanding Safety Objective value for each Operational Hazard is then selected as the input condition for the Allocation of Safety Requirements activity, shown by the shaded boxes in the above tables.

2.3.2 Allocation of Safety Requirements

The Allocation of Safety Requirements or **ASOR** activity develops a Fault Tree for each Operational Hazard. The objective for each fault tree is to apportion Safety Requirements against functional elements of the end-to-end CNS/ATM system and domains to meet the Safety Objective for each application Operational Hazard [7] [8].

Fault trees graphically represent the interaction of failures and other events within a system. Fault tree analysis is a deductive analysis which focuses on one particular undesired event i.e. Operational Hazard and provides a method for determining causes for this event. The undesired event constitutes the top level event of the fault tree diagram [20].

2.3.2.1 Fault Tree Development

Fault trees model the Operational Hazard through combinations of Basic Causes (BC), Environment Conditions (EC) and Internal Mitigation Means (IMM) probability of occurrence values [8]:

- Basic Causes (BC) are identified by evaluating failures of the system functions within the Airborne and Ground Domains and assigning probability values to them. Basis Causes can also be defined as external failure events which can contribute to or cause the Operational Hazard or occur within the ATM application in-question.
- Environment Conditions (EC) are characteristics and elements that constitute the ATM application operating environment. The safety assessment is conducted within this assumed environment [7].
- Internal Mitigation Means (IMM) are mitigations present within the application functional model which help meet the safety objective assigned to the hazard through the reduction of it probability of occurrence. Internal Mitigation Means constitute safety requirements on the ATM functional architecture [6].

A fault tree decomposes an Operational Hazard into a set of linked failures contained within a fault tree branch which must occur for the hazard to happen. Basic Causes at the bottom of the fault tree are linked via logic symbols (known as gates) to one or more top-level event. Fault Trees illustrate how Basic Causes and their interactions can result in each hazard. Internal Mitigation Means can be incorporated within the Fault Tree to reduce the top level event to be compliant with the Safety Objective for the Operational Hazard [8]. This process is shown generically in Figure 8.

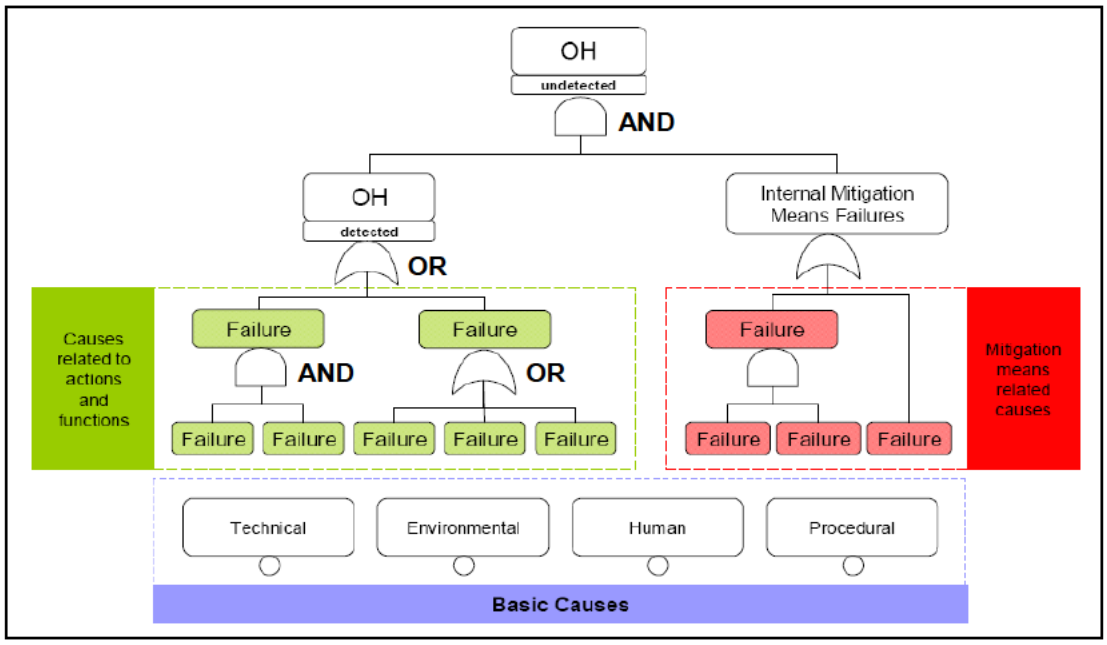

Figure 8. Generic Operational Hazard fault tree

The failure cases are represented by probability values for their occurrence and these initial probabilities are derived from OSA assumptions assessed to be relevant to the particular hazard. The top level event probability is used to determine whether the Operational Hazard Safety Objective can be met for the detected and undetected case of each OH [3].

Failure conditions within the fault tree are linked via 'AND' gates or 'OR' gates. Where a failure condition is represented by an AND relationship, the lower level input failure probabilities are multiplied together to achieve the upper level value and hence all must occur for the hazard condition to be present. Where a failure condition is represented by an OR relationship, the lower level failure probabilities are summed together to achieve the higher level failure probability. In this case, any one of the input failures can cause the hazard to occur [8].

2.3.2.2 Safety Objective Allocation

The Safety Objective Allocation step within the OSA process is performed to demonstrate that the proposed functional architecture, as captured within the fault trees, meets the safety objectives identified for each hazard [7].

Each OH has a likelihood of occurrence probability captured within the top level of the fault tree, linked through the branches of the fault tree to the failure rates of the identified Basic Events and Internal Mitigation Means. This likelihood of occurrence probability is compared against the Operational Hazard Safety Objectives input from the OHA and if it is lower than the most stringent Safety Objective then the ATM application functional architecture is declared to have met the Operational Hazard safety objective [8].

If the likelihood value is greater than any of the safety objectives then additional fault tree mitigation means (IMM) or event tree barriers (EMM) may need to be identified to mitigate the hazard to a tolerably safe level. These additional mitigation means would need to be incorporated within the event and fault trees and hence would increase the number of Safety Requirements against the aircraft or ground functional model elements [7].

The first list of Safety Requirements is developed to capture the expected performance of the IMM incorporated within the OSA fault trees.

2.3.2.3 Safety Requirements Derivation

The final step of the OSA process is to derive Safety Requirements through examination of each Basic Cause, in combination with the relevant OSA assumptions. This set are combined with the IMM SR list from the Safety Objective Allocation step to yield the full set of Safety Requirements for the ATM application under consideration [8].

3 ADS-B NRA ATM Application

ADS-B Non-Radar Airspace ATM application is defined within the 'Safety Performance and Interoperability Requirements Document for the NRA Application', ED-126 [6]. 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) [6].

3.1 ADS-B NRA SPR Logical Model

The ADS-B Non Radar Airspace application is, by definition, applicable to operational environments which currently do not feature surveillance information. The generic ADS-B functional model is modified within the SPR section through the removal of SSR information exchange between the Transmit Aircraft Domain and Ground Domain and the Airborne Receive Domain, which is not relevant to a ground surveillance application [6].

Therefore, the ADS-B NRA logical functional model becomes that shown Figure 9 [6]:

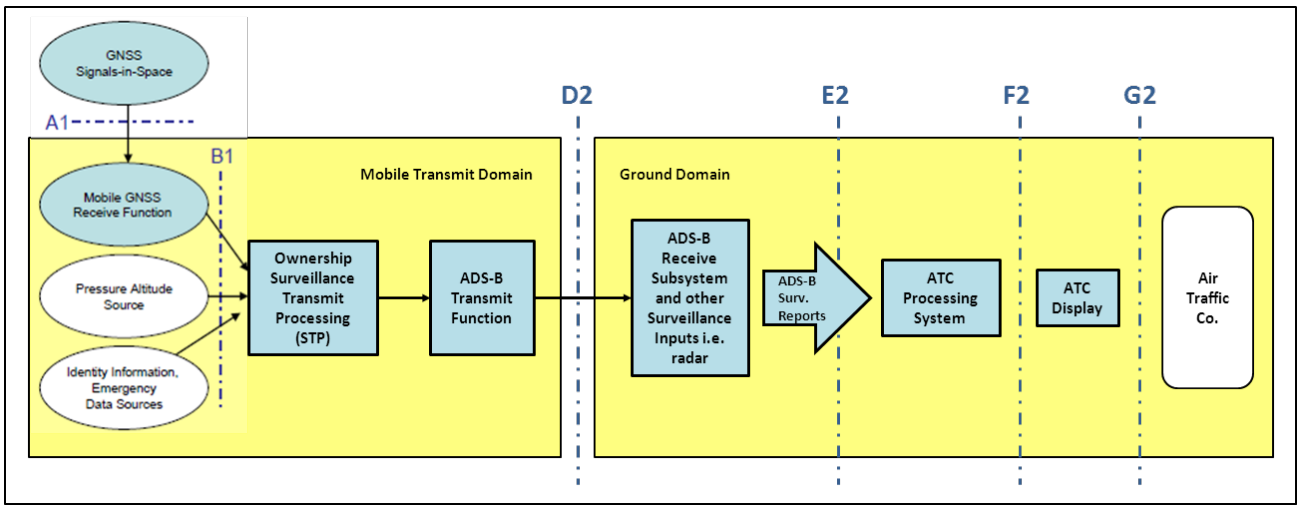

Figure 9. ADS-B NRA Logical Functional Model

The Ground Domain consists of interconnected ADS-B Receive functions, ATC Processing System and ATC Display functions between Interfaces D2 and G2. ADS-B OSED states that the NRA application is only assessed to the interface E2, with the assumption that the ATC processing and display system beyond this interface is unchanged by the source of surveillance data [6].

3.2 ADS-B NRA OSED

The ADS-B-NRA application is designed to support and enhance Air Traffic Services in both En-route and TMA airspaces in non-radar areas (NRA) The introduction of NRA will augment existing air-traffic services by providing 5 NM and 3 NM ATC separation services in areas where it does not exist today, or in areas where procedural separation is applied [6].

ADS-B NRA Operational Services and Environment Description (OSED) defines the following operational conditions [6]:

Performance and safety assessment activities undertaken within ADS-B NRA were restricted to the ADS-B Receive sub-system and delivery of ADS-B surveillance reports, up to interface E2.

ATC processing and procedures are assumed within ED-126 to be independent of the source of surveillance data.

100% of aircraft are under ADS-B Surveillance i.e. all equipped with ADS-B enabled Mode S transponders/transmitters

Only ADS-B enabled traffic is displayed to ATC Controllers

ATC separation tasks are the most demanding ATM application and hence requirements derived to support this task will be sufficient to support other ATM uses of the ADS-B surveillance data i.e. ATC advisory, traffic and flight information services

Enroute traffic are separated by 5NM, corresponding to low to medium density environments

TMA traffic are separated by 3NM, again corresponding to low – medium density operations

Reference radar system is a single layer of SSR in Enroute and TMA environments

Maximum instantaneous count of traffic = 15 aircraft for En-route ATC sector and 7 aircraft for TMA ATC sector at any one time

Number of aircraft managed per Air Traffic Service Unit (ATSU) hour are 30 per En-route ATC sector and 10 TMA ATC sector.

Average duration of a flight within a single ATC sector: 20 minutes for En-route and 6 minutes for TMA

To normalise Enroute and TMA operations, the following ‘flight hr’ to ‘ATC Unit (ATCU) hour’ conversion factors were used to derive Safety Targets and Requirements:

- Enroute ATC Sector = 30 aircraft x 20 min flight duration/ 60 min = 10 fl hrs to 1 ATSU hr
- TMA ATC Sector = 10 aircraft x 6 min flight duration / 60 min = 1 fl hr to 1 ATSU hr

3.3 ADS-B NRA OSA

3.3.1 NRA Operational Hazards

Operational Hazards defined with the ADS-B NRA application are given in Table 5 [6]:

Operational Hazard	Operational Hazard	OSA analysis
OH1	Sudden and unexpected loss of position information for a single aircraft previously identified in the sector.	Yes
OH2	Sudden and unexpected loss of position information for multiple aircraft previously identified in the sector.	Yes
OH3	Incorrect position information for multiple aircraft in a wide area is displayed on the CWP (3 error scenarios developed for both detected and undetected case)	Yes
OH4	Incorrect position information for one aircraft is displayed on the CWP (3 error scenarios have been developed for both detected and undetected cases)	Yes
OH5	Unexpected oscillating Quality Indicator (QI) value	OH1 + OH2
OH6	Loss of or incorrect identification (Mode A code and SPI)	Not assessed
OH7	Loss of or incorrect altitude for a single aircraft	Not assessed
OH8	Loss of or incorrect emergency modes	Not assessed
OH9	Loss of or incorrect identification (Aircraft Id. And 24 bit address)	Not assessed

Table 5. ADS-B NRA Operational Hazards

It is stated within ED-126 that only OH1 to OH5 where assessed to be specific to ADS-B NRA application and these were fully developed within the NRA Operational Safety Assessment (OSA). OH5 was deemed to be combination of OH1 and OH2 and hence covered under the conducted OSA analysis for OH1-OH4. The severity class of each Operational Hazard case was assessed for its operational impact to ATCO within the NRA OSA and from the 'worst credible effect' perspective [6].

Operational Hazards OH1 was assessed for a 'detected' and 'undetected' case of the hazard occurrence. OH2 which only considered the detected case, as the undetected loss of multiple aircraft on the ATC display was deemed to not be a credible failure mechanism. OH3 had three different scenarios modelled for the detected and undetected conditions, as did OH4. This therefore yielded a total of 15 identified Operational Hazards cases within the NRA OSA (see Table 7) [6].

OH6 to OH9 were deemed to be equivalent to operational hazards present in the current radar environment. Through this equivalence of Altitude and Identification data items, they were declared as out of scope for the OSA activity and not assessed. Only ADS-B position information characteristics were assessed within the ADS-B NRA ED-126 OSA [6].

3.3.2 NRA Safety Objectives

ADS-N NRA Operational Hazards are categorised into ATM Hazard Severity Classes, as described within the 1st Iteration Safety Report [5]. Severity Classes 1-4 are defined, with 1 being the most severe in terms of effects to the ATM operation and aircraft in-question and 4 the least. This sub-division of severity class enables the assignment of different ATM Safety Target values to each Severity Class, with the chosen value commensurate to the impact of hazard condition on occurrence [6].

3.3.2.1 ATM Safety Targets for NRA

Overall ATM Safety Targets (ST) for Severity Classes 1–4 were initially defined within the EUROCONTROL Safety Regulatory Requirement 4 or ESSAR 4 document [17]. Inspection of ESSAR 4 reveals that only SC1 had a defined ATM ST value (1.55e-8), with no values for defined SC 2-4 ATM Safety Targets. ED-126 proposed a full set of overall ATM Safety Targets for the NRA application, as shown in Table 6:

	Ambition Factor	ATM ST (per flight hr)	Enroute Overall ATM Safety Targets (per ATSU hr)	TMA Overall ATM Safety Targets (per ATSU hr)
Severity Class 1	1.55	1E-08	1E-07	1E-08
Severity Class 2	1	1E-05	1E-04	1E-05
Severity Class 3	1	1E-04	1E-03	1E-04
Severity Class 4	1	1E-02	1E-01	1E-02

Table 6. ATM Safety Targets and Operational Hazard distribution specified in ADS-B NRA OSA

The ADS-B NRA surveillance application set the ATM Ambition Factor to 1.55 or 1, so that it was the equivalent of the existing radar surveillance environment [6]. Overall ATM Safety Targets in flight hours were further modified to yield Enroute and TMA ST values in ATS Unit or ATSU hrs using the conversion factors calculated in Section 3.2, as shown in Table 6.

3.3.2.2 NRA Safety Targets

Overall ATM Safety Targets for Severity Class 1 -4 now must be apportioned to NRA application through the Overall ATM OH Nmax distribution and values shown in Table 7 [6]:

	Overall ATM Nmax OH Dist.	NRA Nmax OH Dist.	NRA ATM ST - Enroute (per ATSU hr)	NRA ATM ST - TMA (per ATSU hr)
Severity Class 1	20	7	5E-09	5E-10
Severity Class 2	25	0	4E-06	4E-07
Severity Class 3	35	4	2.86E-05	2.86E-06
Severity Class 4	45	4	2.2E-03	2.22E-04
Total	125	15		

Table 7. NRA ATM Safety Targets and Operational Hazard distribution

Overall ATM Safety Target values for Enroute and TMA listed in Table 6 were modified into NRA application Safety Targets through the use of Equation (1), to give the values shown in Table 7. Nmax values from the Overall ATM OH distribution were used in this modification, as the total number of NRA application Nmax OH distribution for SC 1-4 were significant less than the Overall ATM distribution values and hence did not take all of the ATM budget for each Severity Class risk [6].

Comparison of the Overall ATM Operational Hazard distributions used within the ADS-B NRA OSA and those used within the RAD OSA activity shows significant differences in the values for SC 1 to 4 [6], [7]. Inspection of ED-125 [19] reveals that whilst RAD OH distribution conforms to Model 3 of the defined ED-125 Safety Objective Models [7], no matching ED-125 model can be found for the NRA Overall ATM OH distribution shown in Table 7. A similar observation was made when comparing the ADS-B APT ED-125 model compared to the one used within the NRA assessment.

Therefore, it is proposed that significant care should be exercised when comparing Safety Requirements extracted from the ADS-B NRA OSA compared to either RAD or APT documents for ground based ATM surveillance applications.

3.3.2.3 NRA Probability of Effect values

Probability of Effect, Pe, values for the detected 15 OH cases ranged between 0.1 to 1. For the undetected cases the value ranged between 1e-07 to 0.1, a wide range of variation. These values were stated within the NRA SPR document, without the corresponding event trees. This approach is in contrast to that used within the ADS-B RAD and ADS-B APT documents which developed event trees for all assessed Operational Hazards.

3.3.2.4 NRA Safety Objectives

NRA application Safety Targets and Pe values are now combined to generate Safety Objectives for the NRA Operational Hazard set. These are reproduced in Table 8 from ED-126:

d = detected u = undetected

OH	Airspace	Severity	Pe	Safety Objective (per ATSU hr)
OH1d	Enroute	**4**	0.5	**4.44E-03**
	TMA			**4.44E-04**
OH1u	Enroute	**1**	0.1	**5E-08**
	TMA			**5E-09**
OH2d	Enroute	**3**	0.1	**2.86E-04**
	TMA			**2.85E-05**
OH03d Cases 1 & 3	Enroute	**3**	1	**2.86E-05**
	TMA			**2.86E-06**
OH03d Case2	Enroute	**3**	0.1	**2.86E-04**
	TMA			**2.85E-05**
OH03u Case 1	Enroute	**1**	1E-07	***5E-02***
	TMA			***5E-03***
OH03u Case 2 & 3	Enroute	**1**	5E-03	**1E-06**
	TMA			**1E-07**
OH04d Cases 1 – 3	Enroute	**4**	1	**2.22E-03**
	TMA			**2.22E-04**
OH04u Case 1	Enroute	**1**	1E-07	***5E-02***
	TMA			***5E-03***
OH4u Cases 2 &3	Enroute	**1**	5E-03	**1E-06**
	TMA			**1E-07**

Table 8. NRA Safety Objective for OH1 – OH4 set

3.3.3 NRA OH Safety Requirements

Safety Objective associated against detected and undetected OH's were then input into fault trees. This generated the following Safety Requirements applicable to the ADS-B ground receive and ATC processing and display functions within the ADS-B NRA application ASOR process [6]:

OH	SR#	Safety Requirement	SPR Type	SPR#
OH1d & OH1u	SR3	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.	C	13
	SR4	The likelihood that the ADS-B Receive sub-system 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.	L	15
OH1u	SR5	The likelihood that ATC processing system does not notify the Controller of the loss of a track (e.g. through coasting) should be no more than **1E-05** per ATSU-hour	L	28
OH2d	SR6	The likelihood that ADS-B Receive sub-system does not provide updated ADS-B surveillance reports for more than one aircraft from which ADS-B messages are being received shall be no more than **5E-6** per ATSU hour	L	14
	SR7	The likelihood that ATC automation and display subsystem lose all information for more than one aircraft, should be no more than **5E-06** per ATSU-hour	L	28
	SR8	The likelihood that the ADS-B Receive sub-system corrupts ADS-B position information or associated quality indicator for more than one track shall be no more than **5E-06** per ATSU-hour.	C	13
	SR9	The likelihood that ATC automation and display subsystem corrupts ADS-B quality indicator or position for more than one aircraft should be no more than **5E-06** per ATSU-hour	C	29
OH3u & OH03u	SR12	The likelihood that ATC Processing and Display subsystem corrupts position information (multiple aircraft) should be no more than **5E-06** per ATSU hour	C	29
	SR13	The likelihood that the Ground Domain displays 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	C	13
	SR15	The likelihood that the Ground Domains displays incorrect information or no 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	C	13
	SR16	The likelihood that the ATC processing and display subsystem corrupts quality indicators for aircraft shall be no more than **5E-06** per ATSU hour	C	29
OH4d & OH04u	SR17	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	C	29

OH	SR#	Safety Requirement	SPR Type	SPR#
	SR18	The likelihood that Ground Domain displays 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	**C**	**13**

Table 9. Safety Requirements applicable to the ADS-B ground system for ADS-B NRA

NOTE 1: L = Loss C=Corruption

3.3.4 ADS-B NRA Safety and Performance Requirements

The above safety requirements applicable to the ADS-B Receive sub-system i.e. up to interface E2 within the ADS-B NRA logical model, were condensed into the NRA Safety Performance Requirements set, **SPR13 - SPR15** shown in black within Table 9 and incorporated into Table 10:

SPR#	Safety and Performance Requirement	SPR type
SPR13	The likelihood that the ADS-B receive subsystem corrupts ADS-B information through the reception, processing or delivery of data (E2) shall be no more than **5E-06** per ATSU hour	**Corruption**
SPR14	The likelihood that ADS-B receive subsystem does not provide updated 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	**Loss**
SPR15	The likelihood that the 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	**Loss**

Table 10. ADS-B NRA ADS-B receive function SPR set

However, the same process is not followed for the Safety Requirements related to the ADS-B processing and display system function, resident between interface E2 to interface G2 in the ADS-B NRA functional model. This reason stated in ED-126 for this omission was because the ATC system and procedures employed after Interface E2 were assessed not to change as a result of the NRA application [6].

4 ADS-B RAD ATM Application

ADS-B RAD ATM application is defined within the 'Safety Performance and Interoperability Requirements Document for the ADS-B RAD Application', ED-161 [7]. 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 Radar-Controlled Areas using ADS-B surveillance" (ADS-B-RAD) [7].

The ADS-B RAD application is designed to enable the integration of ADS-B surveillance into operational environments which feature radar control information i.e. ICAO Airspace Classes A-D. The RAD application is designed to support the following ICAO Air Traffic Services:

Air Traffic Control Service

- Area Control Service
- Approach Control Service

Flight Information Service (FIS)

Alerting Service

Air Traffic Advisory Service

The ADS-B RAD application was described in detail within 1st Prototype Iteration Safety Report [5].

4.1 ADS-B RAD SPR Logical Model

ADS-B RAD is a ground based surveillance ADS-B out application and hence is concerned with the transmission of ADS-B information from the Transmit Aircraft Domain and reception of the ADS-B information within the Ground Domain. It does not feature Receive Aircraft Domain, thereby modifying the generic ADS-B functional model in the manner shown in Figure 10 within the SPR section [5], [7]:

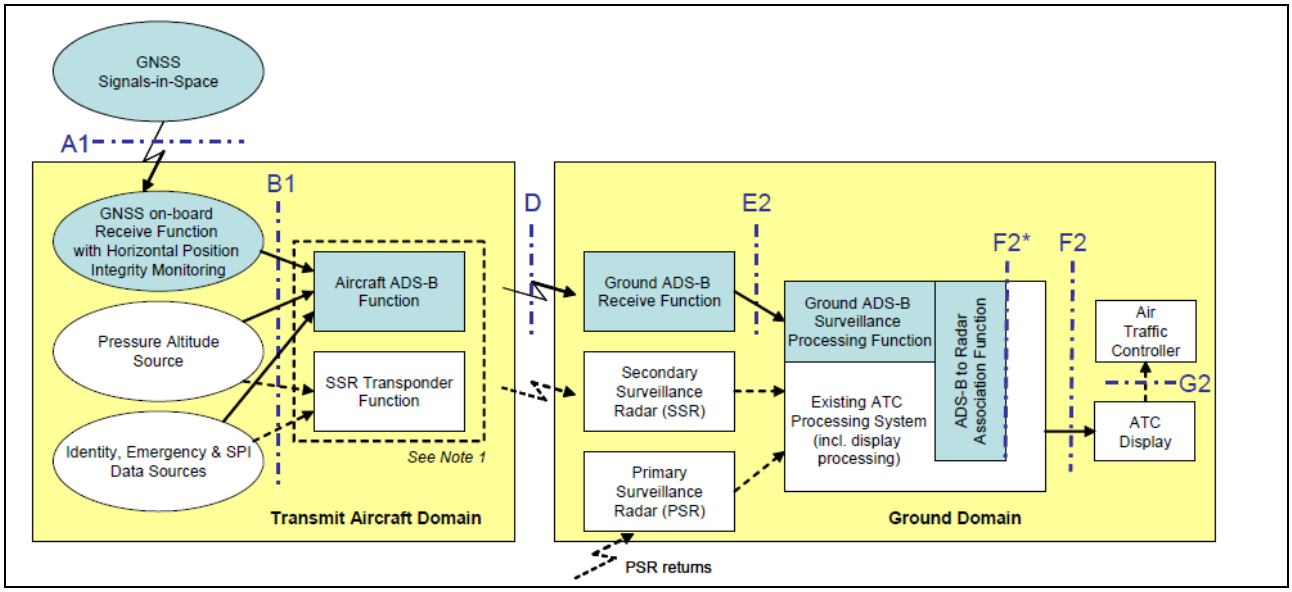

Figure 10. ADS-B RAD Functional Model

The ADS-B Ground Domain consists of interconnected 'ADS-B Ground Receive' function, 'ADS-B Surveillance Processing' function and 'ADS-B to Radar Association' function, located between Interfaces D and F2* [7].

4.2 ADS-B RAD OSED

The ADS-B-RAD application is designed to act as a single layer of surveillance providing ATC services, with radar providing the backup layer of surveillance to mitigate ADS-B failures. It is designed to operate in medium to high density HD operating environments and is analogues with the combination of PSR and SSR in existing HD, TMA and Enroute environments [7].

ADS-B RAD Operational Services and Environment Description defines the following [7]:

ATC Control task through the provision of aircraft separation was deemed the most demanding task and hence ADS-B requirements which assure this task will satisfy all other uses of ADS-B data i.e. FIS, Alerting and Advisory. This is the same requirement as for the ADS-B NRA application.

100% of aircraft present in RAD airspace are equipped with a ADS-B transmitter and SSR/Mode S radar transponder

Altitude and identification information present within the SSR and ADS-B messages are from the same source, as shown by the functional cross-coupling in Figure 5 for ADS-B and SSR Transponder functions

Four reference scenarios are defined, featuring Primary Surveillance Radar and Secondary/Mode S Radar in either single or dual layer of radar configuration for medium or high density operating environments

The Primary Surveillance Radar has an availability of 99.7% or 9.97E-01

The Secondary/Mode S radar has an availability of 99.9% or 9.99E-01

The radar is operating in a no-fault configuration

A sustained difference between ADS-B reported aircraft position and radar measured position for the same aircraft will be indicated to the ATC controller through appropriate display track symbols

Multi-sensor tracking is excluded from analysis. Only ADS-B to radar report association is covered in the RAD assessment.

Traffic shall be separated by 5NM in Enroute airspace, 3NM in TMA, 2.5NM for approach and 2NM for dependant parallel approach.

4 Reference radar environments are defined in the RAD SPR OSED, featuring combinations single layer combinations of SSR + ADS-B, Mode S + ADS-B, PSR+ADS-B

Maximum instantaneous count of traffic;

- Enroute = 20 aircraft in High Density ATC sector.
- TMA = 15 aircraft in Medium Density and High Density ATC sector

Flight hour to ATS Unit hour is set to the same value for all ATC operating environments:

- Fl hr to ATSU conversion factor = 6 flight hr /ATSU hr

4.3 ADS-B RAD OSA

4.3.1 RAD Operational Hazards

Operational Hazards defined with the ADS-B RAD application are given in Table 11 [7]:

Case	Hazard Id	Hazard Description: Single Aircraft event	L/C
1	**OH01**	Sudden and Unexpected Loss of ADS-B Position Information for a *Single* Aircraft	**L**
2	**OH03**	Loss of all ADS-B Data for a *Single* Aircraft	**L**
	OH05	Incorrect Position Information for a *Single* Aircraft –three Test Cases:	
3	***OH05 Case 1***	*Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring for a Single Aircraft*	**C**
4	***OH05 Case 2***	*Horizontal position error resulting from a sustained credible corruption of the position information for a* Single *Aircraft*	**C**
5	***OH05 Case 3***	*Horizontal position error resulting from a sustained credible corruption of the quality indicator for a* Single *Aircraft*	**C**
6	**OH07**	Loss of Emergency Mode after Selected by Flight Crew	**L**
7	**OH08**	Incorrect but Plausible Emergency Mode	**C**

Case	Hazard Id	Hazard Description: Multiple Aircraft event	L/C
14	**OH02**	Sudden and Unexpected Loss of ADS-B Position Information for *Multiple* Aircraft	**L**
15	**OH04**	Loss of All ADS-B Data for *Multiple* Aircraft	**L**
	OH06	Incorrect Position Information for *Multiple* Aircraft – three Test Cases:	
16	***OH06 Case 1***	*Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring for Multiple Aircraft*	**C**
17	***OH06 Case 2***	*Horizontal position error resulting from a sustained credible corruption of the position information for* Multiple *Aircraft*	**C**
18	***OH06 Case 3***	*Horizontal position error resulting from a sustained credible corruption of the quality indicator for* Multiple *Aircraft*	**C**

Case	Hazard Id	Hazard Description: Single Aircraft event	L/C
8	**OH09**	Two 'dispersed' Position Symbols for the *Same* Aircraft	**C**
9	**OH11**	Incorrect Level Information for a *Single* Aircraft	**C**
10	**OH13**	Loss of Level Information for *Single* Aircraft	**L**
11	**OH15**	Incorrect Identity data for a *Single* Aircraft	**C**
12	**OH17**	Loss of Identity data for a *Single* Aircraft	**L**
13	**OH19**	*Single* False Target	**C**

Case	Hazard Id	Hazard Description: Multiple Aircraft event	L/C
19	**OH10**	*Multiple* 'Dispersed' Position Symbols	**C**
20	**OH12**	Incorrect Level Information for Multiple Aircraft	**C**
21	**OH14**	Loss of Level Information for *Multiple* Aircraft	**L**
	OH16	Incorrect Identity data for *Multiple* Aircraft – divided into two sub cases:	
22	***OH16 Case 1***	*Incorrect ID resulting from a sustained credible corruption of ID for* Multiple *Aircraft*	**C**
23	***OH16 Case 2***	*Transposition of IDs between at least two aircraft (swap ID)*	**C**
24	**OH18**	Loss of Identity data for *Multiple* Aircraft	**L**
25	**OH20**	*Multiple* False Targets	**C**

Table 11. ADS-B RAD Operational Hazard list

NOTE 1: L = Loss C = Corruption

25 Operational Hazard cases were defined within the RAD OHA. The RAD OSA assessed the 'Worst Credible Effect' for the OH List and therefore did not present Safety Objectives for the detected and undetected cases, as for the NRA assessment. Only a single SO per OH was presented within the RAD OHA [7].

4.3.2 RAD Safety Objectives

4.3.2.1 RAD Overall ATM System Safety Targets

ADS-N RAD Operational Hazards are categorised into ATM Hazard Severity Classes, as described within the 1st Iteration Safety Report [5] and ED-161 [7]. Severity Classes 1 to 4 are defined, with 1 the most severe in terms of effects to the ATM operation and aircraft in-question and 4 the least. This sub-division of ATM Hazard severity class enables the assignment of ATM Safety Targets to different classes, as defined in ED-125 and reproduced in ED-161 [7].

In contrast to the conservative 'like-for-like' approach adopted for ADS-B NRA, the Ambition Factor (AF) for the ADS-B RAD surveillance application was set at 10, an order of magnitude more stringentthan operations conducted using a radar surveillance only [7]. This is the same value as the ED-125 Ambition Factor recommendation based on SES objectives and EUROCAE WG64 guidelines [13].

Inserting an AF of 10 into the Overall ATM Safety Target values extracted from Table 6 and using the fl hour to ATSU conversion factor of 6 fl hr to 1 ATSU gives:

SC	Overall ATM ST (per flight hr)	Ambition Factor	Overall ATM ST (per flight hr)	Overall ATM ST (per ATSU hr)
Severity Class 1	**1e-08**	**10**	**1e-09**	**6e-09**
Severity Class 2	**1e-05**	**10**	**1e-06**	**6e-06**
Severity Class 3	**1e-04**	**10**	**1e-05**	**6e-05**
Severity Class 4	**1e-02**	**10**	**1e-03**	**6e-03**

Table 12. Overall ATM Safety Targets in ADS-B RAD OSA

The overall ATM Safety Targets given in Table 12 are applicable to the whole ATM system rather than one element i.e. ADS-B RAD application [7]. To enable the calculation of Safety Target for the ADS-B RAD application, an apportionment exercise is required and this is achieved through the appropriate selection of an ATM Operational Hazard distribution model defined in ED-125.

4.3.2.2 RAD application Overall Safety Targets

ED-161 defines ED-125 Model 3 as a suitable ATM Hazard model for modification of the Overall ATM Safety Target values to those applicable to the RAD application [7]. Dividing the Overall ATM ST by the total number of OH per SC from the ED-125 Model 3 yields the RAD application Safety Targets given in Table 13:

SC	Overall ATM ST (per flight hr)	Overall ATM Nmax OH Dist.	RAD application Overall Safety Targets (per flight hr)
Severity Class 1	1e-09	**2**	**5.0E-10**
Severity Class 2	1e-06	**25**	**4.0E-08**
Severity Class 3	1e-05	**25**	**4.0E-07**
Severity Class 4	1e-03	**73**	**1.40E-05**

Table 13. ADS-B RAD Safety Targets and Operational Hazard distribution

4.3.2.3 RAD Apportioned OH Safety Targets and Safety Objectives

The RAD OHA event trees classed RAD OH cases into the SC values shown for each assessed OH in Table 16 and summarised into Table 15 for Severity Classes 1 to 4. Only 22 out of the total of 25 OH cases were specified, as three of the assessed RAD OH were defined at SC5 and hence these had no effect on the ATM operation (Section 2.3.1.1)

SC	Overall RAD ST (per flight hr)	Overall ATM Nmax OH Dist.	RAD Nmax OH Dist.
Severity Class 1	**5.0e-10**	**2**	**2**
Severity Class 2	**4.0e-08**	**25**	**5**
Severity Class 3	**4.0e-07**	**25**	**7**
Severity Class 4	**4.0e-05**	**73**	**7**
	Total	**125**	**22**

Table 14. ADS-B RAD Safety Targets and Operational Hazard distribution

NOTE 1: SC3 Nmax in RAD is given as 7, but there are 8 assessed OH cases of SC3 in Table 16. Likewise for SC4, wHere RAD SC4 = 7 whilst there are 6 assessed OH cases of SC4 in Table 16.

Inspection of the Table 14 shows that the total number RAD OH for Severity Class 2 to 4 were significantly less than the total ATM Nmax value and hence these Safety Targets were not modified when calculating each OH Safety Objective. This situation was not the same for Severity Class 1, as the 2 values are the same and hence it is noted in the RAD OHA that SC1 Safety Objectives were adjusted to account for this [7].

Pe values for each RAD OH case failure scenario were assessed using event trees within the RAD OHA and these values were combined with the RAD application Safety Targets to generate a set of Safety Objectives for each RAD OH. The most stringent value of SO for each OH was then defined as the input condition in the fault tree analysis conducted in the ASOR process.

4.3.3 RAD Safety Requirements

Two sources of RAD Safety Requirements were noted from the ED-161 OSA; barrier requirements from the Event Trees used to derive the RAD OH Safety Objectives and fault tree gates/top level events used for RAD Safety Requirements. This is in-contrast to ADS-B NRA and ADS-B APT, which only defined fault tree gates as Safety Requirements, as per the generic OSA process described in Section 2.3.2.

Ground domain Safety Requirements defined within the ADS-B RAD OSA are listed in Table 15, complete with the source of the SR i.e. event tree barrier or fault tree failure gate [7]:

OH	SR#	Safety Requirement	Barrier (B) /Gate (G)
OH1, OH2, OH15, OH16	**02**	The probability that the ground system detects and notifies the ATCO of duplicate ADS-B IDs (i.e., discrete Mode A or aircraft ID) within the same sector **shall** be at least 99%	**B**
OH1, OH3	**05**	The probability that the ADS-B Ground Domain detects a loss of ADS-B position and provides an indication of such to the existing ATC Processing System **shall** be at least 99.99% (system integrity)	**B**
OH1, OH2 **OH3, OH4** **OH5-TC2, OH5-TC3** **OH6-TC2, OH6-TC3,** **OH7, OH8** **OH9, OH10** **OH11, OH12** **OH13, OH14** **OH15, OH16** **OH17, OH18**	**07**	The likelihood of a ground system integrity failure **shall** be 2.0E-05 or less per ATSU hour This SR is derived from the Fault Tree gate GND SYS INTG: POS LOSS, which has a value or 3.4E-06 per flight hour or 2E-05 per ATSU hr, using the flight hr to ATSU hr conversion factor of 6.	**G**
OH4,	**09**	The likelihood of a ground ADS-B receive function system continuity failure **shall** be 1E-05 or less per hour This SR is derived from the Basic Event GND RCV CONT: ADSB LOSS ALL AC, which has a value or 1.7E-06 per flight hour or 1E-05 per ATSU hr, using the flight hr to ATSU hr conversion factor of 6.	**G**
OH5-TC1, OH5-TC2, OH5–TC3 **OH6-TC1, OH6-TC2, OH6-TC3**	**10**	The probability that the ground system ADS-B to radar association function detects a large ADS-B position error **shall** be at least 99%, where a large error is at least 0.4*applicable separation minimum but less than 10 NM	**B**

OH	SR#	Safety Requirement	Barrier (B) /Gate (G)
OH5-TC1, OH5-TC2, OH5–TC3 **OH6-TC1, OH6-TC2, OH6-TC3**	**11**	The probability that the ground system ADS-B to radar association function detects a significant ADS-B position error **shall** be at least 90%, where a significant error is at least equal to the NIC boundary but less than 0.4*applicable separation minimum	**B**
OH11, OH12	**12**	The probability that the ground system detects and indicates to the ATCO an inconsistency between radar and ADS-B pressure altitude **shall** be at least 99%	**B**
OH8	**13**	The probability that the ground system detects and notifies the ATCO of an inconsistency between ADS-B- and radar-reported emergency modes **shall** be at least 99%	**B**
OH13, OH14	**14**	The probability that the ground system detects a loss of ADS-B reported altitude and displays the corresponding SSR altitude (if available) **shall** be at least 99%	**B**
OH15, OH16	**15**	The probability that the ground system detects and notifies the ATCO of an inconsistency between radar and ADS-B ID data (i.e., Mode A or Aircraft ID) **shall** be at least 99%	**B**

Table 15. Operational Hazard to Safety Requirement mapping in ADS-B RAD ASOR

OH19 and OH20 have no ground based Safety Requirements associated with them. All other RAD Operational Hazards are associated with at least one Safety Requirement.

4.3.4 ADS-B RAD Safety and Performance Requirements

In the same manner as for the used within the NRA SPR and APT Safety and Performance Requirements summary, the Safety Requirements defined with ASOR process fault trees are listed within Table 16 for the ADS-B RAD application ground domain functions [7]:

SPR#	Safety and Performance Requirement	SR
SPR33	The likelihood of an ADS-B Ground Domain system integrity failure shall be **2E-05** or less per ATSU hour	**07**
SPR34	The likelihood of a “Ground ADS-B Receive” function continuity failure shall be **1E-05** or less per ATSU hour	**09**

Table 16. Ground Domain SPR set for ADS-B RAD application

5 ADS-B APT ATM Application

ADS-B APT ATM application is defined within the 'Safety Performance and Interoperability Requirements Document for the ADS-B Airport Surface Surveillance Application (ADS-B-APT)', ED-163. This standard provides the minimum end-to-end operational, safety and performance requirements (SPR) and interoperability requirements (INTEROP) the ADS-B APT application [8].

The ADS-B RAD application is designed to enhance aerodrome operations by adding ADS-B surveillance into aerodromes which presently do not feature surveillance systems. The ADS-B surveillance information is displayed to ATC controller through an appropriate display i.e. CWP. The availability of surveillance data is aimed to both augment airport ATC controller situational awareness e.g. detection of runway incursions and enable the more efficient management of surface traffic e.g. higher throughput of aircraft in poor Visibility Conditions.

The reference environment for ADS-B APT is defined as an airdrome environment featuring a Surface Movement Radar (SMR), as this acts to augment Aerodrome Procedures and not operated in a standalone manner, as for an A-SMGCS system. The addition of identification information from ADS-B is a significant advantage of the ADS-B APT application compared to the non-cooperative SMR operations.

Target Environments for the ADS-B APT application are simple to complex aerodrome layouts, featuring multiple runways but limited to two active runways at any point in time. ADS-B provides the unique means of surveillance.

5.1 ADS-B APT SPR Logical Model

ADS-B APT is a ground based surveillance ADS-B out application and hence is concerned with the transmission of ADS-B information from the Transmit Aircraft Domain and reception of the ADS-B information within the Ground Domain. It does not feature Receive Aircraft Domain, thereby modifying the generic ADS-B Functional Model shown in Figure 4 to that given in Figure 7 within the SPR section [5] [8]:

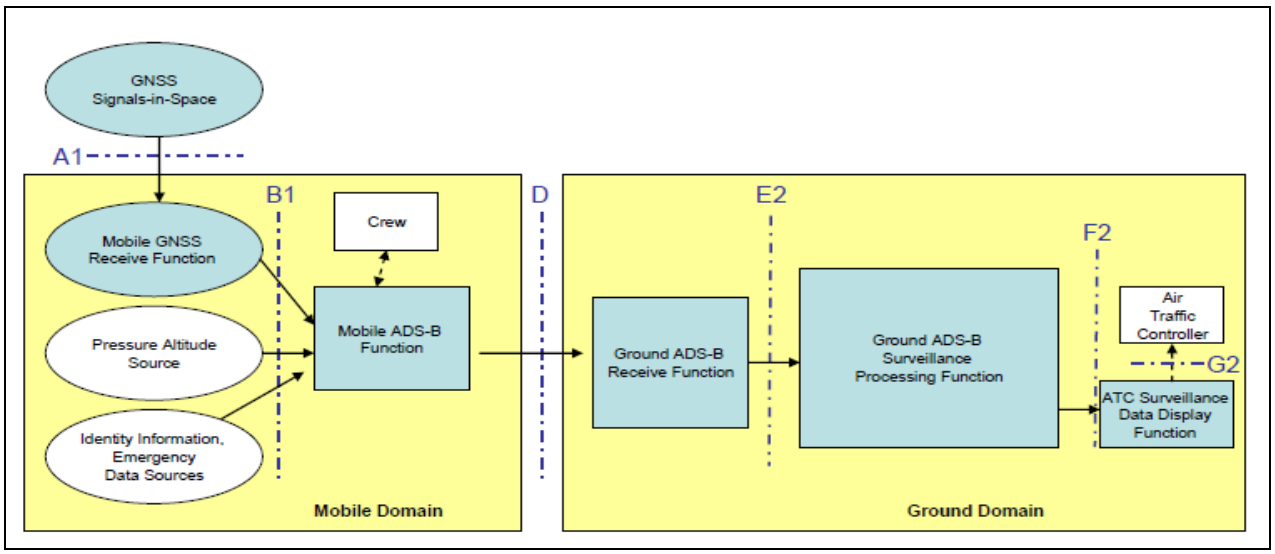

Figure 11. ADS-B APT Functional Model

The ADS-B Ground Domain consists of interconnected 'ADS-B Ground Receive' function, 'Ground ADS-B Surveillance Processing' function and 'ATC Surveillance Data Display Function' function, located between defined Interfaces D and F2 [8]. This is a very similar set of functions to the ADS-B NRA application, which also only features ADS-B surveillance sources.

5.2 ADS-B APT OSED

ADS-B APT Operational Services and Environment Description defines the following [7]:

ADS-B APT is restricted to operations on the airport Manoeuvring Area, except for aircraft identification where operations on the Apron are included

ADS-B surveillance coverage extends beyond the Manoeuvring Area to encompass relevant protection zones i.e. Navaids, etc

APT Operational Hazard Assessment assumes interactions between at least 2 Mobiles, where at least one is an aircraft

100% of Mobiles in Manoeuvring Area are equipped with ADS-B out systems i.e. Mode S transponder or ADS-B transmitter

Simple to Complex aerodrome layout with up to two active runways at any point in time

VHF comms to all Mobiles is available and independent of ADS-B

Three Visibly Conditions are defined, with :

- VC 1 = 75%
- VC 2 = 15%
- VC3 = 10%

20-25 movements per hour for VC1 & VC2 for single runway. Up to 35 per hour for multiple runways (<=2)

VC3 reduces traffic numbers of 15 movements per hour for the active runway

APT specifies latency requirements on aircraft position data which are compliant to ADS-B ED-102A/DO-260B MOPS, in addition to DO-260A and ED-102/DO-260 compliance for Navigation Accuracy indicators

Ground Domain flight hour to operational hour conversion factor was calculated using the following expression:

- 20 aircraft x 11.4 min flight duration on airport / 60 min =

  = 3.8 flight hr to ATSU hours

5.3 ADS-B APT OSA

5.3.1 APT Operational Hazards

Operational Hazards defined with the ADS-B NRA application are given in Table 17 [8]:

Item	Operational Hazard
OH1	Unexpected Loss of Target Information for a Single Mobile
OH2	Unexpected Loss of Target Information for Multiple Mobiles
OH3	Incorrect Horizontal Position Information for a Single Mobile
OH4	Incorrect Horizontal Position Information for Multiple Mobiles
OH5	False Target(s)
OH6	Incorrect Identity Information for a Single Mobile
OH7	Incorrect Identity Information for Multiple Mobiles
OH8	Unexpected Loss of Identity Information for a Single Mobile
OH9	Unexpected Loss of Identity Information for Multiple Mobiles
OH10	Incorrect but Plausible Discrete Emergency Mode

Table 17. ADS-B NRA Operational Hazards

ADS-B APT Operational Hazards are categorised into ATM Hazard Severity Classes within the Operational Hazard Assessment (OHA), as described within the 1st Iteration Safety Report [5] and ED-163 [8]. ATM Severity Classes 1 to 5 are defined, with 1 the most severe in terms of effects to the ATM operation and aircraft in-question and 5 the least. This sub-division of ATM Hazard severity class enables the assignment of ATM Safety Targets to different classes using a Risk Classification Scheme (RCS), as defined in ED-78A, ED-125 and reproduced in ED-163 [8].

All OH's were assessed for the detected condition and undetected condition, except for OH2 where it was deemed that the non-detection of the loss of multiple Mobiles on the ATC Controller display was not a credible failure case for the OH. Therefore, 19 OH Test Cases were assessed within the conducted OHA [8].

The OHA yielded the following APT application Operational Hazard SC Nmax distribution [8]:

SC	APT OH	APT OH Dist. $Nmax_i$
Severity Class 1	**OH01u, OH06u, OH07u**	**3**
Severity Class 2	**N/A**	**0**
Severity Class 3	**OH03u, OH04u, OH05u,**	**3**
Severity Class 4	**OH02, COH07u,**	**2**
Severity Class 5	**OH1d, OH06d, OH07d, OH08, OH09**	**5**
	Total	**13**

Table 18. ADS-B APT Severity Class Operational Hazard distribution

No Severity Class 2 hazards were allocated to ADS-B APT within the OHA. Severity Class 5 Operational Hazards do not contribute to the APT OH Distribution values, as a SC5 hazard is defined in the ED-78A to have not impact on the ATM system.

5.3.2 RAD APT Safety Objectives

Safety Targets apportioned to the whole ATM system for different application were set for recent ADS-B applications in ED-125 i.e. ADS-N RAD and APT are given in Table 21. ADS-B APT application adopted an Ambition Factor of 10, in-alignment with ADS-B RAD and ED-125 recommendation for modifications to the existing ATM system, yielding the ATM ST values given in Table 14 column 4 [8].

ADS-B APT application was defined to be applicable to Simple to Complex aerodromes, featuring up to two active runways within the OSED. Inspection of ED-125 reveals that this configuration was defined to be an Airport of Complexity 2, which is defined to have the Nmax Operational Hazard distribution shown in Table 19. Apportioning the overall ATM ST values to those applicable to the ADS-B APT application through the use of Equation (1) gives the ST per ATM OH distribution shown in Table 19 [8]:

SC	ATM ST (per flight hr)	Ambition Factor	ATM ST (per flight hr)	ATM OH Dist. $Nmax_i$ – APT 2	ST per ATM OH Dist. (per flight hr)
Severity Class 1	1e-08	**10**	1e-09	**3**	**3.3E-10**
Severity Class 2	1e-05	**10**	1e-06	**15**	**6.7E-08**
Severity Class 3	1e-04	**10**	1e-05	**30**	**3.3E-07**
Severity Class 4	1e-02	**10**	1e-03	**77**	**1.3E-05**

Table 19. ATM Safety Targets, Operational Hazard distribution and APT Safety Targets

Therefore, APT ATM Operational Hazard Safety Targets are of the same order of magnitude compared to ADS-B RAD ST values and several orders of magnitude more severe than those specified in the ADS-B NRA SPR document.

ATM Safety Targets were apportioned to the ADS-B APT application within ED-163 through comparison between the Overall ATM OH Distribution values and the APT value, as shown in Table 21 per Operational Hazard Severity Class [8]. ADS-B APT therefore takes the whole budget of the Overall ATM OH for Severity Class 1, thereby sub-dividing the total budget by a factor of 3 for between OH01u, OH06u and OH07u. as shown in Table 21. Similar activities were not required for the APT application SC 2 & 4 Safety Targets, as these values were significantly below the Overall ATM budget [8].

SC	ST per ATM OH Dist. (per flight hr)	Overall ATM OH Dist. Nmax	APT application OH Dist. $Nmax_i$	APT application ST (per flight hr)
Severity Class 1	3.3E-10	**3**	**3**	**1E-10**
Severity Class 2	6.7E-08	**15**	**0**	
Severity Class 3	3.3E-07	**30**	**3**	**3.3E-07**
Severity Class 4	1.3E-05	**77**	**2**	**1.3E-05**

Table 20. ADS-B APT Safety Targets

Pe values for APT OH were derived through the use of an event tree per Operational Hazard case, in the same manner used for ADS-B RAD. Each event tree branch contributed a Pe value and ATM Severity Class. These values were combined into a Safety Objective per event tree branch and the most demanding was declared as the Safety Objective for the assessed Operational Hazard [8].

The Safety Objectives were again used as the input condition for the derivation of the ADS-B APT Safety Requirements through Fault Tree analysis in the ASOR process.

5.3.3 ADS-B APT Safety Requirements

Inspection of the APT OSA fault trees and event trees demonstrates that in contrast to ED-161 RAD OSA and in the same manner as ED-126 OSA, only fault tree requirements were defined as Safety Requirements with barrier requirements from the event trees defined as Environment Conditions and OSA Assumptions.

Ground domain Safety Requirements for ADS-B APT are given in Table 21 [8]:

OH	SR#	Safety Requirement
OH1u, OH02, OH05u, OH07all OH06u	**02**	The likelihood of the Ground Domain system integrity failure **shall** be 1.00E-03 or less per ATSU hour. This SR is derived from the Basic Event SYS_INTG_GND, which has a value or 2.63E-04 per flight hour or 1E-03 per ATSU hr, using the flight hr to ATSU hr conversion factor of 3.8.
OH2	**03**	The likelihood of the Ground Domain system continuity failure **shall** be 1.00E-03 or less per ATSU hour. This SR is derived from the Basic Event SYS_INTG_GND, which has a value or 2.63E-04 per flight hour or 1E-03 per ATSU hr.
OH03u,	**04**	The normal (no fault) accuracy of ADS-B displayed positions **shall** lead to a misleading position 1.14E-03 per ATSU hr This SR is applied to both the Mobile and Ground Domain and is derived from the Basis Event DATA_RARE_NORM, which has a value of 3E-04 per flight hr.
OH02-mod	**05**	If GNSS ground monitoring is implemented, the likelihood that the Ground Domain position source monitoring function produces a false alert, **shall** be 1.00E-03 or less per ATSU hour.
OH06u-mod	**06**	If GNSS ground monitoring is implemented, the probability that the Ground Domain position source monitoring function fails to detect a position source data continuity or integrity failure **shall** be 1.00E-02 or less per failure event

Table 21. ADS-B APT Safety Requirements to OH mapping

Safety Requirements 05 & 06 relate to the implementation of a GNSS signal quality monitoring function within the ADS-B APT ground architecture. This feature is proposed to help meet the GPS accuracy and position monitoring performance requirements and is not driven by system safety requirements. Therefore, it is not included within the ADS-B Functional Model shown in Section 5.1.

5.3.4 ADS-B APT Safety and Performance Requirements

ADS-B APT Safety Requirements were combined into the following APT Safety and Performance Requirements set for the Ground Domain [8]:

SPR#	Safety and Performance Requirement	SR
SPR6	The horizontal position source accuracy (at interface B1) shall be less than or equal to 10 meters (95%)	**04**
SPR20	The likelihood of the Ground Domain system integrity failure **shall** be 1.00E-03 or less per ATSU hour	**02**
SPR21	The likelihood of the Ground Domain system continuity failure **shall** be 1.00E-03 or less per ATSU hour	**03**

Table 22. Ground Domain SPR set for ADS-B APT application

Note that SPR6 is defined at interface B1 (Figure 11) and hence is resident within the Mobile Domain of the APT Functional Model.

6 Enhanced ADS-B Ground System

6.1 Enhanced ADS-B GS SPR Logical Model

The enhanced ADS-B ground system (GS) developed within SESAR WP15.4.5 comprises enhanced ADS-B Ground Stations and an enhanced Surveillance Data Processing and Distribution (SDPD) system i.e. EUROCONTROL ARTAS, connected by modified ASTERIX CAT 21 and 23 interfaces [1].

Inspection of the logical models for ADS-B NRA, RAD and APT application concludes that the enhanced ADS-B ground system elements reside within the Ground Domain of each application, between the defined interfaces D2 and F2. This conclusion supports the enhanced ADS-B ground system proposed within the 1st Iteration Safety Report and repeated in Figure 12 [5]:

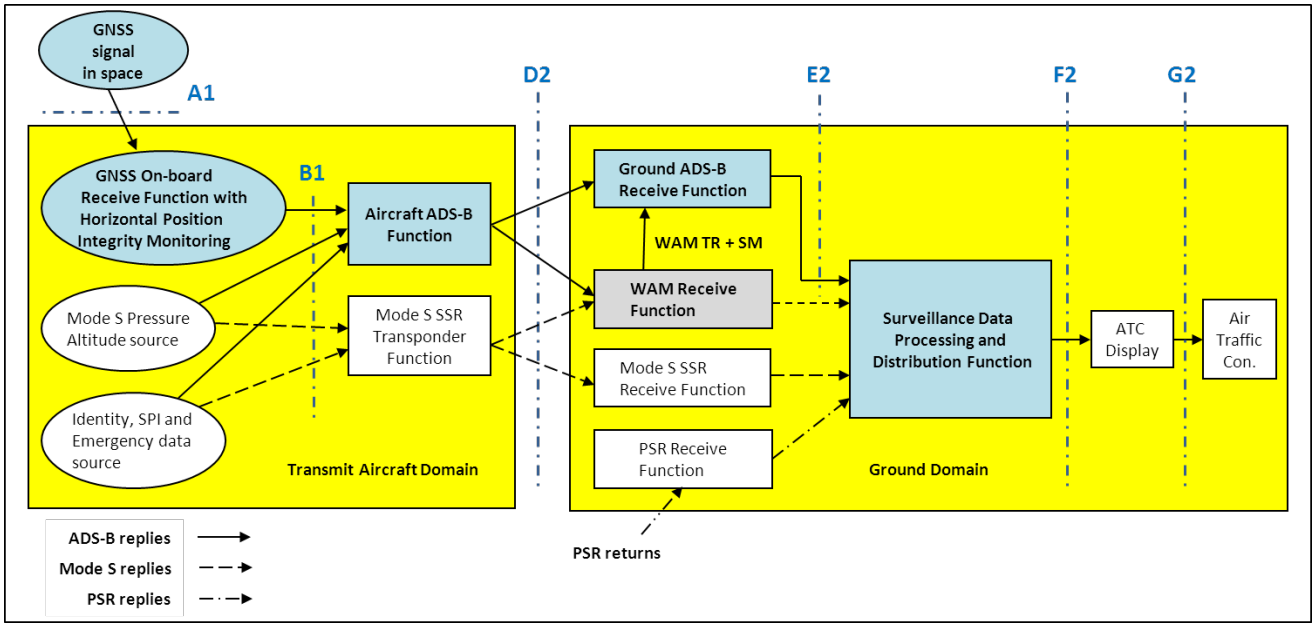

Figure 12. Enhanced ADS-B Ground System Functional Model

The ADS-B Ground Domain consists of connected 'Ground ADS-B Receive' function and Surveillance Data Processing and Distribution' functions between interfaces D2 and F2. Good commonality is noted between the proposed ADS-B functional model above and those proposed in the NRA (Figure9), RAD (Figure10), and APT (Figure11).

The 'WAM receive' function provides WAM target reports and service and status messages to the ADS-B Data Validation function implemented within the 2nd Iteration Prototype Groundstation, as described within the 2nd Iteration Security Assessment report [18].

6.2 Enhanced ADS-B GS Safety and Performance Requirements

Given the good commonality between the functional model proposed for the enhanced ADS-B ground system and the defined models within the supported ADS-B applications, the Safety and Performance Requirements for each application were combined and allocated against elements of the enhanced ADS-B ground system, shown in Table 23.

ADS-B RAD and APT applications feature Ground Domain Safety and Performance Requirements covering both the ADS-B Receive and ATC processing and display functions. However, ADS-B NRA SPR only covered the ADS-B Receive function, even though the Safety Requirements were allocated

against the ATC processing and display functions within the conducted OSA. To address these missing SR, new NRA SPR numbers 27-30 are proposed within Table 9 and repeated within Table 23:

ADS-B App Source	SPR#	Safety and Performance Requirement	C or L	Enhanced ADS-B Element
NRA	**SPR13**	The likelihood that the ADS-B receive subsystem corrupts ADS-B information through the reception, processing or delivery of data (E2) shall be no more than **5E-06** per ATSU hour	C	1090 GS
NRA	**SPR14**	The likelihood that ADS-B receive subsystem does not provide updated 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	L	1090 GS
NRA	**SPR15**	The likelihood that the 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	L	1090 GS
NRA	**SPR27**	The likelihood that ATC processing system does not notify the Controller of the loss of a track (e.g. through coasting) should be no more than **1E-05** per ATSU-hour	L	SDPD
NRA	**SPR28**	The likelihood that ATC automation and display subsystem lose all information for *more than one aircraft*, should be no more than **5E-06** per ATSU-hour	L	SDPD
NRA	**SPR29**	The likelihood that ATC automation and display subsystem corrupts ADS-B quality indicator or position for one or aircraft should be no more than **5E-06** per ATSU-hour	C	SDPD
RAD	**SPR33**	The likelihood of an ADS-B Ground Domain system integrity failure shall be **2E-05** or less per ATSU hour	C	1090 GS + SDPD
RAD	**SPR34**	The likelihood of a "Ground ADS-B Receive" function continuity failure shall be **1E-05** or less per ATSU hour	L	1090 GS
APT	**SPR20**	The likelihood of the Ground Domain system integrity failure shall be **1.00E-03** or less per ATSU hour	C	1090 GS + SDPD
APT	**SPR21**	The likelihood of the Ground Domain system continuity failure shall be **1.00E-03** or less per ATSU hour	L	1090 GS + SDPD

Table 23. Enhanced ADS-B Ground System input SPR set from ADS-B applications

NOTE 1: L = Loss C = Corruption

The above SPR set is proposed for consideration in the design of the enhanced ADS-B ground system and its specification by ANSP considering its implementation into their ATM infrastructure.

It should still be noted that significant care should be exercised when comparing Safety Requirements extracted from the ADS-B NRA OSA compared to either RAD or APT documents for ground based ATM surveillance applications due to inconsistencies noted earlier in the report within the Overall ATM Operational Distribution used for determining OH Safety Objectives and hence Safety Requirements.

7 Conclusions

WP15.4.5b Prototype 2nd Iteration has been defined to support ADS-B RAD and ADS-B APT applications explicitly, in-addition to the implicit ADS-B NRA application [1]. Each ADS-B ATM application is defined within its Safety and Performance and Interoperability Requirements Document. This report describes the structure of each SPR document, comprising a Operational Service and Environment Description (OSED), Operational Performance Assessment (OPA), Operational Safety Assessment (OSA) and Interoperability Assessment (IA).

Safety Requirements and Performance Requirements generated within the OSA and OPA respectively are combined into Safety and Performance Requirements (SPR) within the SPR summary section. The SPR summary section also contains the ADS-B application Functional Model, for the purpose of allocation of Operational, Performance and Safety Requirements within the Airborne and Ground domains in the performed assessments.

The report presents a summary of the ADS-B NRA, RAD and APT SPR documents, comprising:

SPR Functional Model for each application and salient points from the OSED

Detailed summary of the Operational Safety Assessment comprising

- Operational Hazard list
- ATM Safety Target and ADS-B application Safety Target determination,
- Safety Objectives and Probability of Effect values,
- Safety Requirements for each application and
- Safety and Performance Requirements derived from the Safety Requirements

The final section of this report draws all elements into a proposed enhanced ADS-B ground system functional model and combined NRA, RAD and APT SPR requirements set for consideration in the design of the enhanced ADS-B ground system developed within WP15.4.5.

This report is aimed at Air Navigation Service Providers who are unfamiliar with the format and content of the available ADS-B applications standards and are considering integrating the enhanced ADS-B ground system into their surveillance infrastructure. The report presents a summary of the available ADS-B applications and hence help the ANSP to select a ADS-B operating environment which matches their own needs and informs them of the relevant Safety Requirements which they should consider within a system procurement activity.

It is further planned that the identified Safety Requirements will be validated against the three manufacturers ADS-B ground system elements within the 3rd Iteration Safety Assessment report, document D22, as this prototype will comprise the fully developed enhanced ADS-B ground system within the WP15.4.5 project. The validation approach will be identified and agreed within the 3rd Iteration Kick Off Activity through consultation with EUROCONTROL and SJU Safety Subject Matter Experts and is expected to feature use of relevant Safety Guidance Material generated in SESAR WP16.06.01 and EUROCAE ED-109/ED-153.

8 Assumptions

None

9 References

[1] SJU 15.04.05a Specification Baseline Document, **D17**, Ed. 00.01.00, Oct 2010

[2] SJU 15.04.05a ADS-B Surveillance System Spec. for It 2, **D19**, Ed. 00.03.00, September 2011

[3] SJU 15.04.05a ADS-B 1090MHz Ext. Squitter Ground Station Spec – Iteration 2, **D09** Ed 00.01.02, September 2011

[4] SJU 15.04.05b Second Iteration – Baseline Report/Matrix, **D10** Ed 00.01.00, April 2013

[5] First Iteration – Provision of Final Safety Assessment Report, **D08** Ed 00.01.00, April 2012

[6] EUROCAE SAFETY, PERFORMANCE AND INTEROPERABILITY REQUIREMENTS DOCUMENT FOR ADS-B-NRA APPLICATION, **ED-126**, Dec 2006

[7] EUROCAE SAFETY, PERFORMANCE AND INTEROPERABILITY REQUIREMENTS DOCUMENT FOR ADS-B-RAD APPLICATION, **ED-161**, Sept. 2009

[8] EUROCAE SAFETY, PERFORMANCE AND INTEROPERABILITY REQUIREMENTS DOCUMENT FOR ADS-B AIRPORT SURFACE SURVEILLANCE APPLICATION (ADS-B-APT), **ED-163**, Dec 2010

[9] EUROCAE Technical Specification for a 1090 MHz Extended Squitter ADS-B Ground Station, **ED-129**, June 2010

[10] SJU 15.04.05a SDPD Specification – Iteration 2, **D10** Ed 00.03.00, September 2011

[11] SJU 15.04.05a Interface Specifications for Second Iteration, **D11** Ed 00.01.00, October 2011

[12] SJU 15.04.05b Security Assessment for 15.04.05b Prototype Second Iteration, **D16** Ed 00.01.00, July 2013

[13] PROCESS FOR SPECIFYING RISK CLASSIFICATION SCHEME AND DERIVING SAFETY OBJECTIVES IN ATM, **ED-125**

[14] Minimum Operational Performance Standards for 1090MHz Extended Squitter Automatic Dependant Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B), RTCA **DO-260B**, Dec 2009.

[15] GUIDELINES FOR COMMUNICATION, NAVIGATION, SURVEILLANCE, AND AIR TRAFFIC MANAGEMENT (CNS/ATM) SYSTEMS SOFTWARE INTEGRITY ASSURANCE, **ED-109**, March 2002

[16] GUIDELINES FOR ANS SOFTWARE SAFETY ASSURANCE, **ED-153**, August 2009

[17] **ESARR 4** RISK ASSESSMENT AND MITIGATION IN ATM, Ed 1.0, April 2001

[18] Security Assessment for 15.04.05b 2nd Prototype Iteration, **D16** Edition 00.01.00, July 2013

[19] GUIDELINES FOR APPROVAL OF THE PROVISION AND USE OF AIR TRAFFIC SERVICES SUPPORTED BY DATA COMMUNICATIONS, **ED-78A**, Dec 2000.

[20] Fault Tree Handbook, U.S. Nuclear Regulatory Commission NUREG-0492

-END OF DOCUMENT-