Security Assessment for 15.04.05b 2nd Prototype Iteration

Document information	
Project Title	Surveillance Ground System Enhancements for ADS-B (Prototype Development)
Project Number	15.04.05b
Project Manager	Thales
Deliverable Name	Security Assessment for 15.04.05b 2nd Prototype Iteration
Deliverable ID	Del 16
Edition	00.01.00
Template Version	03.00.00
Task contributors	
EUROCONTROL;INDRA;NATS;NORACON;SELEX;THALES	

Abstract

SESAR WP15.4.5 is tasked with the implementation of enhancements into the ADS-B ground based surveillance system to address security limitations of current ADS-B technology. It is planned that the enhanced ADS-B ground system will deliver surveillance services that can augment existing radar services within High Density TMA type airspace and offer standalone surveillance within lower density operating environments [1].

WP15.4.5b will develop three pre-industrialisation prototypes of the enhanced ADS-B ground system, termed the 1st, 2nd and 3rd Prototype Iteration. Each Iteration corresponds to a separate SESAR CONOPS and 2nd Prototype Iteration aligns with SESAR 'Trajectory Based Operations' CONOPS [1].

The ADS-B ground system is defined to comprise remote enhanced ADS-B groundstations [3] connected to an enhanced SDPD system [4], via modified ASTERIX CAT 21 & 23 interfaces [5]. The enhanced data is distributed from the SDPD system via modified CAT 62 and 65 interfaces [5].

This report details the selected security enhancements implemented into the 1st and 2nd Iteration enhanced ADS-B ground system [13], [2]. It describes in detail the development path of selected 1st Iteration enhancements into improved versions incorporating new functionality within the 2nd Iteration and demonstrates that each of the implemented enhancements act as security enhancements to ADS-B, through the implemented validation tests.

Authoring & Approval

Prepared By		
Name & Company	**Position & Title**	**Date**
[redacted] NATS	[redacted]	11/07/2013
[redacted] NATS	[redacted]	11/07/2013

Reviewed By		
Name & Company	**Position & Title**	**Date**
[redacted] THALES	[redacted]	11/07/2013
[redacted] INDRA	[redacted]	02/07/2013
[redacted] THALES	[redacted]	04/07/2013
[redacted] SELEX	[redacted]	28/06/2013
[redacted] NORACON	[redacted]	03/07/2013
[redacted] EUROCONTROL	[redacted]	08/07/2013

Reviewed By – *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	**Position & Title**	**Date**
None		

Approved for submission to the SJU		
Name & Company	**Position & Title**	**Date**
[redacted] THALES	[redacted]	11/07/2013
[redacted] INDRA	[redacted]	
[redacted] EUROCONTROL	[redacted]	08/07/2013
[redacted] SELEX	[redacted]	08/07/2013
[redacted] NORACON	[redacted]	09/07/2013

Rejected By		
Name & Company	**Position & Title**	**Date**
None		

Rational for rejection
None

Document History

Edition	Date	Status	Author	Justification
00.00.01	21/06/2013	Draft	[redacted]	First Draft
00.01.00	11/07/2013	Final version		Inclusive of partner 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 is tasked with the implementation of enhancements into the ADS-B ground based surveillance system to address security and integrity limitations of ADS-B technology [1]. It is planned that the enhanced ADS-B ground system will offer a surveillance service that can augment existing radar services within High Density TMA type airspace and offer standalone surveillance services in lower density operating environments [1].

WP15.4.5b will develop three pre-industrialisation prototypes of the enhanced ADS-B ground system, termed the 1st, 2nd and 3rd Iteration. Each Iteration corresponds to a separate SESAR CONOPS and Prototype 2nd Prototype Iteration is aligned with SESAR Trajectory Based Operations CONOPS [1].

This report assesses the security limitations within an unencrypted broadcast technology such as ADS-B and describes the WP15.4.5 selected enhancements to the ADS-B ground system to address these limitations. The enhanced ADS-B ground system will comprise interconnected remote ADS-B groundstations and a central SDPD system [2].

WP15.4.5b contains three ADS-B groundstation suppliers; Thales, Indra and Selex and one SDPD supplier, EUROCONTROL. Each supplier has implemented selected security enhancements into their element of the Prototype 2nd Prototype Iteration enhanced ADS-B ground system and these are defined within its Baseline Matrix and elaborated within this report [6].

Three security enhancements were selected for incorporation with WP15.4.5b Prototype 2nd Prototype Iteration, with different manufacturers implementing different enhancements within their elements of the enhanced ADS-B ground system, as shown in Table 1 [6]:

Item No.	Enhancement	Thales ADS-B GS	Selex ADS-B GS	Indra ADS-B GS	EUROCNTRL SDPD
1	**Enhanced ADS-B target report validation via WAM integration**	N	Y	N	Y
2	**Behavioral Analysis of Targets**	N	N	Y	Y
3	**Time Differential of Arrival**	Y	Y	N	Y

Table 1. Security enhancement incorporation within Prototype 2nd Prototype Iteration

Three security enhancements selected for incorporation within the 2nd Prototype Iteration enhanced ADS-B ground system are described in detail within this report. These enhancements are analysed and proposed to offer security enhancements to ADS-B, as they provide independent validation of the reported ASD-B message data items, through either:

- comparison with measured results or
- inspection of data value to determine if it falls within a validity range

The validation tests were conducted within the 'ADS-B Data Validation' function within the enhanced ADS-B groundstation and the results reported to the SDPD for processing using Target Report Descriptor results field in ASTERIX CAT 21.

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 2nd Prototype Iteration and a summary of the security limitations within ADS-B technology. It details the enhancements implemented into Prototype 2nd Prototype Iteration to counter the described security issues [2].

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 ADS-B systems into their ATM system.

1.3 Inputs from other projects

WP15.4.5a ADS-B surveillance system specifications, groundstation specifications, interface specifications and SDPD specifications for the enhanced ADS-B ground system.

1.4 Structure of the document

- Executive Summary
- Chapter 1: Introduction
- Chapter 2: Safety and Security
- Chapter 3: WP15.45.b ADS-B Security Enhancements
  - 1st Prototype Iteration ADS-B Applications and Enhancements
  - 2nd Prototype Iteration ADS-B Applications and Enhancements
  - Mapping of security enhancements between Iterations
- Chapter 4: 2nd Iteration Security Enhancements
  - WAM integration
  - Behavioural Analysis
  - Time
- Chapter 5: Assumptions
- Chapter 6: References

1.5 Functional Block Purpose

1.5.1 Enhanced ADS-B ground system overview

WP15.4.5b is tasked with taking the system, test and interface specifications input from WP15.4.5a and developing enhanced ADS-B ground system prototypes. These were termed 1st, 2nd and 3rd Prototype Iterations and this document is concerned with 2nd Prototype Iteration of the enhanced ADS-B ground system [1].

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

- ADS-B groundstation(s) [3]
- Surveillance Data Processing and Distribution (SDPD) system [4]
- ASTERIX Category interfaces i.e. ADS-B target reports in CAT 021 and service messages in CAT 023 and System Track data in CAT 062 and service messages in CAT 063 [5]

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

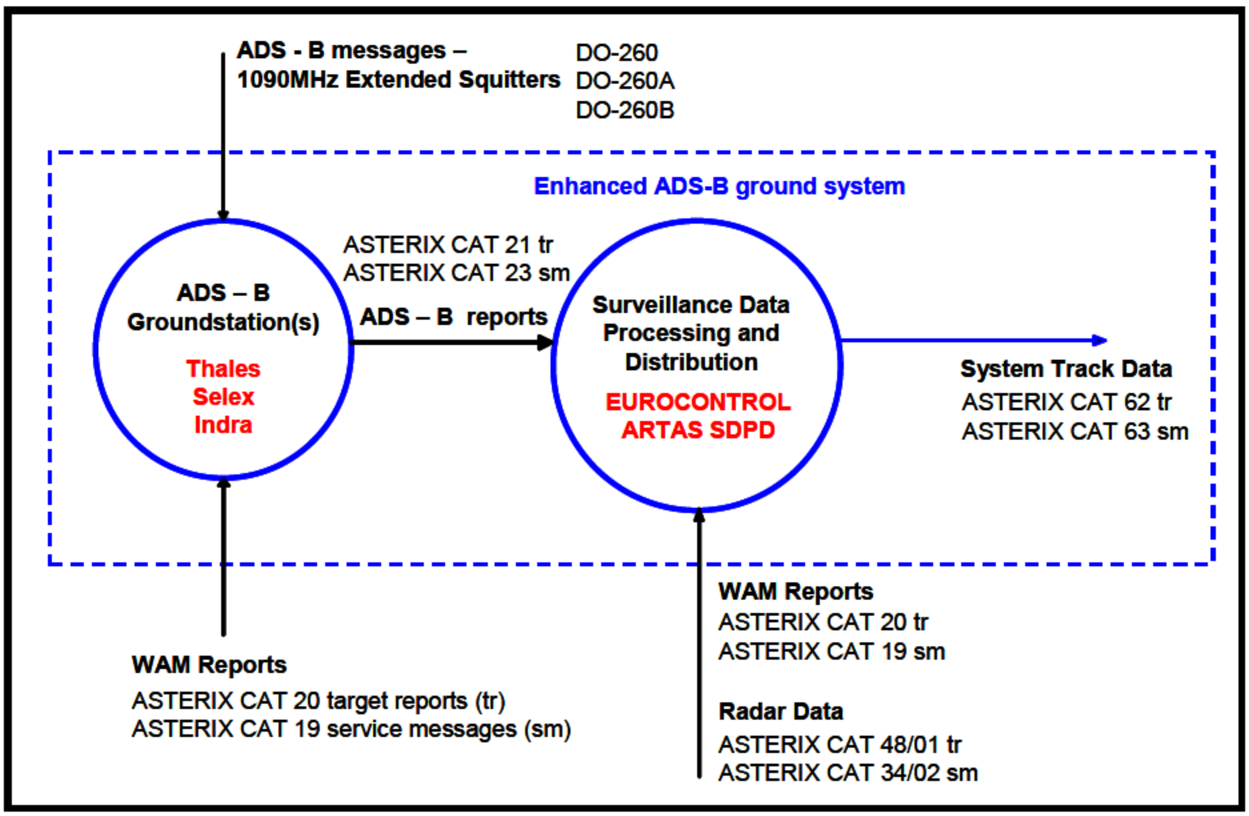

Figure 1. Enhanced ADS-B ground system schematic

NOTE 1: sm = service messages tr = target messages

1.6 Functional block Overview

1.6.1 Enhanced ADS-B groundstation overview

The primary functions of the non-enhanced ADS-B groundstation (GS) compliantto ADS-B NRA Groundstation Technical Specification ED-129 are [3]:

- Receive 1090 MHz RF input on the **Air Interface** via the 'Antenna' function
- Extract ADS-B message payload data from 1090MHz Extended Squitter ADS-B messages, within the '1090 ES Reception' function
- Timestamp the decoded ADS-B messages using the time signals input from 'UTC Time Sync' function presented from the **Time Signals** interface
- Assemble the ADS-B message data into ASTERIX Category 021 target reports within the 'Report Assembly' function
- Dispatch the ASTERIX CAT 021 ADS-B target reports and ASTERIX CAT 023 service messages to client systems over the **Ground Interface** from the 'Report Assembly' function
- Interact with Remote Control and Monitoring systems through the **Management Interface** implemented within the 'GS Management and Status Reporting' function
- Determines the internal status of the groundstation equipment through the 'BITE' function

A schematic diagram showing the functional block diagram of the enhanced ADS-B groundstation is shown in Figure 2:

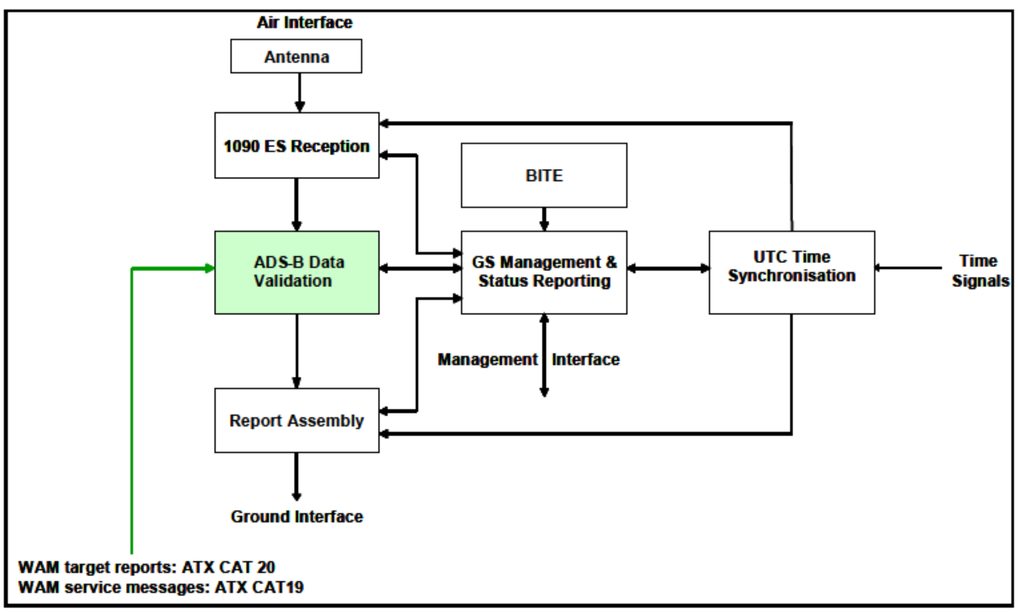

Figure 2. Enhanced ADS-B groundstation functional overview

Comparison with the functional blocks defined for the ADS-B-NRA groundstation in ED-129 [7], shows that the 'ADS-B Data Validation' function (shown in green in Figure 2) has been added in the enhanced ADS-B groundstation. This element performs the security enhancements implemented into WP15.4.5b Prototype 2nd Prototype Iteration groundstation, including integration with WAM target reports and service messages as shown.

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 Groundstations and serves fused surveillance track updates to client systems, such as Controller Working Position (CWP) displays. Aircraft data updates contain measured or reported 2-D horizontal position, reported altimeter altitude, velocity, status and other information extracted from aircraft on-board systems and received by ground based surveillance sensors [4].

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 [4].

The SDPD uses the input service 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 streams and hence to discard or include each particular surveillance target data stream in the composite picture creation process.

The EUROCONTROL ARTAS product was selected as the SDPD element within the enhanced ADS-B system and is designed around four main functions [4];

- 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.

The enhancements implemented into the ARTAS SDPD product within WP15.4.5b are located within the TRACKER and SERVER functions, highlighted in Figure 3. The enhancements improve the SDPD's ability to discriminate false ADS-B targets from real aircraft and to either associates to the track and sets the flag (multi-sensor validation) or initiates a new track and sets the flag (other validations). .

A functional block diagram of the ARTAS SDPD system is shown in Figure 3 [4]:

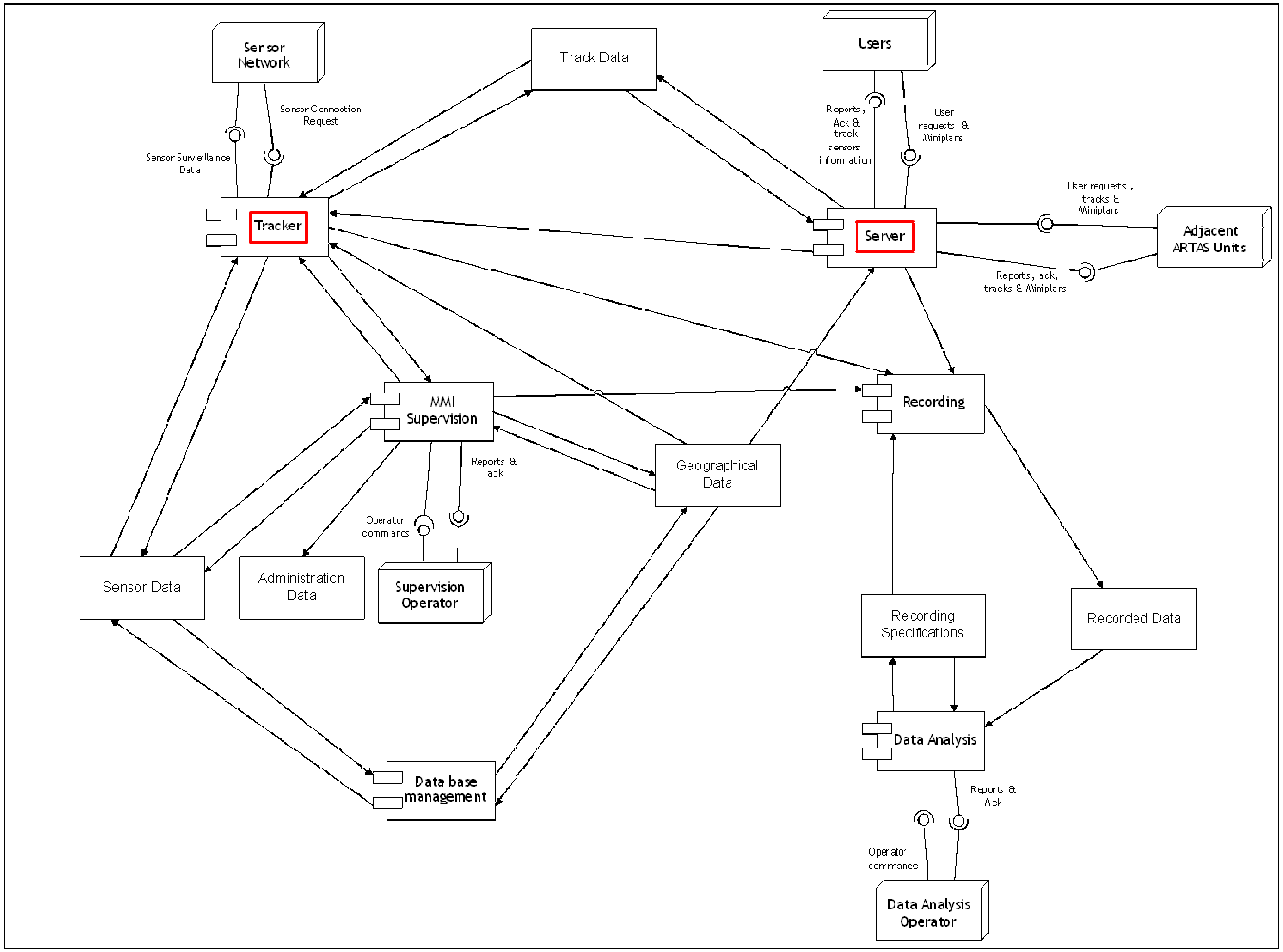

Figure 3. ARTAS functional overview

1.7 Glossary of terms

NA

1.8 Acronyms and Terminology

Term	Definition
ADS-B	Automatic Dependent Surveillance - Broadcast
ADS-B RAD	Enhanced ATS in Radar Areas (“ADS-B out” application)
ARTAS	ATM suRveillance Tracker And Server
ASTERIX	All-purpose Structured EUROCONTROL Surveillance Information Exchange
ATC	Air Traffic Control
ATCO	Air Traffic Control Officer
ATM	Air Traffic Management
BAR	Behavioural Analysis Result
BITE	Built-in Test System
CAT	Data Category
CONOPS	Concept of Operations
CWP	Controller Working Position
ED	EUROCAE Document
ES	Extended Squitter
EUROCAE	European Organisation for Civil Aviation Equipment
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GS	Ground Station
ICAO	International Civil Aviation Organization
INTEROP	Interoperability
Mode S	MODE Select
MOPS	Minimum Operational Performance Standards

Term	Definition
PVC	Position Velocity Check
RF	Radio Frequency
RTCA	Radio Technical Commission for Aeronautics
SDPD	Surveillance Data Processing and Distribution
SESAR	Single European Sky ATM Research (Programme)
SJU	SESAR Joint Undertaking
SSR	Secondary Surveillance Radar
TDOA	Time Difference Of Arrival
TMA	Terminal Manoeuvring Area
WAI	WAM Integration
WAM	Wide Area Multilateration

Table 2. Acronyms and Terminology

2 Safety & Security

Safety aspects of the 2nd Prototype Iteration ADS-B ground system are covered within the D15 Safety Assessment report [8]. This report will focus on the security enhancements implemented into the 2nd Iteration Prototype.

2.1 ADS-B security issues and limitations

2.1.1 Denial of Service – External ADS-B signals

Automatic Dependant Surveillance – Broadcast or ADS-B is a ground based surveillance technology which receives Extended Squitter ADS-B messages transmitted at 1090MHz from suitability capable and enabled transmitter or Mode S transponder devices carried by aircraft and air vehicles. Mode S Extended Squitter ADS-B messages contain the aircraft allocated 24-bit ICAO address, Aircraft Identification, Mode A code, Pressure Altitude coded in either 25ft or 100ft resolution, aircraft velocity and heading and aircraft 2-D horizontal position coded in a Lat, Lon value.

Several ADS-B ATM applications are targeted for incorporation within the Prototype 2nd Prototype Iteration of the enhanced ADS-B ground system. The principal one is the ADS-B RAD application [7], which involves the augmentation of the current air traffic situation picture created by Primary and Secondary radar surveillance sources within high density airspace by ADS-B surveillance services.

A functional diagram of the enhanced ground ADS-B surveillance system role within the modified ADS-B RAD logical model as defined in the 1st Prototype Safety Report is shown in [9]:

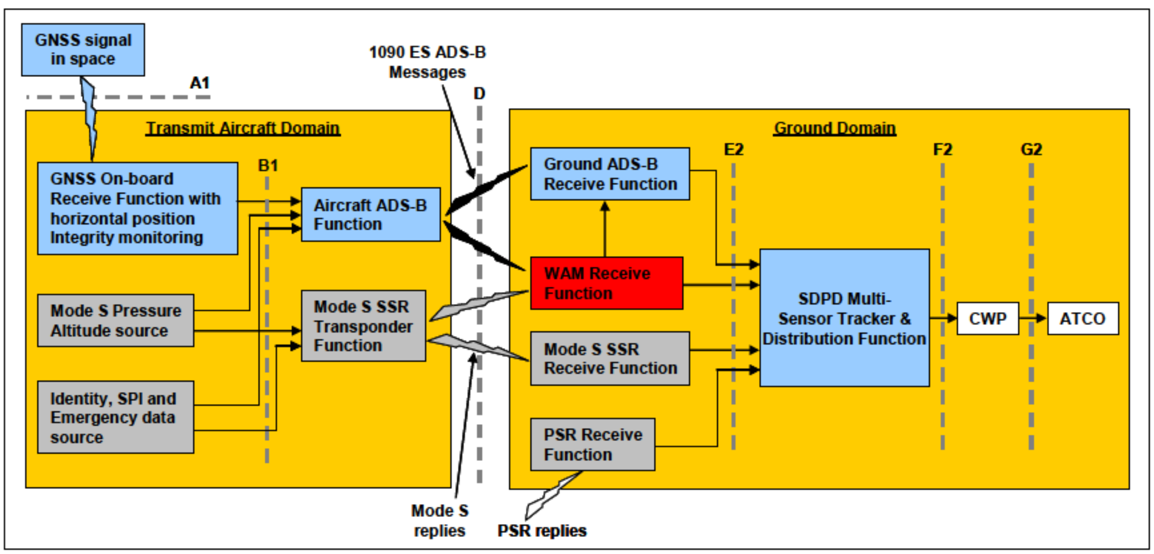

Figure 4. ADS-B surveillance system within the ADS-B RAD architecture

Inspection of the above figure shows that all of the data which is encoded within the ADS-B messages is derived from the aircraft avionics systems. The 2D horizontal position contained within the ADS-B message is derived from the on-board GNSS reception and horizontal position integrity monitoring function. The on-board GNSS horizontal positioning function is derived from GPS signals at present.

This dependency on aircraft derived information explains the term 'Dependant' surveillance applied to ADS-B. Other cooperative surveillance technologies, such as Wide Area Multilateration and Mode S SSR, measure the aircraft horizontal position and hence these are termed 'Independent' surveillance systems.

The prime security issue with ADS-B technology is that the ground system is entirely dependant on the integrity of the information within the aircraft ADS-B messages [8]. The transmission of misleading ADS-B information can be derived from two sources:

- The deliberate transmission of false ADS-B messages from an airborne or ground based transmitter(s), which produces valid ADS-B 1090MHz Extended Squitter messages not corresponding to real aircraft
- An aircraft with a mal-functioning transponder/transmitter which broadcasts incorrect and hence false ADS-B messages, possibly in-addition to its correct ADS-B message set.

The broadcasting of false ADS-B messages impacts on performance of ADS-B surveillance service, as real and false targets are now present within the delivered service. The presence of the false ADS-B targets is assessed to have three negative effects on the supplied surveillance service:

1. Increases Air Traffic Controller (ATCO) workload, as the ATCO may have to issue avoidance instructions to real aircraft to avoid a false ADS-B target displayed on the Controller Working Position display. This avoidance action is required as the controller has presently no means to determine if the displayed ADS-B target is a real aircraft or a false target in a non-fusion tracker ATM system. The increased ATCO workload could either lead to controller situational awareness is severely impaired to the point where provision of ATC services may no longer be possible or to reductions in airspace capacity in certain ATC sectors and hence a lowering of the ATM system efficiency levels, possibly leading to a withdrawal of the surveillance service from use.
2. The presence of identified false ADS-B targets would lower the confidence of the ATCO using the service to control real aircraft, again triggering a withdrawal of surveillance service from operational usage.
3. The presence of false ADS-B messages from mal-functioning Mode S transponders/transmitters may prevent the successful decoding of the real ADS-B message from the aircraft and prevent real aircraft tracks being displayed to the controlling ATCO. The ATCO would be unaware of the lack of real aircraft tracks and may instead be controlling aircraft using false ADS-B information, with the potential for separation minima erosion and collision risk occurring between pairs of controlled aircraft.

The first two of these issues reduce the efficiency the supplied ADS-B surveillance service operations and may necessitate the withdrawal of its usage. Hence this type of event is termed a 'denial of service attack'. An alternative term for this injection of false ADS-B targets into the surveillance service is a 'spoofing attack', as the surveillance system is spoofed or misled into the true nature of the received false ADS-B messages.

2.1.2 GPS/GNSS jamming

ADS-B is dependant on GPS/GNSS signals for horizontal position information, as shown in Figure 4. Therefore, jamming of input GNSS signals i.e. GPS would prevent the GNSS on-board reception function from producing horizontal position information for broadcast by the ADS-B messaging function. This form of activity is another form of Denial of Service attack, as it prevents the broadcast ADS-B information from containing position information, which is a key requirement for the delivery of ATC information to controlled traffic.

The availability of the GNSS function is however declared as outside of the scope of the enhanced ADS-B system, as it is an avionics issue rather than one located with the ground based ADS-B functionality and hence is not addressed by WP15.4.5.

3 WP15.04.05b ADS-B security enhancements

3.1 1st Prototype Iteration Applications and Enhancements

WP15.4.5a Specification Baseline Definition document D17 defined the following ADS-B ATM applications and enhancements to be incorporated within the WP15.4.5b 1st Prototype Iteration [1]:

ADS-B ATM applications	Security Enhancements	Technology enhancement
ADS-B RAD ATSA-ITP ATSA-VSA ATSA-AIRB	Simple ADS-B target report validation through comparison with WAM target data Multi-sensor data fusion consistency checks Use of increased timestamp accuracy for TOA functionalities Power measurements and range correlation Angle of arrival measurements Track consistency verification - velocity versus position change	ADS-B message decoding compliant to ED-102A/DO-260B [12]

Table 3. Enhancements implemented within the 1st Iteration Prototype

3.1.1 ADS-B ATM Applications

Supported ADS-B ATM applications within the 1st Iteration were:

- ADS-B RAD
- ATSA-ITP
- ATSA-VSA
- ATSA-AIRB

Airborne Traffic Situational Awareness or ATSA ADS-B applications are concerned with the broadcast of ADS-B messages in the Transmit Aircraft Domain and reception and display in the Receive Aircraft Domain. As all ATSA applications reside within the airborne domain, they were declared as outside of scope of the enhanced ADS-B ground system after assessment for the 1st Iteration [13].

Therefore, the ADS-B ATM application selected for incorporation within the 1st Iteration Prototype was **ADS-B RAD**.

3.1.2 Security Enhancements

The three groundstation manufacturers implemented selected security enhancements within their ADS-B groundstations in Iteration One, as described within the 1st Prototype Iteration Baseline Report [10]. EUROCONTROL implemented all security enhancements into the SDPD system, hence ensuring full interoperability between the different GS manufacturers for future ANSP deployments of enhanced ADS-B ground systems.

The WP15.4.5b 1st Iteration Baseline Report defined the mapping between implemented security enhancement and WP15.4.5b ADS-B groundstation manufacturer and is reproduced in Table 4 [10]:

Item No.	Security Enhancement	Thales ADS-B GS	Selex ADS-B GS	Indra ADS-B GS	EUROCONTRL SDPD
1	Simple ADS-B target report position validation through WAM target data comparison	Y	Y	N	Y
2	Angle of Arrival measurement	N	N	Y	Y
3	Position change vs velocity check	Y	N	N	Y
4	Power measurement vs range correlation	N	N	Y	Y
5	Time of Arrival vs Aircraft Calculated Distance from ADS-B GS Validation	N	Y	N	Y
6	Multi-sensor data fusion consistency checks	NA	NA	NA	Y

Table 4. Security enhancement incorporation within 1st Prototype Iteration

3.1.3 Technology Enhancement

All WP15.4.5b ADS-B groundstation manufacturers i.e. Thales, Selex and Indra developed ADS-B prototype groundstations within the 1st Iteration which were able to decode ADS-B messages formatted to the new ADS-B Change 2 Minimum Operating Standards (MOPS), ED-102A/DO-260B [12].

This new functionality was in addition to the ability to be able to decode ADS-B messages formatted to ADS-B Change 0 MOPS, ED-102/DO-260 and ADS-B Change 1 MOPS, DO-260A [14].

3.2 2nd Prototype Iteration Applications and Enhancements

WP15.4.5a Specification Baseline Definition document D17 defined the following ADS-B ATM applications and enhancements to be incorporated within the WP15.4.5b 2nd Prototype Iteration, in addition to the baseline established in the 1st Iteration [1]:

ADS-B applications	Security Enhancements	Technology Enhancement
ADS-B APT ADS-B ADD ATSA SURF ASPA-Flight Deck Interval Management (FIM)	Enhanced ADS-B target report validation through WAM target report comparison TDOA Multi-ground station target tracking Increased antenna sectorisation to improve the localization performance Behavioural analysis of targets Enhancements from CASCADE process (to reflect any requirements stemming from the safety, performance and interoperability work on ADS-B integration with WAM)	Automatic network bandwidth optimisation techniques.

Table 5. Enhancements implemented within the 2nd Iteration Prototype

3.2.1 ADS-B ATM Applications

Supported ADS-B ATM applications within the 2nd Iteration were:

- ADS-B APT
- ADS-B ADD
- ATSA SURF
- ASPA-Flight Deck Interval Management (FIM)

Again, the ATSA SURF application was declared as out of scope for the 2nd Iteration, as it was assessed to have no impact on the ground surveillance segment. In a similar vein, the Airborne Separation Application ASPA-FIM was also declared to have no impact on the ground environment and hence out of scope [2].

ADS-B Airborne Derived Data (ADD) was proposed for incorporation within the 2nd Prototype Iteration within the WP15.4.5a Specification Baseline Document D17 [1]. However, the extraction of non-ED-102A-DO-206B provided ADD items from aircraft transponders was assessed to require the incorporation of integrator into the ADS-B groundstation of the enhanced ADS-B ground system. This was rejected on the grounds of increased system cost and technical complexity for the 2nd Prototype [2].

The selected ADS-B ATM application for incorporation within the 2nd Iteration Prototype enhanced ADS-B ground system was **ADS-B APT**. This was in-addition to ADS-B RAD from the 1st Iteration.

3.2.2 Security Enhancements

Further security enhancements were considered for incorporation within 2nd Prototype Iteration, in addition the 1st Iteration baseline [2]:

- Enhanced ADS-B target report validation through comparison with WAM target reports
- Enhancements from CASCADE process (to reflect any requirements stemming from the safety, performance and interoperability work on ADS-B integration with WAM)
- Use of TDOA Techniques
- Multi-Ground Station target tracking
- Increased antennas sectorisation to improve the localisation performance
- Behavioural analysis of targets

Analysis was conducted by WP15.4.5a project group on the proposed security enhancement set and following this activity 3 enhancement were retained for incorporation into the 2nd Prototype Iteration [2]:

- Enhanced ADS-B target report data item validation through comparison with WAM target reports
- Time Difference Of Arrival aircraft position validation techniques
- Behavioural analysis of targets

The 2nd Iteration Baseline Report defined the mapping of selected security enhancement to groundstation manufacturers in the same used for Iteration One. This is shown in Table 6 [6]:

Item No.	Security Enhancement	Thales ADS-B GS	Selex ADS-B GS	Indra ADS-B GS	EUROCONTRL SDPD
1	Enhanced ADS-B target report validation via WAM integration	N	Y	N	Y
2	Behavioral Analysis of Targets	N	N	Y	Y
3	Time Differential of Arrival	Y	Y	N	Y

Table 6. Security enhancement incorporation within 2nd Prototype Iteration

3.2.3 Technology enhancement

Automatic network bandwidth optimisation techniques was the technology enhancement incorporated into the enhanced ADS-B groundstation within the 2nd Iteration enhanced ADS-B ground system. This was implemented by Thales and Indra [6].

3.3 Mapping of Security Enhancements between Iterations

Table 7 shows the mapping of security enhancements introduced into the 1st Prototype Iteration and their further development within the 2nd Prototype Iteration of the enhanced ADS-B ground system [6], [10]. It also shows the implementing ADS-B groundstation manufacturer against the selected security enhancement:

Item	Enhanced ADS-B Ground System Security Enhancements				
	1st Prototype Iteration	Imp. Man.		2nd Prototype Iteration	Imp. Man.
1	Simple ADS-B target report position validation via WAM target report comparison	T, S	➔	Enhanced ADS-B target report validation via WAM target report comparison	S
2	Track consistency verification (velocity versus position change).	T	➔	Behavioral analysis of targets	I
3	Use of increased timestamp accuracy for TOA functionalities	S	➔	Time Difference Of Arrival techniques	T, S
4	Power measurement vs range correlation	I			
5	Angle of arrival measurement	I			
6	Multi sensor data fusion consistency check	E			

Table 7. Development of enhancements from 1st to 2nd Prototype Iteration

NOTE 1: Imp. Man. = Implementing ADS-B Groundstation Manufacturer
NOTE 2: T = Thales S= Selex I = Indra

EUROCONTROL are not specified within the above table, as all selected enhancements were implemented into the ASTERIX interfaces and SDPD system (Tables 4 & 5).

It can be seen from Table 7 that security enhancements implemented in the 1st Iteration ADS-B groundstation have not necessarily been continued by the manufacturer into the 2nd Prototype and this decision is judged to be on the grounds of cost and implementation complexity.

4 2nd Iteration Security Enhancements

The following sub-sections describe selected security enhancements within the 1st Prototype Iteration of the enhanced ADS-B ground system and their subsequent development within the 2nd Prototype Iteration, incorporating new functionality into the ADS-B ground system.

4.1 ADS-B message validation via WAM integration

4.1.1 1st Prototype Iteration – Simple WAM Integration

The vast majority of ADS-B 1090 ES systems are deployed as part of a combined WAM and ADS-B systems. Such integration not only offers advantages of infrastructure sharing between the two surveillance technologies but also has the potential for improvement of the ADS-B integrity capability through comparison between WAM and ADS-B target data [2]. The objective of this activity was to provide protection against deliberate spoofing of ADS-B reported position information and hence implement improved integrity checking within the ADS-B ASTERIX CAT 21 target reports [13].

Within the enhanced ADS-B groundstation, each 1090 Extended Squitter ADS-B message received on the 'Air Interface' in the 'Antenna' Function is decoded within the '1090 ES Reception' function, as shown in Figure 2 and described within the ADS-B 1090 MHz Ext. Squitter Ground Station Specification - Iteration 1 [14]. ADS-B messages compliant to the new version of the ADS-B MOPS, ED-102A/DO-260B are extracted within all WP15.4.5b manufacturers 1st Iteration enhanced groundstations, as shown in Table 3. All decoded ADS-B messages are timestamped by the 'UTC Time Synchronisation' function within the ADS-B groundstation.

4.1.1.1 ADS-B horizontal position validation

All decoded ADS-B messages from the 1090 GS Reception are input into the 'ADS-B Data Validation' function shown in Figure 2. Those ADS-B messages containing aircraft horizontal position updates are set into a 'Pre-validated Position' state. All other ADS-B messages within the 1st Iteration ADS-B groundstation are passed to the 'Report Assembly' function for ASTERIX CAT 21 target report creation and broadcast.

The 1090 GS identifies WAM CAT 20 target reports with the same Mode S 24 bit address to the 'Pre-validation Position' ADS-B message and sets the one with closest time of applicability to the ADS-B 'Pre-validation Position' message as the WAM 'Reference Report' [14]. Horizontal position information within the ADS-B 'Pre-validated Position' message is compared to corresponding value in the WAM 'Reference Report' and if below a threshold then the WAM Integration (WAI) horizontal position test result is set to 'Valid'. If outside the threshold then the WAI test result is set to 'Not Valid'. If this process is disabled or if no suitable WAM 'Reference Report' is available then the WAI test result is set to 'Not Validated' [3].

The WAI horizontal position test result is communicated to the SDPD system through the modified ASTERIX CAT 21 I021/040, Target Report Descriptor Third Extension - Error Conditions 'WAI field' data item, as defined within the 1st Iteration Interface Specification [15] and associated modified ASTERIX Category 21 version 2.77 [17]. The WAI field is 2 bits in lengths, allowing four combinations of values. Inspection of the defined WAI states in ASTERIX CAT 21 specification demonstrates that only three are defined, with one set to 'reserved' status [17]. This undefined state is developed in Iteration Two (Section 4.1.2).

The setting of the CAT 20 'Reference Report' is controlled by a user definable threshold, which determines the maximum allowable time difference between the ADS-B and WAM target report for the comparison process to operate [3].

The above process is dependant on the ADS-B groundstation receiving valid WAM target data for comparison purposes. This is determined through inspection of the GO/NOGO status bit within the input ASTERIX CAT 19 WAM service message stream shown in Figure 2, by the groundstation ADS-B Data Validation function. If the status bit is set to GO then the WAI process is performed. If it is in the NOGO state then the process is suspended and the WAI result is set to Not Validated [3].

The SDPD takes into account the WAI status of ADS-B horizontal position target reports and uses this to identify potential spoofing when the WAM integration was not successful and the ADS-B target report could not be associated with an existing track. It will also encode the WAI status within the output ASTERIX CAT 62 target report data, which can be used to set an appropriate display symbol for validated or potentially suspicious ADS-B plot on the ATCO Common Working Position (CWP) display [16].

WAM integration testing within the 1st Iteration enhanced ground system is solely concerned with ADS-B horizontal position integrity. It is therefore proposed that the implemented WAI functionality is a security enhancement of ADS-B technology, as it enables the identification of ADS-B messages not associated with real aircraft within the ADS-B groundstation through comparison with the measured WAM target report aircraft position. The WAI test result status can be used by the SDPD system to either associate to the track and sets the flag (multi-sensor validation) or initiates a new track and sets the flag (other validations) and flag them appropriate i.e. through an particular symbol, when displayed to ATC controllers on the CWP display.

4.1.2 2nd Prototype Iteration – Enhanced WAM Integration

Within the 2nd Iteration Prototype, the WAM Integration comparison process was expanded to encompass the following 'pre-validated' ADS-B message types [3]:

- ADS-B Airborne Position Message – set to 'Pre-validated Position' ADS-B message
- ADS-B Airborne Velocity Message – set to 'Pre-validated Velocity' ADS-B message
- ADS-B Target State and Status Message – set to 'Pre-validated Status' ADS-B message
- ADS-B Surface Position Message – set to 'Pre-validated Surface' ADS-B message

For each one of the 'Pre-validated' ADS-B messages, a WAM CAT 20 target report is assigned 'Reference Report' status within the ADS-B Validation Function, if the WAM 'Reference Report' and ADS-B 'Pre-validation' message are within the defined Time of Applicability threshold [3].

Building on the approach developed for the 1st Iteration ADS-B horizontal position validation, further data validation comparison tests were defined within the 2nd Iteration 'ADS-B Validation' function [2]. These tests featured selected ADS-B data items extracted from the 'pre-validated' ADS-B messages and compared against the equivalent WAM 'Reference Report' parameter, using a definable threshold to determine the 'pass-fail' criterion.

Table 8 describes the ADS-B parameter under examination and also as shows the logical grouping of the performed tests into four Test groups:

i) Position Test,

ii) Altitude Test result,

iii) Velocity Test and

iv) Mode S Data Test [3]:

Test	ADS-B message type	WAM Integration threshold test	WAI Test Group
1	Pre-validated Position	ADS-B horizontal position vs WAM horizontal position	**Position Test**
2	Pre-validated Position	ADS-B Altitude vs WAM Measured Height (Local Cartesian Coordinates)	**Altitude Test**
3	Pre-validated Velocity	ADS-B Velocity over Ground vs WAM Calculated Track Velocity (Local Cartesian Coordinates)	**Velocity Test**
4	Pre-validated Velocity	ADS-B True Airspeed vs WAM True Airspeed extracted from BDS (5,0) Track and turn report	**Mode S Data Test**
5	Pre-validated Velocity	ADS-B North/South Velocity and Direction vs WAM True Track Angle and Ground Speed extracted from BDS (5,0) Track and turn report	**Mode S Data Test**
6	Pre-validated Velocity	ADS-B East/West Velocity and Direction vs WAM True Track Angle and Ground Speed extracted from BDS (5,0) Track and turn report	**Mode S Data Test**
7	Pre-validated Velocity	ADS-B Magnetic Heading vs WAM Magnetic Heading extracted from BDS (6,0) Heading and speed report	**Mode S Data Test**
8	Pre-validated Velocity	ADS-B Indicated Airspeed vs WAM Indicated Airspeed extracted from BDS (6,0) Heading and speed report	**Mode S Data Test**
9	Pre-validated Velocity	ADS-B Barometric Vertical Rate vs WAM Barometric Altitude Rate extracted from BDS (6,0) Heading and speed report	**Mode S Data Test**
10	Pre-validated Surface	ADS-B Heading/Ground Track and Movement against WAM True Track Angle and Ground Speed extracted from BDS (5,0) Track and turn report	**Mode S Data Test**
11	Pre-validated Surface	ADS-B Heading/Ground Track vs WAM Magnetic Heading extracted from BDS (6,0) Heading and speed report	**Mode S Data Test**
12	Pre-validated Status	ADS-B Selected Altitude vs WAM Selected Altitude extracted from BDS (4,0) Selected Vertical Intention	**Mode S Data Test**
13	Pre-validated Status	ADS-B Barometric Pressure Setting (BPS) vs WAM BPS extracted from BDS (4,0) Selected Vertical Intention	**Mode S Data Test**

Table 8. 2nd Iteration Pre-validation ADS-B message and WAM Reference report WAI tests

Note that the Velocity tests and Mode S tests Mode S MB data test cases 4-13 can only be performed if the WAM system is configured for Enhanced Mode S operation i.e. features an active interrogator.

Inspection of Table 8 demonstrates that each of the test(s) contribute to the setting of the respective Test group result in the manner:

- Test 1 sets the Position Test group result
- Test 2 sets the Altitude Test group result
- Tests 3 sets the Velocity Test group result
- Tests 4-13 sets the Mode S Data Test group result.

Each Test group result returns either a 'Suspicious' or 'Consistent' result [3]. These results are reported to the enhanced SDPD for processing through the modified ASTERIX CAT 21 I021/040, Target Report Descriptor Third Extension - Error Conditions 'WAI field' data item [5] and associated ASTERIX Category 21 version 2.79 [18], in the manner shown in Table 9:

Position Test Group Result	Velocity Test Group Result	Altitude Test Group Result	Mode S data Test Group Result	ATX 021 WAI bits
Consistent	Consistent	Consistent	Consistent	**00**
Not performed	Not performed	Not performed	Not performed	**10**
Consistent	Consistent	Consistent	**Suspicious**	**11**
			All other possible combinations	**01**

Table 9. ADS-B WAM Integration test results mapping to the WAI field

The four different validation results yielded the following WAI field settings [3]:

- 00 the report is VALID
- 01 the report is NOT VALID
- 10 the report is NOT VALIDATED
- 11 the report is VALID EXCLUDING MODE S DATA

Note that in the 2nd Iteration, the 'reserved' field from the 1st Iteration Prototype is now deployed to provide the 'Valid excluding Mode S Data' for SDPD processing. The inclusion of '11' WAI test result within the 2nd Iteration groundstation is because of the large number of data items contained within the Mode S Data Test, meaning that a small number of failures within this item should not set the result to a 'Not Valid' state and hence exclusion from the tracking process.

In the same manner as for the 1st Iteration, the SDPD can be configured to use the result of the WAI field to either associate to the track and sets the flag (multi-sensor validation) or initiates a new track and sets the flag (other validations) and indicate their status in the output ASTERIX CAT 62 target reports for appropriate display to ATC controllers on the CWP [4].

WAM Integration testing implemented within the 2nd Prototype Iteration enhanced ADS-B ground system is therefore proposed to be a security enhancement of ADS-B, as it provides an independent validation of the identification and position information content of the decoded ADS-B messages and enables reports which fall below the validation criterion to be either suppressed from the tracking process or display using appropriate symbology to the ATC controller, enabling these targets to be handled using the correct ATC procedures.

4.2 Behavioral Analysis of Targets

4.2.1 1st Iteration Velocity test

The 1st Prototype Iteration ADS-B groundstation featured functionality within ADS-B Data Validation function to verify that each velocity value reported within the ADS-B Velocity message matched the velocity value calculated from successive horizontal position updates. If the value was outside of a definable threshold then the result was tagged as 'Velocity Inconsistent', otherwise was tagged as 'Velocity Consistent' [14].

The above result was reported to the SDPD through the modified ASTERIX CAT 21 data item ASTERIX CAT 21 I021/040, Target Report Descriptor Third Extension - Error Conditions 'Position Velocity Check or PVC field' data item, as defined within the 1st Iteration Interface Specification [15] and associated modified ASTERIX Category 21 version 2.77 [17]. This again returns three values; Valid, Not Valid or Not validated, with the fourth set to reserved state as per the WAI field in the 1st Iteration ADS-B groundstation [17].

The SDPD takes into account the reported status of the PVC field in the tracking process, either associates to the track and sets the flag (multi-sensor validation) or initiates a new track and sets the flag (other validations) and flags them appropriately for CWP display within the ASTEROX CAT 62 target report. [16].

4.2.2 2nd Iteration Behavioural Analysis test

The Behavioural Analysis Test implemented in the 2nd Iteration ADS-B groundstation expanded 1st Iteration Velocity test to compass the following ADS-B parameter set [2], [6]:

1. Velocity (1st Iteration)
2. Acceleration
3. Acceleration Change
4. Heading
5. Heading Change
6. Altitude
7. Altitude Change
8. Vertical rate
9. Vertical Rate Change

Each parameter is examined to determine if it fell between a declared validity range, with the result declared as 'Consistent' if met, otherwise set to 'Inconsistent'. Each parameter test was enabled or disabled through a software switch [3]

The Behavioural Analysis test results are consolidated into an overall BAR test result [3]. The PVC field introduced within the 1st Iteration groundstation was replaced by the BAR field, described within the 2nd Iteration Interface Specification [5] and associated ASTERIX Category 21 version 2.79 [18].

The BAR field featured four states, in a similar manner to implemented 2nd Iteration WAI field:

- 00 Behaviour is VALID in all tests returned a 'Consistent' result
- 01 Behaviour is NOT VALID if any test failed i.e. Inconsistent
- 10 Behaviour is NOT VALIDATED if any of the above tests are not performed
- 11 Behaviour is 'VALID ONLY FOR A SUB-SET OF TESTS'

In the same manner as for the 1st Iteration, the SDPD uses the result of the BAR field to either associates to the track and sets the flag (multi-sensor validation) or initiates a new track and sets the flag (other validations) and indicate their status in the output ASTERIX CAT 62 target reports for appropriate display to ATC controllers on the CWP [4].

The Position Velocity Change test introduced within the 1st Iteration and developed into the Behavioral Analysis test in the 2nd Iteration is therefore proposed to offer security advantages to the enhanced ASDS-B ground system compared to an ADS-B groundstation developed to be compliant to ED-129. The new target report information within the PVC and BAR results enables the ARTAS SDPD system to identify potentially false ADS-B targets and process them according to the ANSP required configuration.

4.3 Time Differential of Arrival

4.3.1 1st Iteration Time of Arrival test

The 1st Iteration enhanced ADSB ground system specification defined a security enhancement to undertake ADS-B aircraft position validation through Time of Arrival (TOA) vs calculated aircraft distance test [13]. The ToA-distance test was designed to enable networked ADS-B groundstations to undertake aircraft position validation through the exchange of ADS-B information on aircraft detected in the common coverage volume between three or more ADS-B groundstations [3].

A networked ADS-B groundstation cluster is shown schematically in Figure 5:

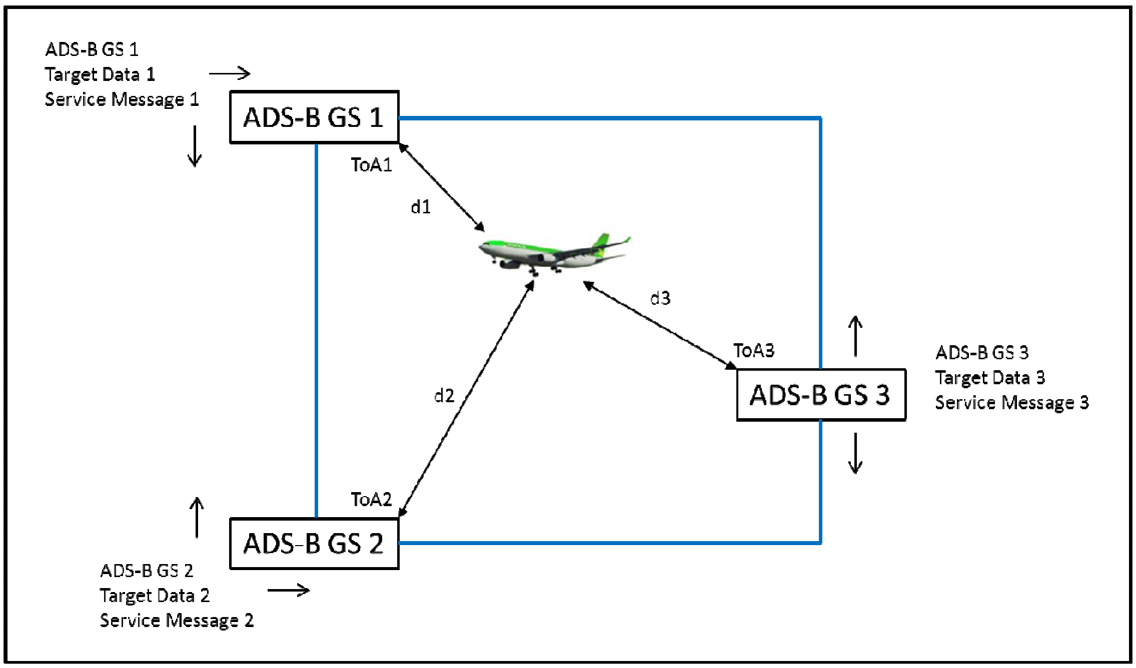

Figure 5. Time of Arrival horizontal position validation test schematic

The Time of Arrival test operates in a step-wise process and is actioned within the ADS-B Data Validation function within the enhanced ADS-B groundstation [3]:

1. Each enhanced ADS-B groundstation determines the aircraft slant ranged corrected distance from itself, using the reported ADS-B message horizontal position, reported aircraft altitude and the receiver surveyed position to calculate the distance. It should be noted that the ADS-B groundstation does not measure the aircraft position, but extracts and calculates it from the reported ADS-B message position information.

2. Each clustered ADS-B groundstation sends two data streams to other groundstations configured within the network:

Data Stream 1	ASTERIX CAT 21 target reports or manufacturer dependant raw ADS-B messages containing aircraft Mode S address, Time of Arrival ($ToA_{1,2,3}$) and calculate slant range corrected aircraft distance ($d_{1,2,3}$).
Data Stream 2	ASTERIX CAT 23 service messages or manufacturer specific groundstation Operational Status messages.

3. If the ADS-B Data Validation function receives target and service message streams from >= 2 ADS-B groundstations, in-addition to itself, then the ToA/Distance is performed. Likewise, >= 2 ADS-B data streams must indicate an Operational status for the ToA test to be performed.

4. If both above conditions are not met then the ToA test is not performed and the result is set to 'Not Validated'.

5. The ADS-B Data Validation function associates its own ADS-B target detections with ADS-B target reports received from different ADS-B groundstations featuring the same Mode S address into a ToA-Distance validation assessment group.

6. Each ToA-Distance assessment group is processed using the logical expression:

   'Time of Reception (Arrival) of position message from nearest ADS-B sensor <= ToR of second closest ADS-B sensor'

   and

   'Slant range corrected distance from nearest sensor <= Target distance from second nearest sensor'

   If the above condition is True then the ADS-B position data is declared as 'Valid'. Otherwise, it is set to 'Not Valid'.

The result of the ToA/Distance test is reported to the enhanced SDPD system through the modified ASTERIX CAT 21 data item ASTERIX CAT 21 I021/040, Target Report Descriptor Third Extension - Error Conditions 'Time of Arrival Validation or ToA' field, as defined within the 1st Iteration Interface Specification [15] and associated modified ASTERIX Category 21 version 2.77 [17]. The ToA field features the following conditions:

- VALID - Test is performed and data passes the validation criterion (step 4)
- NOT VALID – Test is performed and fails validation criterion
- NOT VALIDATED – Test is not performed (step 3)
- Reserved for future use.

The enhanced SDPD system is configured to use the result of the ToA field to either associate to the track and sets the flag (multi-sensor validation) or initiates a new track and sets the flag (other validations) and indicate their status in the output ASTERIX CAT 62 target reports for appropriate display to ATC controllers on the CWP [4].

The ToA/Distance test enables the enhanced ADS-B ground system to identify if the calculated aircraft distance from each ADS-B groundstation conforms to the expected Time of Arrival relationship and use this result to either track the target, filter them or and flag is as potentially false for display. This test is therefore proposed to be a security enhancement of ADS-B, as it enables ADS-B target reports not exhibiting the correct relationship i.e. potentially false messages to be identified and handled in an appropriate manner.

4.3.2 2nd Iteration Time Difference of Arrival test

The 2nd Iteration developed the concept of networked ADS-B groundstations validating ADS-B calculated horizontal position into the Time Difference of Arrival (TDOA) test. TDOA techniques are commonly used in Wide Area Multilateration (WAM) systems to measure aircraft horizontal position and in ICAO RVSM compliance Height Monitoring Systems to measure aircraft vertical height.

4.3.2.1 Time Difference of Arrival technique used in WAM systems

The principle of Time Difference Of Arrival is illustrated in Figure 6:

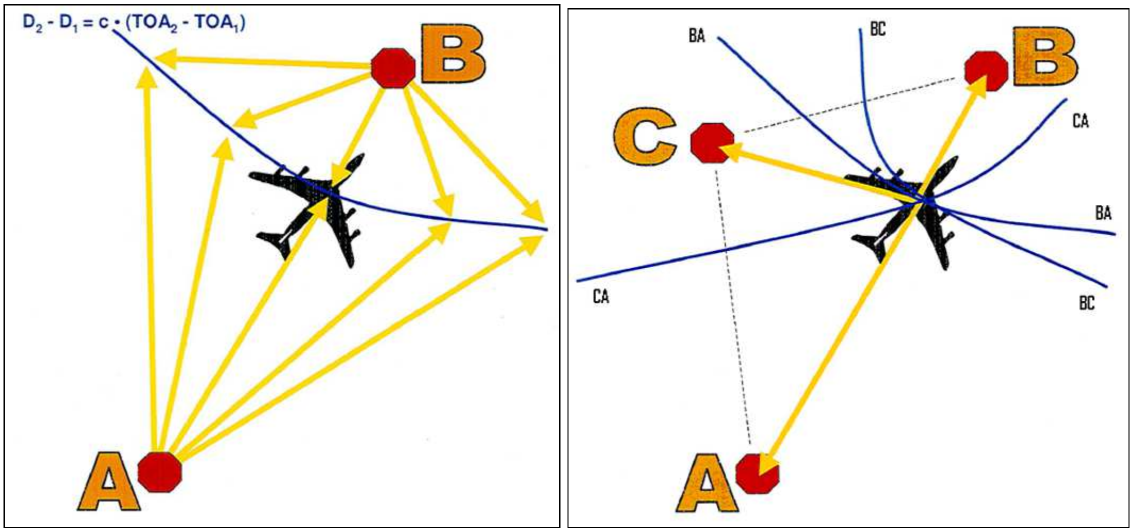

Figure 6. Principle of Time Difference of Arrival

The same 1090 Extended Squitter ADS-B message signal is detected, decoded and timestamped with a ToA value within each networked ADS-B groundstation. Each groundstation sends the others Mode S information and ToA values in ADS-B target messages and the ADS-B 'Data Validation Function' associates these into separate TDOA assessment groups, if they feature the same Mode S address [2].

The ADS-B Data Validation takes each TDOA assessment group target reports and calculates the location of the aircraft on a hyperbolic arc between selected pairs of ADS-B groundstations. This process is shown in the left hand diagram of Figure 6 for Groundstations A and B, using the relative TDOA- relative distance equation:

$$Arc\ \mathrm{BA} = D_2 - D_1 = c * (ToA_2 - ToA_1)$$

where c is the speed of light, $D_2 – D_1$ is the aircraft relative distance between Groundstations A and B, TOA_2 is the Time of Arrival of the signal at ground station B and ToA_1 is the Time of Arrival of the signal at ground station A.

Further groundstation pairwise calculations, as shown in the right hand diagram of Figure 6, allow the intersection point of multiple arcs to be determined (Arcs CA, BC, BA) and the collation of these points into a single solution generates the position measurement of the aircraft location. This is the TDOA technique a WAM system uses when measuring aircraft position.

It should be noted that high precision time-stamp units i.e. ~1ns, are required to effect the TDOA measurement technique, as an increase in the error of arrival time measurement for each RF pulse acts to decrease the accuracy of the determined aircraft position and hence position accuracy.

4.3.2.2 TDOA technique application with Enhanced ADS-B ground system

The TDOA test implementation within Iteration 2 ADS-B enhanced groundstation network was specified to operate using the minimum construction of a single TDOA arc, as shown in left hand diagram of Figure 6. This set a minimum requirement of 2 groundstations to form the ADS-B network and validate the reported 3D position through comparison with the hyperbolic arc position [3].

If the difference in positions was less then the defined threshold value then the test was declared as 'Valid' and reported to the SDPD system through the ToA Validation Result field, in the same manner as for the ToA test implemented in the 1st Iteration groundstation [18]. If less than two ADS-B groundstation were declared as operational within the network the test was suspended and the result 'Not Validated' returned to the SDPD [3] [18].

Again, the SDPD system uses the validation result to either associate to the track and set the flag (multi-sensor validation) or initiates a new track and set the flag (other validations) and report the status of the test to the end user in ASTERIX CAT 62 for display [2], [4].

The 2nd Iteration TDOA measurement of the aircraft location is an improvement on the 1st Iteration ToA/distance technique, as it validated the aircraft 3D position rather than 2D distance. It is proposed that it acts as a security enhancement of ADS-B, as it validates the aircraft position through a measurement process, rather than being solely dependant on the integrity of the ADS-B message itself.

5 Assumptions

N/A

6 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 15.04.05a SDPD Specification – Iteration 2, **D10** Ed 00.03.00, September 2011

[5] SJU 15.04.05a Interface Specifications for 2nd Prototype Iteration, **D11** Ed 00.01.00, October 2011

[6] SJU 15.04.05b 2nd Prototype Iteration – Baseline Report/Matrix, **D10** Ed 00.01.00, April 2013

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

[8] SJU 15.04.05b – Safety Assessment for 15.04.05b Prototype Second Iteration, **D15**, July 2013

[9] SJU 15.04.05b Safety Assessment for 15.04.05b Prototype First Iteration, **D08,** Ed 00.01.00, May 2012

[10] SJU 15.04.05b First Iteration – Baseline Report/Matrix, **D02** Ed 00.01.02, July 2012

[11] EUROCAE/RTCA SPR Document for ADS-B RAD Application, **ED-161**/DO-318, Sept. 2009

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

[13] ADS-B Ground Surveillance Specifications for First Iteration, **D18** Ed 00.01.00, Dec 2011

[14] ADS-B 1090 MHz Ext. Squitter Ground Station Specification - Iteration 1, **D05** Edition 00.02.00, March 2011.

[15] Interface Specifications for first iteration, **D07** Ed 00.01.00, March 2011.

[16] SDPD Specification - Iteration 1, **D06** Edition 00.01.00, March 2011

[17] EUROCONTROL STANDARD DOCUMENT FOR SURVEILLANCE DATA EXCHANGE Part 12 : Category 021 ADS-B Reports, SUR.ET1.ST05.2000-STD-12-01, Edition **2.77**

[18] EUROCONTROL STANDARD DOCUMENT FOR SURVEILLANCE DATA EXCHANGE Part 12 : Category 021 ADS-B Reports, SUR.ET1.ST05.2000-STD-12-01, Edition **2.79**

6.1 Use of copyright / patent material / classified material

No copyright/patent/classified material; is included in this report

-END OF DOCUMENT-