Safety Assessment for 15.04.05b Prototype Third 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 Third Iteration
Deliverable ID	Del 22
Edition	00.01.01
Template Version	03.00.00
Task contributors	
EUROCONTROL;INDRA;NATS;NORACON;SELEX;THALES	

Abstract

SESAR WP15.4.5 has the task of implementing enhancements into ADS-B ground surveillance system to address security limitations of ADS-B technology and to ensure compliance of the ground equipment to the latest ADS-B Airborne Equipment Minimum Operational Performance Specification (MOPS), ED-102A/DO-260B.

WP15.4.5b contains three ADS-B ground station suppliers; Thales Air Systems, Indra and Selex and one SDPD supplier, EUROCONTROL. Each supplier has made an implementation decision on incorporation of the active ranging ADS-B security enhancement into their element of the Prototype 3rd Prototype iteration enhanced ADS-B ground system.

This report articulates the outcome of a safety assessment conducted against the third iteration prototype security enhancements. The assessment identified a number of safety requirements to be satisfied by the implemented Enhanced ADS-B Ground Systems, and proposed two recommendations for optimisation of the system design.

Authoring & Approval

Prepared By		
Name & Company	Position & Title	Date
[redacted]	NATS [redacted]	19/11/2014

Reviewed By		
Name & Company	Position & Title	Date
[redacted] THALES	[redacted]	12/11/14
[redacted] INDRA		12/11/14
[redacted] THALES		12/11/14
[redacted] SELEX		12/11/14
[redacted] NORACON		12/11/14
[redacted] EUROCONTROL		12/11/14
[redacted] NATS		12/11/14
[redacted]		12/11/14

Reviewed By – *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date
[redacted]/NATS	[redacted]	31/10/14
[redacted]/Thales		31/10/14
[redacted]/NATS		31/10/14

Approved for submission to the SJU		
Name & Company	Position & Title	Date
[redacted] THALES	[redacted]	01/12/14
[redacted] INDRA		13/11/14
[redacted] NATS		13/11/14
[redacted] EUROCONTROL		02/12/14
[redacted] SELEX		13/11/14
[redacted] Noracon		19/11/14

Rejected By		
Name & Company	Position & Title	Date
None		

Rational for rejection
None.

Document History

Edition	Date	Status	Author	Justification
00.01.01	19/11/2014	Initial edition	[redacted]	First Draft

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

List of tables

List of figures

Executive summary

WP15.4.5 introduced technology enhancements (see Table 2-1) into ADS-B ground systems, the SDPD and their associated interfaces. The enhancements related to 7-individual tests, across three iterative prototypes introduced by three ADS-B OEMs; an addition test was included within the SDPD. Each ADS-B OEM was obliged to incorporate at least one enhancement. The ADS-B ground system outputs to the SDPD the results of the implemented tests as part of the ASTERIX category 21, where there are four possible results:

Test results	Field code	Description
Validated and valid	00	The enhancement check occurred validating the ADS-B data
Validated and not valid	01	The enhancement check occurred and did not validate the ADS-B data
Not validated	10	The enhancement check did not occur
Partially validated and valid (BAR)*	11	The enhancement check occurred and validating a sub-set of the ADS-B data
Valid except for Mode S (WAI)*		The enhancement check occurred but was unable validate Mode-S data
Reserved (all others)		Not a valid output

* Only behaviour analysis result (BAR) and WAM integration (WAI) validation results use this output

The SDPD response depends on the values set within the message, irrespective of the enhancement the SDPD responds the same way. For three of the four results, the SDPD can form new tracks where no existing tracks that are associated, or associate with existing tracks where they do exist. The exception to this, is the 'validated and not valid' results; the SDPD can still form a new track, but this will occur irrespective of current tracks that could be associated. This is summarised below:

Ground system result	Ground field code	Possible ARTAS response	
		New track*	Track association**
Validated & valid	00	Y	Y
Validated & not valid	01	Y	N
Not validated	10	Y	Y
Partially validated and valid (BAR)	11	Y	Y
Valid except for Mode S (WAI)			
Reserved (all others)			

*On first reception, ARTAS generates a new track if no tracks from other sensors are present to associated with, subsequent reports with the same values will be associated to this new track;
**Associates with an existing track if tracks from other sensors are present;

The SDPD has an additional security enhancement test, which compares to theoretical radar coverage, with the ADS-B track, where there is no correlation the SDPD, indicates a possible erroneous ADS-B track. The output from the SDPD is ASTERIX category 62 messages, which directly forwards the results from six of the ADS-B ground system tests along with the additional SDPD flag. The remaining seventh test is binary flag representation of the results (valid or invalid).

Additionally, the ADS-B ground system also outputs a service message stating whether a particular test was performed (where incorporated), for all tests these are binary flags '1' is active, '0' is inactive.

A failure modes and effects Analysis (FMEA) was performed against the proposed additions to identify any impact to 'pre-enhancement' SPRs by consideration, for example, of the reference sets, as well as any new SPRs incurred by the new functionality.

The resulting requirements have been specified in a manner allowing them to be 'relative' to any existing set. This has been done to avoid the introduction of 'compatibility' or 'translation' issues that would likely have followed from stating the new requirements against any particular scheme or method followed for the 'pre-enhancement' system. The security enhancements are judged not to comprise new safety functions, thus the recommendations and requirements identified by this report are chiefly concerned with the protection of extant safety functions.

The FMEA was a guideword driven activity with subject matter experts (SME) who provided domain knowledge of both the pre and post-enhancement ADS-B ground system and associated wider surveillance systems. The safety assessment further analysed safety dependencies derived against new or modified (by their design or by their use) inputs to the ADS-B ground system, for example, for their potential to invalidate downstream dependencies on function independence. The output of the FMEA identified the following requirements, assumptions and recommendations:

SR_01	It shall be demonstrated that the implementation of the security enhancements does not compromise the robustness of the extant ADS-B functionality.
SR_02	It shall be demonstrated that the implementation of the security enhancements satisfies the integrity targets as derived from treatment of their failure modes as potential causes to extant ADS-B system/service level hazards for credible but incorrect track data display.
SR_03	The implementation of the security checks at the enhanced ADS-B Ground System shall ensure that assembly of the reports output to the SDPD can integrate only those check results associated with any given report.
SR_04	Implementation of the security enhancements shall ensure that the enhanced ADS-B Ground system is unable to interfere with the interfacing WAM services (where applicable).
SR_05	An assessment shall be conducted for each deployment that intends to employ a WAM interface at the enhanced ADS-B Ground system that balances the potential for credible but incorrect data on that interface causing the enhanced ADS-B Ground System to inappropriately flag its output as 'invalid' against the mitigation for security threats that the WAM interface would afford.
SR_06	Demonstration that WAM inputs to the enhanced ADS-B Ground system (where applicable) are unable to cause loss of ADS-B output to the SDPD under all normal and credible failure cases for the WAM input shall be conducted to a level of confidence commensurate with the severity of the consequence from loss of both WAM and ADS-B inputs to the SDPD.
SR_07	Implementation of the '1030 interrogation' function (as part of the implementation of the 'Range from Active Interrogation' check), where applicable, shall conform with all relevant prescribed standards for that interface (e.g. ICAO Annex 10, Volume IV) (Ref: [13]).

ASSUM_01	It is assumed that the SDPD responses to the set of flags set by the enhanced ADS-B ground system security checks are assured as suitable and safe outside the scope of the WP15.4.5b assessment (including treatment of 'partial valid' and 'not validated' outputs as if 'validated & valid').
ASSUM_02	It is assumed that the means of display to air traffic control (ATC) of new or associated tracks under the 'not valid' case (including any indicators used to identify that status for the track) and any other associated user notifications (e.g. system alerts) are assured as suitable and safe outside the scope of the WP15.4.5b assessment.
ASSUM_03	It is assumed that the protection afforded to the ground system output during its onward transmission and subsequent processing is equally applicable to reports from both enhanced and non-enhanced ground systems, and that this protection is appropriate for the most safety-significant failure mode associated with that data (expected to be credible but incorrect aircraft position information).
ASSUM_04	It is assumed that none of the enhanced ADS-B ground system implementations introduce additional functionality beyond the specified security checks (e.g. no additional logging conducted).
ASSUM_05	It is assumed that a security check flag state of '11' in the ASTERIX CAT 21 output results in an SDPD response as defined for the flag states '00' and '10' for all specified checks.

Recommendation 1	Either (i) the 'default value' (i.e. the state reported in the ATX CAT 21 output unless otherwise revised by the Data Validation function) of the security check flags should be '10', 'Not Validated' OR (ii) the ATC CAT 21 '00' default state for the security check flags should be revised to correspond to 'Not Validated' (with the corresponding revision to the definition of the '01' state).
Recommendation 2	Assessment of a configuration to be employed for an enhanced ADS-B ground System deployment must be cognisant of the balance between correctly identifying invalid reports and causing unnecessary tracks / track statuses to be displayed to ATC. Such assessments must consider the 'performance' of the security checks in a given operational security environment, where that performance may be influenced by factors including, for example, (i) any check result aggregation, (ii) configured 'sensitivity' of the checks, (iii) configuration of flag 'persistence' required to enact a displayed state change.

Although the system as specified will work, recommendations are further proposed since it was viewed that the specified design may be sub-optimal.

1 Introduction

1.1 Purpose of the document

This document presents the approach taken by, and the results of, the safety assessment conducted for the ADS-B security enhancements proposed by 'WP15.4.5b Project Initiation Report (PIR): Surveillance Ground System Enhancements for ADS-B (Prototype Development)' (Ref: [1]).

Its outputs provide guidance to original equipment manufacturers (OEM) for the safe implementation of 15.4.5b ADS-B enhancements into their individual products.

1.2 Approach

1.2.1 Overview

WP15.4.5 is scoped to introduce technology enhancements into ADS-B ground systems and Surveillance data processing and distribution (SDPD) system and modified interfaces between the elements. These are collectively described as the enhanced ADS-B Ground System. This document describes the approach taken the required Safety Assessment against the enhanced ADS-B ground system developed within SESAR WP15.4.5b and its resulting outputs.

1.2.2 SESAR Safety Approach

WP16.06.01 has developed SESAR Safety Reference Material, Figure 1-1 is presented within document 16.06.01 D06-002:

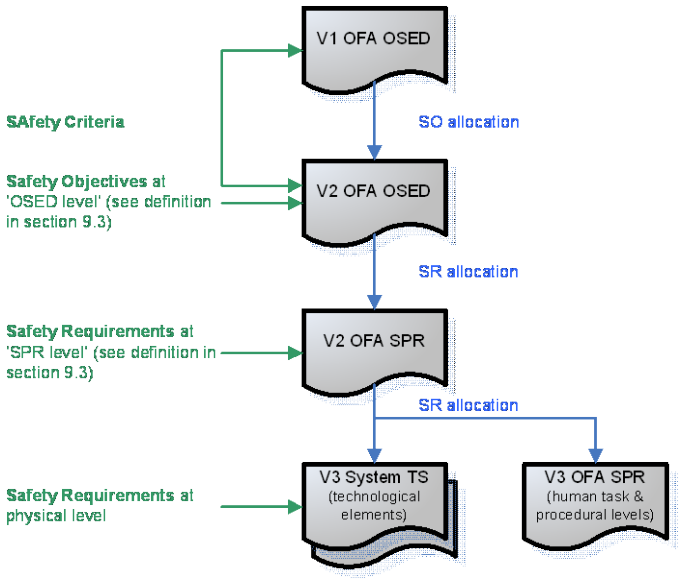

Figure 1-1 Safety Criterion, Objectives and Requirements cascade within SESAR

The Operational Focus Area sets the top level safety criterion for the selected operational improvements and environment and these flow down to safety objectives and Requirements at the V2 operating environment level then into the equipment at the V3 physical level. WP15.4.5b is devised as V3 level project within the European operational concept validation methodology (E-OCVM), as it develops Pre-Industrialisation Prototype systems. Within SESAR, it delivers a technology element in support of higher V1 and V2 levels.

1.2.3 WP15.4.5 links to Operational Focus Areas

Project scope for WP15.4.5 was defined within the over-arching 'Specification Baseline Document, D17 Edition 00.01.00, which suggested Operational Projects and hence Operational Focus Areas which were expected to provide input requirements for the project to incorporate within the different iterations of the ADS-B ground system development.

Using the logical path defined for SESAR Safety Requirements definition at an equipment level specified in Figure 1, it would be expected that the operational focus area (OFA) level projects would set safety criterion (SAC), which would be translated into Safety Objectives and Requirements at the V2 level and therefore into equipment level Safety Requirements i.e. enhanced ADS-B ground system.

Review of documentation within the suggested Operational Projects revealed **no** linkage to WP15.4.5, which is reflected within WP15.4.5 specifications that use legacy EUROCAE ADS-B Ground system safety & performance requirement (SPR) documents i.e. ADS-B RAD ED-161 (Ref: [2]) and ADS-APT ED-163 (Ref: [3]) as the source for performance and safety requirements for the enhanced ADS-B ground system design. Due to this lack of linkage between active Operational Projects and WP15.4.5, guidance was sought from WP16.06.1 on the appropriate source of safety requirements for consideration within the design of the enhanced ADS-B ground system.

The project manager indicated that the GEN SUR SPR (Ref: [4]) document under preparation by the EUROCONTROL CASCADE through EUROCAE WG5 SG4 should be used as the V2 SPR material for the source of ground function Safety Requirements.

However, as the security enhancements do not in-of-themselves introduce new safety functions, the outputs of the safety assessment, which are chiefly concerned with the protection of *extant* safety functions, were specified in a manner allowing them to be 'relative' to any existing set. This was done to avoid the introduction of 'compatibility' or 'translation' issues that would likely have followed from stating the new requirements against any particular scheme or method followed for the 'pre-enhancement' system.

1.3 Structure of the document

Executive Summary			
Section	1	Introduction	Defines the objective of the document and the process involved.
Section	2	Proposed Security Enhancements	Provides an high-level of the security enhancements descriptions for both ground system and ARTAS.
Section	3	Safety Assessment	Describes the approach employed and outlines the results.

1.4 Functional Block Overview

This section provides an overview of the enhanced ADS-B ground system and the SDPD as specified in the WP15.4.5b security assessment for 15.04.05b 3rd prototype iteration Ref: [5].

1.4.1 Enhanced ADS-B ground system overview

The primary functions of the enhanced 1090 ADS-B Ground system as per ADS-B surveillance system specification system specification Ref: [6] are:

- Receive 1090 MHz radio frequency (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 universal time constant (UTC) time synchronisation 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;
- Interacts with the Remote Control and Monitoring system through the Management Interface, using simple network management protocol (SNMP) messaging protocols;
- Determines the internal status of the ground system equipment through built in test equipment (BITE);

A functional block diagram of the 1090MHz ground system is shown in Figure 1-2.

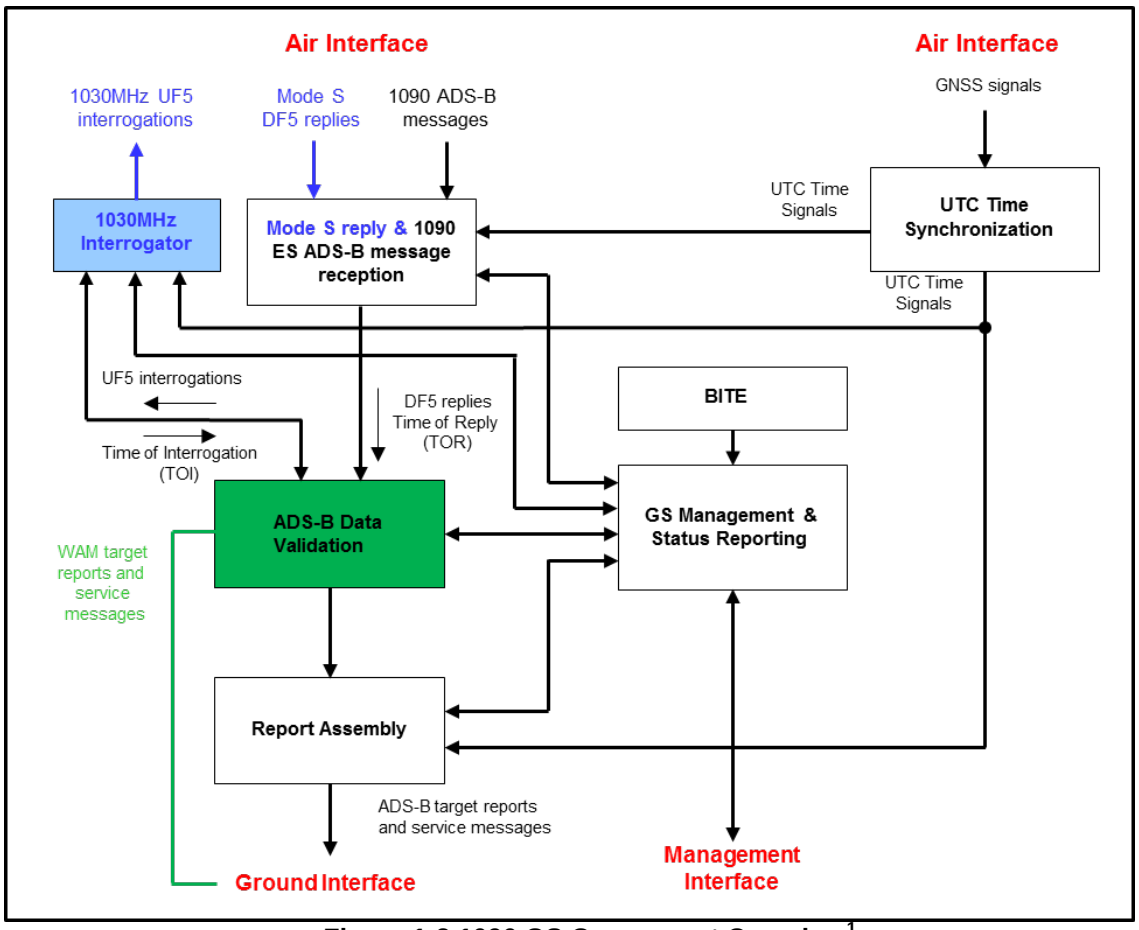

Figure 1-2 1090 GS Component Overview[1]

In comparison with the functional blocks specified against the basic ADS-B-RAD ground system in ED-129 (Ref: [7]) it is noted that the ADS-B Data Validation functional block (in green) has been added incorporating the additional security enhancement functionality, along with a 1030MHz interrogator (in blue).

1.4.2 SDPD system overview

The SDPD receives aircraft data from individual surveillance sensors, including ADS-B 1090 MHz ES ground system, and serves fused surveillance track updates to client systems such as controller working position (CWP). 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.

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 (wide area multilateration (WAM)) and 021 (ADS-B) target messages and fused into a composite air picture. 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.

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

The EUROCONTROL ARTAS product was selected as the SDPD element within the enhanced ADS-B system and is designed around four main functions as defined in Ref: [6]:

- 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 1-3.

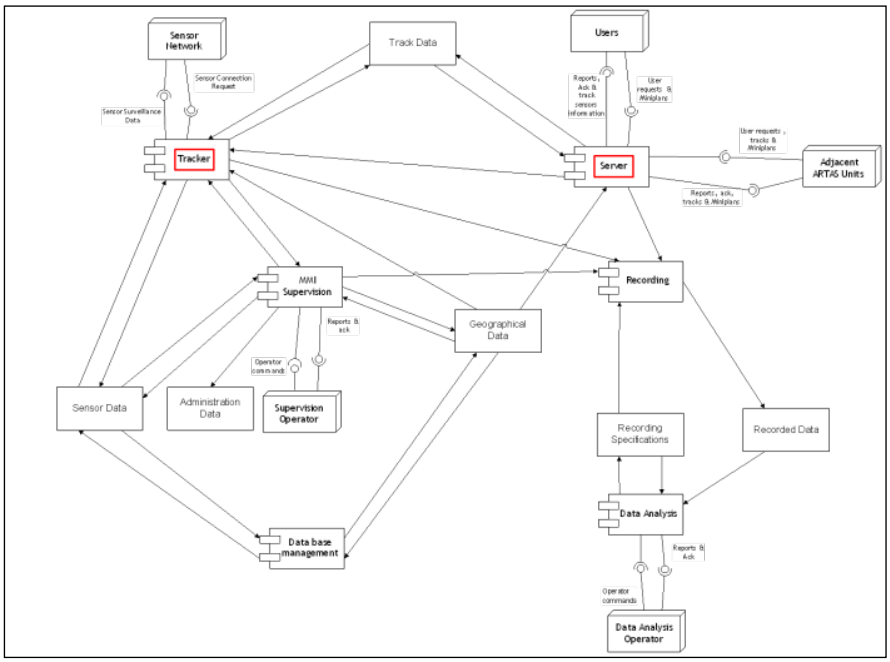

Figure 1-3 ARTAS functional overview

1.5 Glossary of terms

ADS-B ground station	A standalone ADS-B receiver within no connectivity or cognisance of other ADS-B receivers,
ADS-B ground system	A group of receivers coupled together in order to facilitate the networking for implemented security enhancements

1.6 Acronyms & Terminology

Term	Definition
ADS-B	Automatic dependent service broadcast
AoA	Angle of arrival validation result
ATC	Air traffic control
BAR	Behaviour analysis result
BITE	Built in test equipment
CWP	Controller working position
E-OCVM	European operational concept validation methodology
ES	Extended squitter
FMEA	Failure modes and effects analysis
GNSS	Global navigation system services
MSV	Multi-sensor validation
OEM	Original equipment manufacturer
OFA	Operational focus area
PRV	Power/range validation result
RAI	Range from active interrogation
RF	Radio frequency
SAC	Safety criterion
SARP	Standards and recommended practices
SDPD	Surveillance data processing and distribution
SME	Subject matter experts
SNMP	Simple network management protocol
SPR	Safety & performance requirement
TDoA	Time difference of arrival
TLA	Three letter acronym
TMA	Terminal manoeuvre area
ToA	Time of arrival validation result
UTC	Universal time constant
WAI	WAM integration validation result
WAM	Wide area multilateration

2 Proposed Security Enhancements

2.1 Overview

The generation of positional and identification data by ADS-B relies on the use of both global navigation system services (GNSS) and aircraft avionics. Hence, ADS-B is inherently vulnerable to both intentional and unintentional manipulation resulting in the generation of erroneous positional data. To mitigate this potential issue, a number of security enhancements have been proposed within WP15.4.5 to validate the ADS-B position data, using the same ADS-B signals, providing a level of increased confidence.

SESAR WP15.4.5b (see Ref: [5], [8] & [9]) was tasked with the implementation of enhancements into the ADS-B ground based surveillance system to address security and integrity ADS-B technology limitations. It is planned that the enhancements will offer a surveillance service that augment existing radar services in High Density terminal manoeuvre area (TMA) airspace and offer standalone services in lower density operating environments. WP15.4.5b developed three pre-industrialisation prototype enhanced ADS-B ground systems, termed the 1st, 2nd and 3rd iteration. This report covers all implemented security enhancements for the ADS-B grounds receive system.

2.2 ADS-B Ground system Security Enhancements Description

2.2.1 Implemented Security Enhancements

WP15.4.5b details three ADS-B ground system OEMs who have implemented selected security enhancements in their prototype iterations enhanced ADS-B ground systems, as detailed in Table 2-1. As part of their involvement in the project, ground system OEMs had to implement at least one security enhancement, although some chose to implement more. A number of enhancements implemented in the first iteration were updated or replaced with modified or improved enhancements. Several enhancements were implemented by more than one OEM.

Item No.	Security Enhancement	TLA	Thales ADS-B GS	Selex ADS-B GS	Indra ADS-B GS
1st Prototype Iteration Security Enhancements					
1.	Simple ADS-B target report position validation through WAM target data comparison	WAI*	Y	Y	N
2.	Angle of Arrival measurement	AoA	N	N	Y
3.	Position change vs velocity check	BAR**	Y	N	N
4.	Power measurement vs range correlation	PRV	N	N	Y
5.	Time of Arrival vs Aircraft Calculated Distance from ADS-B GS Validation	TOA	N	Y	N
2nd Prototype Iteration Security Enhancements					
6.	Enhanced ADS-B target report validation via WAM integration	WAI*	N	Y	N
7.	Behavioral Analysis of Targets	BAR**	N	N	Y
8.	Time Differential of Arrival	TDOA	Y	Y	N
3rd Prototype Iteration Security Enhancements					
9.	Range measurement from active interrogation	RAI	Y	Y	Y

* Item 6 replaces item 1 due to further development of Item1; **item 7 replaces item 3 due to further development of Item 3;

Table 2-1. Security enhancement incorporation within prototype Iteration

2.2.2 ADS-B Ground system Outputs

The data is output from the ADS-B sensor in ASTERIX category 21, item 40, 'target report descriptor' as the 3rd, 4th and 5th extension of the primary subfield, see §5.2.5 of Ref:[10].

		Bits							
	Bit	8	7	6	5	4	3	2	1
Error conditions	3rd extension	0	BAR		ToA		WAI		FX
	4rd extension	0	TDoA		AoA		PRV		FX
	5th extension	0	0	0	0	0	RAI		FX

Table 2-2 Category 21 output message format

Where the field codes in Table 2-4 and Table 2-2 are defined in Table 2-3

BAR	Behaviour analysis result	Possible results as per Table 2-4
ToA	Time of arrival validation result	
WAI	WAM integration validation result	
TDoA	Time difference of arrival validation	
AoA	Angle of arrival validation result	
PRV	Power/range validation result	
RAI	Range from active interrogation	
FX	File extension indication: 0 indicates end of data and 1 indicates extension into the next extent	

Table 2-3 Field codes

The security enhancements each have a 2-bit output as detailed in Table 2-4. Each test outputs these in separate message formats as per Table 2-2.

Validated and valid;	00	The enhancement check occurred validating the ADS-B data
Validated and not valid;	01	The enhancement check occurred and did not validate the ADS-B data
Not validated	10	The enhancement check did not occur
Partially validated and valid (BAR)	11	The enhancement check occurred and validating a sub-set of the ADS-B data
Valid except for Mode S (WAI)		The enhancement check occurred but was unable validate Mode-S data
Reserved (all others)		Not a valid output

Table 2-4 Security enhancement test result flags

Bits 7/6 (BAR) indicate the result of an internal validation of the contents of the ADS-B data by comparing with the targets behaviour. It verifies that the parameter derived from the target's performance (e.g. heading, velocity, rate of vertical movement and others) match the ADS-B report. The value "11" indicates that target data has been validated against target behaviour but that only a subset of behavioural data was available so not all tests could be executed.

Bits 3/2 (WAI) indicate the result of a validation of the target report with data coming from a WAM application providing data to the ADS-B ground domain. The value "11" indicates that the validation was successful but that either no Mode S MB data was available or that the validation with available Mode S MB data failed. While FX represent the file extension, where 'indicates' end of data item and a '1' indicates the relevant file extension (3rd, 4th or 5th), this is present in every octet. Irrespective of the test employed, the ground system will output the flags as detailed in Table 2-4 to the SDPD, which needs to interpret the results and act accordingly.

2.3 SDPD Security Enhancements Description

2.3.1 ADS-B Ground system Checks

On receipt of the ASTERIX category 21 message from the ADS-B ground system, the SDPD, response depends on the flag values within the message. Irrespective of the enhancement used, for a given enhancement result (e.g. 00, 01, 10, 11), the SDPD responds the same way. For three of the four results, the SDPD forms new tracks where there are no existing tracks that are associated.

The exception to this, is the 'validated and not valid' (01) results, where the SDPD can still form a new track, but this will occur irrespective of current tracks that could be associated. Table 2-5 presents the possible behaviours that may occur depending upon on the enhancement results.

Ground system result	Ground system output	Possible ARTAS response	
		New track*	Track association**
Validated & valid	00	Y	Y
Validated & not valid	01	Y	N
Not validated	10	Y	Y
Partially validated and valid (BAR)	11	Y	Y
Valid except for Mode S (WAI)			
Reserved (all others)			

*Generates a new track if no tracks from other sensors are present to associated with;
**Associates with an existing track if tracks from other sensors are present;

Table 2-5 SDPD usage of ground system flags

Amplifying on Table 2-5, an invalid output ('not validated and valid') from an ADS-B ground system can only result in a new track being formed, irrespective if there is an existing track available that it may have associated with. Whereas all other outputs from the ADS-B ground system can associate with existing tracks if the validation flags of the report, match with those of the track or, where the report has flags set to valid, which are presently invalid in the track.

Where the SDPD initiates a track from an ADS-B report, it will retain any associated flag provided by the ADS-B ground system, which will be forwarded to the user. These flags are used to decide if an ADS-B report is associated or not and will be forwarded to the user to indicate a potential spoofing event. If the ADS-B report indicates potential spoofing and the corresponding track does not, the ADS-B report will not be associated, but will initiate a new track indicating potential spoofing.

ADS-B-only tracks that are updated by ADS-B reports that are not validated will have the corresponding flags set. If a doubtful ADS-B report is associated to existing true tracks, the track attributes and track states could be manipulated, e.g. the track position may be influenced by the ADS-B report and may no longer reflect the true position. This safety risk is avoided by not associating the report, but by initiating a new track instead.

However, if the existing track has the same flags set or the report has flags set to valid which are invalid in the track, the report is associated to avoid initiating a new track for each report. The flag reset will only occur when they are no longer set in the associated ADS-B reports for a configurable duration.

2.3.2 SDPD Multi-Sensor Validation Check

The SDPD also performs a security enhancement check called multi-sensor validation (MSV). In the event that a track is only updated by an ADS-B report, where the horizontal position of that track is

within the theoretical coverage of an active radar feeding the multi-sensor tracker, the MSV test indicates that the multi-sensor validation has failed and that the ADS-B track may be a false target. In areas where the radar is unable to detect flights, such as the cone of silence or terrain masking, this function may raise false alarms. The MSV is single bit flag, located in bit-2 of the sixth extension.

2.3.3 SDPD Security Enhancement Outputs

The data is output from the ADS-B sensor in ASTERIX category 62, item 80, 'target report descriptor' as the 5th, 6th and 7th extension of the primary subfield, see §5.2.6 of Ref:[11], with the format as per Table 2-6, with the outputs as defined in Table 2-7.

		Bits							
	Bit	8	7	6	5	4	3	2	1
Error conditions	5th extension	IEC	BAR		ToA		WAI		FX
	6th extension	TDoA		AoA		PRV		MSV	FX
	7th extension	0	0	0	0	0	RTD		FX

Table 2-6 SDPD outputs

Validated and valid;	00	The enhancement check occurred validating the ADS-B data
Validated and not valid;	01	The enhancement check occurred and did not validate the ADS-B data
Not validated	10	The enhancement check did not occur
Partially validated and valid (BAR)	11	The enhancement check occurred and validating a sub-set of the ADS-B data
Valid except for Mode S (WAI)		The enhancement check occurred but was unable validate Mode-S data
Reserved (all others)		Not a valid output

Table 2-7 SDPD output options

The field codes are as for Table 2-3, with the addition of:

IEC*	Default value = 0	Inconsistent emergency code = 1
MSV		Multi sensor validation failed = 1
RTD**		RTD validation failed

* This is not a security enhancement and is not covered any further in this document
** RTD is round trip delay, which replacesthe terminology for RAI;

2.4 Service Message Modifications

To support the security enhancements, the service messages have been modified. Within the enhanced ADS-B ground system design, ASTERIX category 023 for service messages had a single data item changed to incorporate the status of the active 'security enhancement' checks. Table 2-8 shows the service message contents, where the results are as shown in Table 2-9.

	Bits							
Bit	8	7	6	5	4	3	2	1
Octet 2	SC			WAI	TOA	PRV	BAR	FX
2nd extension	0	RAI	WDS	TDoA	LAL		AoA	FX

SC = service class; LAL = Active load adaptation level, neither associated with the enhancment checks

Table 2-8 Service message format

WAI	0 = not active 1 = active
TOA	
PRV	
BAR	
FX	
TDoA	
AoA	

Table 2-9 Message results

Therefore, the number of reported tests matches the total number of security enhancements within the ground system within CAT 23 in the 3rd Iteration design. The resultant output only indicates that a particular security enhancement is enabled and not that it has been performed. Service messages go to the SDPD, but are not used as part of the health check upon the security enhancement outputs.

3 Safety Assessment

3.1 Approach Introduction

An assessment of the ADS-B Security Enhancements proposed by WP15.4.5b project initiation report (Ref: [1]) was conducted on 09 September 2014, as documented in the resulting meeting minutes (Ref: [12]), §3.3 consist of an extract of the meeting minutes.

The workshop comprised two stages:

First, a Failure Modes Effect Analysis (FMEA) of the functions to be implemented under WP15.4.5b;

Second, a structured brainstorm of the impact of the Enhancements' implementation on the wider Surveillance system operation;

In particular, this second assessment was intended to capture where the change may invalidate pre-existing assumptions (explicit or otherwise) made for, or undermine safe behaviour of, the pre-Enhancements system.

A FMEA is a structured, systematic and comprehensive examination of a design to identify and document undesirable system behaviour. The approach is based on exploiting the knowledge and experience of the personnel present in a structured manner to identify and analyse potential hazards. Each function to be implemented for the Security Enhancements was considered step-by-step by application of guideword prompts, as listed below.

Guidewords	**Meaning / *notes***
Happens	*Considers if correct operation of the function is inherently hazardous.*
Fails to happen	The function fails to operate.
Incorrect	The function fails to operate correctly; incorrect, corrupt or partial output.
Early	The function takes place earlier than intended, either in 'relative' terms of a sequence of activities or in 'absolute' terms against a system 'clock'.
Late	The function takes place later than intended, either in 'relative' terms of a sequence of activities or in 'absolute' terms against a system 'clock'.
Duplicated	The function occurs more often than intended for a given initiating event.
Other	*Any other behaviour of the function the workshop could identify that hasn't been captured under the other guidewords.*

3.2 Requirements, Assumptions and Recommendations

For ease of reference, the following sub-sections collate all entries made during the meeting.

3.2.1 Requirements

SR_01 It shall be demonstrated that the implementation of the security enhancements does not compromise the robustness of the extant ADS-B functionality.

SR_02 It shall be demonstrated that the implementation of the security enhancements satisfies the integrity targets as derived from treatment of their failure modes as potential causes to extant ADS-B system/service level hazards for credible but incorrect track data display.

SR_03 The implementation of the security checks at the enhanced ADS-B Ground System shall ensure that assembly of the reports output to the SDPD can integrate only those check results associated with any given report.

SR_04 Implementation of the security enhancements shall ensure that the enhanced ADS-B Ground System is unable to interfere with the interfacing WAM services (where applicable).Ground system

SR_05 An assessment shall be conducted for each deployment that intends to employ a WAM interface at the enhanced ADS-B Ground System that balances the potential for credible but incorrect data on that interface causing the enhanced ADS-B Ground System to inappropriately flag its output as 'invalid' against the mitigation for security threats that the WAM interface would afford.

SR_06 Demonstration that WAM inputs to the enhanced ADS-B Ground System (where applicable) are unable to cause loss of ADS-B output to the SDPD under all normal and credible failure cases for the WAM input shall be conducted to a level of confidence commensurate with the severity of the consequence from loss of both WAM and ADS-B inputs to the SDPD.

SR_07 Implementation of the '1030 interrogation' function (as part of the implementation of the 'Range from Active Interrogation' check), where applicable, shall conform with all relevant prescribed standards for that interface (e.g. ICAO Annex 10, Volume IV (Ref: [13])).

3.2.2 Assumptions

ASSUM_01 It is assumed that the SDPD responses to the set of flags set by the enhanced ADS-B ground system security checks are assured as suitable and safe outside the scope of the WP15.4.5b assessment (including treatment of 'partial valid' and 'not validated' outputs as if 'validated & valid').

ASSUM_02 It is assumed that the means of display to air traffic control (ATC) of new or associated tracks under the 'not valid' case (including any indicators used to identify that status for the track) and any other associated user notifications (e.g. system alerts) are assured as suitable and safe outside the scope of the WP15.4.5b assessment.

ASSUM_03 It is assumed that the protection afforded to the ground system output during its onward transmission and subsequent processing is equally applicable to reports from both enhanced and non-enhanced ground systems, and that this protection is appropriate for the most safety-significant failure mode associated with that data (expected to be credible but incorrect aircraft position information).ground system.

ASSUM_04 It is assumed that none of the enhanced ADS-B ground system implementations introduce additional functionality beyond the specified security checks (e.g. no additional logging conducted).

ASSUM_05 It is assumed that a security check flag state of '11' in the ASTERIX CAT 21 output results in an SDPD response as defined for the flag states '00' and '10' for all specified checks.

3.2.3 Recommendations

Recommendation_1 Either (i) the 'default value' (i.e. the state reported in the ATX CAT 21 output unless otherwise revised by the Data Validation function) of the security check flags should be '10', 'Not Validated' OR (ii) the ATC CAT 21 '00' default state for the security check flags should be revised to correspond to 'Not Validated' (with the corresponding revision to the definition of the '01' state).

Recommendation_2 Assessment of a configuration to be employed for an Enhanced ADS-B Ground System deployment must be cognisant of the balance between correctly identifying invalid reports and causing unnecessary tracks / track statuses to be displayed to ATC. Such assessments must consider the 'performance' of the security checks in a given operational security environment, where that performance may be influenced by factors including, for example, (i) any check result aggregation, (ii) configured 'sensitivity' of the checks, (iii) configuration of flag 'persistence' required to enact a displayed state change.

3.3 Meeting record

3.3.1 Introductions & Clarifications

Round-the-table introductions were conducted, with following people present:					
Volker Seidelmann	VS	Thales	Bob Hromadka	BH	Thales
Neil Gardner	NG	NATS	Andy Scott	AS	NATS
Richard Hayward	RH	NATS	Nick Young	NY	NATS
AS presented the Briefing Material in order to establish a common understanding amongst attendees of the nature of the changes and the scope of the assessment to be conducted.					
VS identified that the 'Time of Arrival Validation' check required a minimum of 2 ADS-B ground system outputs.					
VS identified that the Thales Enhanced ADS-B ground system included an 'ADS-B Server', performing data validation checks on the output from connected ADS-B ground systems. The output comprises 'combined' (for that ground system) ASTERIX CAT 21 & 23 reports.					
BH identified that the 'ADS-B Server' may be implemented as a redundant pair, such that if 'Server A' fails, 'Server B' is able to take over.					
VS and NG stated that they believed the architecture of the Indra implementation closely matched that described by VS for the Thales system. They further stated that they understood that the Selex implementation has Data Validation checks conducted at the ground system, with a given ground system acting as the 'master' in any network of multiple ground systems.					
It was agreed that the 'ADS-B network' interface, illustrated in the hand-out as an external interface to a given ground system, should be identified as an internal interface within the wider Enhanced ADS-B Ground system, whereas the WAM interface remained an external interface.					
The meeting agreed that the revised understanding of the Enhanced ADS-B Ground system architectures would not significantly impact the intended approach for the safety assessment, which was to be conducted against a given function irrespective of where it was physically implemented. AS noted that it may influence arguments on the partitioning of the new functions from existing ADS-B functionality, but that – where found to be necessary – any associated requirements or recommendations raised by the workshop would be stated so as to be 'implementation agnostic'.					
Subsequent to the workshop, during review of the resulting minutes and this safety report, it was further identified that implementation of the 'Range from Active Interrogation' check introduces a new '1030 Interrogation' air interface.					

3.3.2 ADS-B Ground Functionality

These points resulted in revised illustrations for the 'Enhanced ADS-B Ground system' and the wider system context in which it sits as shown at Figure 3-1 and Figure 3-2, respectively.

In comparison with the functional blocks specified against the basic ADS-B-RAD ground system in ED-129 Ref: [6] it is noted that the ADS-B Data Validation functional block has been added incorporating the additional security enhancement functionality. Additionally, aspects of the 'Report Assembly' function may also be performed by the '1090 ES Reception' function for provision of ATX CAT 21 reports to the 'ADS-B Validation' function – implementation dependent. Certain validation checks may instead employ 'raw' ADS-B output. Furthermore, '1030 interrogation' capability is implementation dependent. Where not implemented, the air interface is unidirectional.

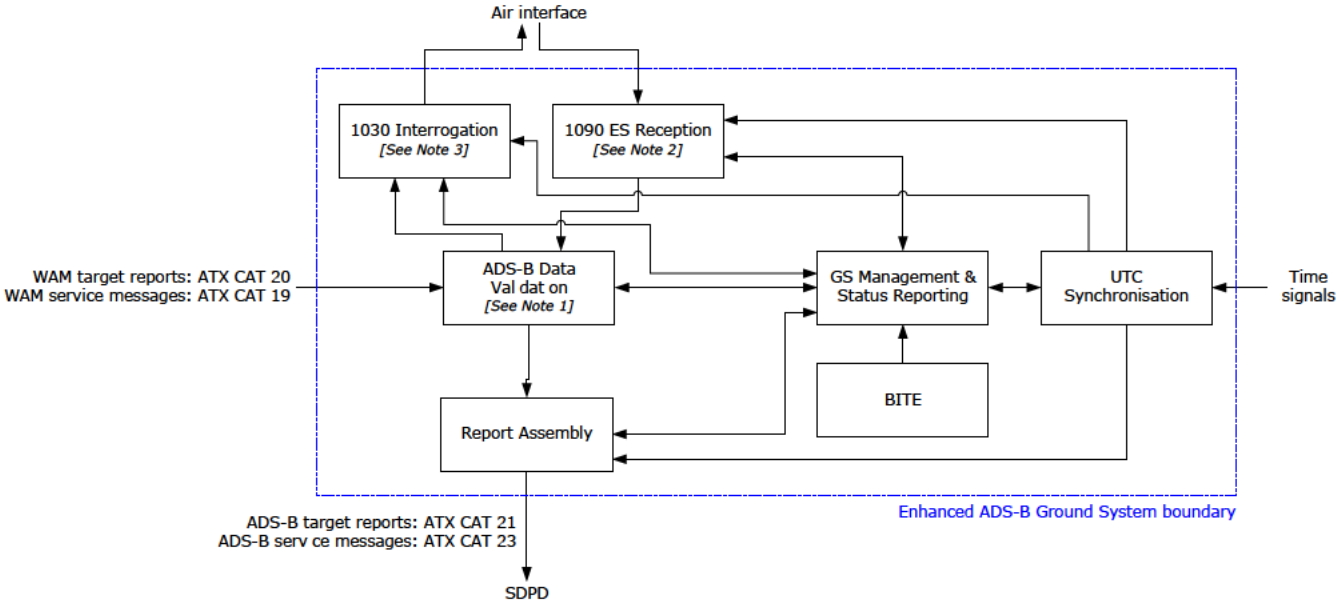

Figure 3-1 Enhanced ADS-B ground system

3.3.3 ADS-B Ground system

Where the security enhancements require networking capability between ADS-B ground systems to facilitate the security enhancements, the workshop agreed that the functional context and description must be modified to capture such a change. Hence, the ADS-B ground system terminology needs to be modified to 'ADS-B ground system'. This change allowed the workshop (et al) to capture the enhancements and their associated enablers, such as appropriate report assemblers.

Figure 3-2 depicts the ADS-B ground system context and data flow, where the scope of WP15.4.5b is defined via the blue (inner) dashed line. The workshop was performed on this basis.

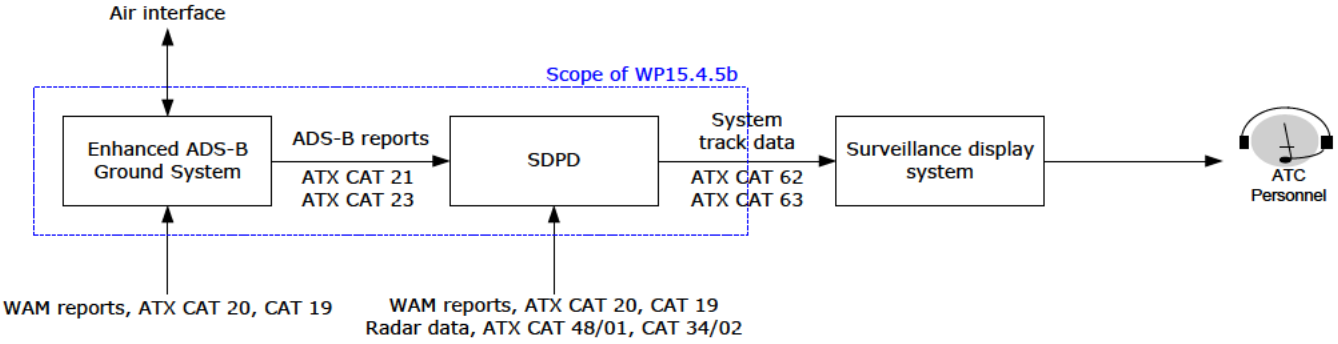

Figure 3-2 Enhanced ADS-B ground System context

3.3.4 Failure Modes and Effects Analysis

The meeting did not make any changes to the proposed guide word set. The record of the safety assessment of the functions introduced for the Security Enhancements is provided at 3.4. As a result of discussions on the changes to the 'Report Assembly' function as required to accommodate the introduction of the 'Data Validation' function, this function was also assessed following consideration of the individual security checks.

The meeting then considered if the introduction of the WAM interface to the ADS-B Ground system had the capacity to undermine any pre-existing assumptions or dependencies (explicit or otherwise) made for the pre-Enhancements system. It was identified that it had the potential to introduce a common cause failure between the WAM and ADS-B components of a supported service. Two mechanisms for this were identified:

1.	Failure of the ADS-B Ground system causing failure of the WAM system, by means of data transmission over the new interface. The meeting identified no need for the interface to be bi-directional. A safety requirement was raised to ensure provision of a suitable control against this potential failure mode. It was noted that this could be achieved in a number of ways (e.g. network traffic control) and that the requirement should not be solution-specific. ***SR_04**: Implementation of the security enhancements shall ensure that the enhanced ADS-B Ground system is unable to interfere with the interfacing WAM services (where applicable).*
2.	Failure of the WAM system causing failure of the ADS-B Ground system, by means of the new interface. a. Failure of the WAM system that provided credible but incorrect data to the ADS-B Ground system could cause the associated security check flag to be set to '01: Validated & not valid' inappropriately. A new, non-associated track would be generated with the corresponding 'check failed' status. In the case where the incorrect WAM data was similarly provided to the SDPD (with no mitigation of that failure by the SDPD), the ADS-B generated track may be presented to ATC as 'suspect' whereas the WAM generated / supported track may not. While hazards will already be identified for a service so-supported to the effect of 'credible but incorrect surveillance data', the failure state is now altered by a potentially misleading 'qualifier' of the ADS-B track that may hamper ATC diagnosis and response to the system state. ***SR_05**: An assessment shall be conducted for each deployment that intends to employ a WAM interface at the enhanced ADS-B Ground system that balances the potential for credible but incorrect data on that interface causing the enhanced ADS-B Ground System to inappropriately flag its output as 'invalid' against the mitigation for security threats that the WAM interface would afford.*
	b. WAM input to the ADS-B Ground system that is, for example, non-valid, out of range, etc. may cause failure of Ground system that system if a corresponding susceptibility is introduced by the changes made for the security enhancements. This failure mode often referred to as the 'poison pill' problem. This failure mode has the potential to cause loss of both the WAM and affected ADS-B inputs (as experienced by the SDPD), if the WAM input able to cause this failure is treated as invalid by the SDPD and discarded. This failure is particularly significant to the ATS if persistent. ***SR_06**: Demonstration that WAM inputs to the enhanced ADS-B Ground system (where applicable) are unable to cause loss of ADS-B output to the SDPD under all normal and credible failure cases for the WAM input shall be conducted to a level of confidence commensurate with the severity of the consequence from loss of both WAM and ADS-B inputs to the SDPD.*

A second external interface change was identified during review of the meeting minutes and this Safety Assessment Report. Implementation of the 'Range from Active Interrogation' check introduces a new '1030 Interrogation' air interface, as represented at Figure 3-1. The assessment provided, below, for this interface was subsequently approved by workshop attendees during review of Issue 2 of the minutes.

The 1030Mhz interrogation is an implementation of a widely used interface that is required to conform to – as a minimum - the relevant standards and recommended practices (SARPs) from ICAO Annex 10 Volume IV Ref: [13]. It is assessed, therefore, that this interface does not necessitate specific safety requirements beyond adherence to the relevant extant specifications in order for the potential impact on aircraft from its introduction by the security enhancements to be adequately controlled.

SR_07 Implementation of the '1030 interrogation' function (as part of the implementation of the 'Range from Active Interrogation' check), where applicable, shall conform with all relevant prescribed standards for that interface (e.g. ICAO Annex 10, Volume IV (Ref: [13])).

It further remains necessary to ensure that the extant ADS-B ground station functions are also not compromised by its introduction. This falls within the scope of safety requirement SR_01 (see §3.4), as the new interface is delivered by implementation of the 'Range from Active Interrogation' check.

3.4 Assessment Record

Ref.	Item / Function	Guideword	Failure mode clarification (if required)	Potential cause(s)	Effect(s)		Mitigation(s)
					Local	End	
1	Data Validation: 'Behaviour Analysis' check	Happens	N/A	N/A – 'as designed'.	N/A	N/A	N/A
2		Fails to happen	See 'Effect(s)'.	• Hardware failure. • Implementation (e.g. code) error.	'Default state' left on associated flag. No further effect in the absence of a security threat – SDPD specified to treat 'Valid' and 'Not Validated' outputs in the same way.	For subsequent use of ASTERIX CAT 21 output, SDPD would use ADS-B report to generate track / in track association (where applicable). *In the presence of an active security threat* (i.e. function fails to occur and so does not flag a report as 'Validated & Not Valid'), this could cause the subsequent display of a track to ATC to be credible but incorrect (either in terms of its reported position and/or track status). Potential associated loss of ATC confidence in use of the system. The meeting noted that ED-161 identifies this state (broadly corresponding to either OH05 or OH06 depending on the number of aircraft impacted) as having the potential to yield a 'Severity Class 1' outcome, but assesses that the 'Class 2' outcome drove the associated target occurrence rate. If only the ASTERIX CAT 23 entry for the check was not updated (so potentially left as '0: Not Active'), any downstream system which used the CAT 23 flags to determine use of the associated CAT 21 results would incur the same effect as above. NG noted that the ARTAS specification indicated that ARTAS does not use the revised CAT 23 output for this purpose. The meeting identified a concern that the implied default states for the CAT 21 and CAT 23 flags was '00: Validated and valid' and '0: Not Active', respectively. It was considered more appropriate for the default CAT 21 flag to be 'Not validated', with action required by the Enhanced ADS-B Ground System to revise this state. This would then avoid any risk associated with the status of a given report being misrepresented by a downstream system. ***RECOMMENDATION_1****: Either (i) the 'default value' (i.e. the state reported in the ASTERIX CAT 21 output unless otherwise revised by the*	See recommendation in 'Effect(s)'. Function development under appropriate design practises (e.g. coding standards). The meeting noted that, unless an argument was made that the new functions were adequately partitioned from extant ADS-B functionality, their implementation would be required to show that the robustness of those extant functions had not been compromised, in addition to demonstrating that the robustness of the functions themselves was sufficient. This latter consideration is then dependent on whether the assessment for a given deployment treats security threats as valid causes to a 'safety' hazard. Where this is the case, the integrity targets associated with correct completion of the new functions would be driven by that for the most significant extant ADS-B functions (for which their failure would now be a potential cause). ***SR_01****: It shall be demonstrated that the implementation of the security enhancements does not compromise the robustness of the extant ADS-B functionality.* ***SR_02****: It shall be demonstrated that the implementation of the security enhancements satisfies the integrity targets as derived*

Ref.	Item / Function	Guideword	Failure mode clarification (if required)	Potential cause(s)	Effect(s)		Mitigation(s)
					Local	End	
						Data Validation function) of the security check flags should be '10', 'Not Validated' OR (ii) the ATC CAT 21 '00' default state for the security check flags should be revised to correspond to 'Not Validated' (with the corresponding revision to the definition of the '01' state).	*from treatment of their failure modes as potential causes to extant ADS-B system/service level hazards for credible but incorrect track data display.*
3		Incorrect	Check flagged as 'invalid' when not.	• Implementation (e.g. code) error. • 'Sensitivity' of parameter configuration. • Incorrect / inappropriate logic employed for check result 'aggregation'.	Flag set to '01' incorrectly.	Unnecessary presentation of new, non-associated track to ATC or, (when ADS-B present as 'single source'), track inappropriately flagged as having failed security checks. ATC workload impact to resolve. Potential impact to pilot workload for responding to ATC queries. The meeting noted that ED-161 identifies this state (broadly corresponding to either OH09 or OH10 depending on the number of aircraft impacted) as having the potential to yield a 'Severity Class 3' outcome ("significant workload impact") for the case where multiple aircraft were impacted. The meeting identified that, when considering logic employed for aggregating the results for multiple ground systems, or 'sensitivity' of parameters set for a given check, there was the potential to alter the distribution between 'valid when not' and 'invalid when not' reporting states. An example discussed was for a simple 'voting' logic. Output behaviour would likely differ if a report were to be flagged as 'invalid' if the 'sub-result' from '1 out of 5' ground system checks came back as invalid, as compared to logic that instead required '4 out of 5' sub-results to come back as invalid in order to generate an 'invalid' combined result. The aggregation method employed would (in part) be balancing the need to avoid unnecessary 'split track' behaviour vs. the need to correctly identify invalid data. VS further identified that behaviour at the SDPD would similarly influence how these two outcomes would result, when considering how often a state would need to 'persist' for before the SDPD updated the associated track. For	See above.

Ref.	Item / Function	Guideword	Failure mode clarification (if required)	Potential cause(s)	Effect(s)		Mitigation(s)
					Local	End	
						example, on receipt of a report flagging an 'invalid' check result, does the SDPD immediately update the associated track (which may lead to a rapid 'toggling' between two states displayed to ATC if a security check flag was changing often), or does it require the result to remain 'invalid' for a given duration / number of reports? ***RECOMMENDATION_2***: *Assessment of a configuration to be employed for an Enhanced ADS-B Ground System deployment must be cognisant of the balance between correctly identifying invalid reports and causing unnecessary tracks / track statuses to be displayed to ATC. Such assessments must consider the 'performance' of the security checks in a given operational security environment, where that performance may be influenced by factors including, for example, (i) any check result aggregation, (ii) configured 'sensitivity' of the checks, (iii) configuration of flag 'persistence' required to enact a displayed state change.*	
4			Check flagged as 'valid' or 'not validated' when not.		See 'End'.	As identified at 'Fails to happen'. In the presence of an active security threat, this could cause the subsequent display of a track to ATC to be credible but incorrect.	-
5			ASTERIX CAT 23 flag for check status incorrect		ASTERIX CAT 23 flag for check status incorrect	See discussion on effect of incorrect ASTERIX CAT 23 output under 'Fails to happen'. Not significant while SDPD does not use CAT 23 flags to determine use of associated CAT 21 results.	-
6		Early	N/A	Not considered a credible failure mode.	N/A	N/A	N/A
7		Late	Late calculation / presentation of security check result	Function performance (coding error, under-specified platform resource)	If conduct of the check was 'late', such that the associated CAT 21 report was released 'without'	See 'Fails to happen'. SR_01 addresses this concern (where poor 'performance' of the Data Validation function must not degrade the robustness of the extant ADS-B functions). The meeting discussed what the state of a given check's flag should 'default' to if the checks did	-

Ref.	Item / Function	Guideword	Failure mode clarification (if required)	Potential cause(s)	Effect(s)		Mitigation(s)
					Local	End	
					the results, the effects would be as assessed for 'Fails to happen'.	not complete 'on time' before report release by the Report Assembly function (where permitted to do so prior to result receipt). The meeting considered both a default state as well as use of the 'previous state' until a state change was reported (either at the Ground System or by the SDPD). It was concluded that the Ground System behaviour recommended by Recommendation_1 was appropriate, and that SDPD behaviour had been appropriately recommended as part of Recommendation_2.	
8			Results for check on a given report <*M*> are added 'late' to a subsequent report <*M + n*>	-	Potentially as for 'Incorrect', in the presence of an active security threat.	The meeting identified the potential for implementing the 'Report Assembly' and 'Data Validation' functions independently as well as an integrated function. The latter could cause distribution of the entire ASTERIX CAT 21 report to be delayed on delay calculating the security check results. The former could give rise to inappropriate 'collating' of results and report. A safety requirement (SR) was proposed to address this case. ***SR_03***: *The implementation of the security checks at the enhanced ADS-B Ground System shall ensure that assembly of the reports output to the SDPD can integrate only those check results associated with any given report.*	See 'Effect(s)'.
9		Duplicated	-	A coding error leading to check 'loops' was briefly discussed but not considered to be a cred ble failure mode. Thought l kely to lead to check failure than duplicated output, but would be expected to be caught during system verification.	-	-	Function development under appropriate design practises (e.g. coding standards).
10		Other	N/A	N/A	N/A	N/A	N/A
11	Data Validation: remaining checks	Happens	NG raised a concern that the ARTAS specification did not clearly state the resulting (SDPD) behaviour after receipt of a '11' state security check flag for all check types. ***ASSUM_05***: *It is assumed that a security check flag state of '11' in the ASTERIX CAT 21 output results in an SDPD response as defined for the flag state '00'*				
12		Fails to happen					

Ref.	Item / Function	Guideword	Failure mode clarification (if required)	Potential cause(s)	Effect(s)		Mitigation(s)
					Local	End	
13		Incorrect	*and '10' for all specified checks.* Owing to SDPD behaviour being specified as common for each 2bit check flag, the meeting did not assess that there would be any significant difference between the results of the analysis for 'Behaviour Analysis' (as above) and the remaining checks. Incorrect external data input (i.e. WAM reports) was highlighted as not being employed by all checks, so would be identified as a 'Potential cause' to only a subset. See section 3.3 for wider consideration of the 'architectural' implications of the addition of the WAM interface. The meeting considered whether a surveillance display system would ever be specified / adapted to discard tracks which had an associated 'security check invalid' flag, i.e. track discarding beyond the behaviour specified for the SDPD. It was noted that any decision in this regard, while outside the scope of WP15.4.5b, would be necessarily influenced by the 'trade off' between display of spurious split / statused tracks to ATC (and resulting workload increase) vs. avoidance of presentation of credible but incorrect track data owing to an active security threat. Similar to the concerns that gave rise to recommendation 2, this would have to include assessment of the 'performance' of the security checks themselves (i.e. detection of security threads vs. 'false positives') and a range of potential operational security environments.			
14		Early					
15		Late					
16		Duplicated					
17		Other					
18	Report assembly (as modified for the Enhancements)	Happens	N/A	N/A – 'as designed'.	N/A	N/A	N/A
19		Fails to happen	-	• Hardware failure. • Implementation (e.g. code) error.	Missing ASTERIX CAT 21 and/or 23 output.	Consequence would be environment dependent (e.g. if used supplementary to radar or if ADS-B use was as 'sole source').	See requirements stated at 'Behaviour Analysis: Fails to happen'.
20		Incorrect	-	As above.	See 'End'.	Incorrect track data to Controller. Consequence severity as identified for that case (i.e. pre-Enhancement system state) dependent on environment.	See 'Fails to happen'.
21		Early	-	Not considered credible.	N/A	N/A	N/A
22		Late	-	Function performance (coding error, under-specified platform resource)	See 'End'.	Not considered significant to scope of this assessment – existing requirements cover use of timestamps to ensure data used by downstream systems is 'current'. Those requirements are not changed by introduction of the Enhancements (and so must be maintained).	See 'Fails to happen'.
23		Duplicated	-	None discussed.	See 'End'.	Not considered significant to scope of this assessment – concern is same as that for the 'pre-Enhancements' system.	See 'Fails to happen'.
24		Other	N/A	N/A	N/A	N/A	N/A

4 References

[1] WP15.4.5b Project Initiation Report (PIR): Surveillance Ground System Enhancements for ADS-B (Prototype Development)

[2] EUROCAE safety performance and interoperability requirements document for ADS-B-RAD application, ED-161, Sept. 2009

[3] EUROCAE safety performance and interoperability requirements document for ADS-B airport and surface surveillance (ADS-B-APT), ED-163, Dec 2010

[4] Safety and performance requirements document on a generic surveillance system supporting air traffic control services Gen Sur SPR Draft

[5] SJU WP15.4.5b security assessment for 15.04.05b 3rd prototype iteration 2014 **D23**

[6] SJU 15.04.05a ADS-B Surveillance System Specification. for Third Iteration, **D20**

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

[8] SJU WP15.4.5b security assessment for 15.04.05b 1st prototype iteration 2011 **D18**

[9] SJU WP15.4.5b security assessment for 15.04.05b 2nd prototype iteration 2013 **D16**

[10] EUROCONTROL standard document for surveillance data exchange, part 12, category 021 ADS-B reports

[11] EUROCONTROL standard document for surveillance data exchange part 9, category 062, SDPS track message

[12] WP15.4.5b: ADS-B Security Enhancements Safety Assessment 09-Sep-2014 Meeting Minutes, SESAR/SAF/01, Issue 2

[13] ICAO Annex 10, Volume IV: Surveillance and Collision Avoidance Systems Fifth ed., inc. admts 70-89

-END OF DOCUMENT-