INDUSTRIAL RESEARCH

sesar JOINT UNDERTAKING

D12.3.120 - PJ.14-W2-84c-TRL6- Final TS/IRS - Secured Surveillance Systems (Single and Composite Systems)

Deliverable ID:	**D12.3.120**
Dissemination Level:	**PU**
Project Acronym:	**PJ.14-W2-I-CNSS**
Grant:	**874478**
Call:	**H2020-SESAR-2019-1**
Topic:	**SESAR-IR-VLD-WAVE2-12-2019**
Consortium Coordinator:	**Leonardo**
Edition Date:	**06 December 2022**
Edition:	**00.01.01**
Template Edition:	**02.00.06**

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Authoring & Approval

Authors of the document

Beneficiary	Date
Thales	06.12.2022
Indra	06.12.2022
ENAIRE	06.12.2022
Eurocontrol	06.12.2022

Reviewers internal to the project

Beneficiary	Date
Thales	06.12.2022
Indra	06.12.2022
ENAIRE	06.12.2022
Eurocontrol	06.12.2022

Reviewers external to the project

Beneficiary	Date

Approved for submission to the S3JU By - Representatives of all beneficiaries involved in the project

Beneficiary	Date
Thales	06.12.2022
Indra	06.12.2022
ENAIRE	06.12.2022
Eurocontrol	06.12.2022

Rejected By - Representatives of beneficiaries involved in the project

Beneficiary	Date

Document History

Edition	Date	Status	Beneficiary	Justification

EUROPEAN PARTNERSHIP

Co-funded by the European Union

00.01.00	16.09.2022	final	Thales	Version for submission to SJU
00.01.01	06.12.2022	final	Thales	Version for submission to SJU covering additional comments

PJ.14-W2-I-CNSS

PJ.14-W2-84C-TRL6- NEW USE AND EVOLUTION OF COOPERATIVE AND NON-COOPERATIVE SURVEILLANCE - SECURED SURVEILLANCE SYSTEMS (SINGLE AND COMPOSITE SYSTEMS)

This Final TS/IRS is part of a project that has received funding from the SESAR3 Joint Undertaking under grant agreement No 874478 under European Union's Horizon 2020 research and innovation programme.

Abstract

This technical specification (Final TS/IRS) defines functionality, interfaces and performance requirements for security functions of secured surveillance systems with the specific focus on cooperative and cooperative dependent surveillance ground sensors (ADS-B/WAM). These enable the operational use of these security functions. It covers the sensor based radio frequency related threat detection and validation capabilities, security function performance requirements (mainly in terms of missed detection and false alarm) and definition of interoperable detection forwarding mechanisms. Related to target threat detection forwarding a specific ASTERIX target validation message is proposed and included in this specification. Through the defined detection performance and interoperable interface definition the sensor based security functions are expected to allow the use of ADS-B as an independent surveillance layer in high density airspace. This work is the continuation of the SESAR1 Project 15.04.06 and SESAR2020 Wave 1 PJ14-04-03 T05.
In 15.4.6 threat definition and classification and initial indications were developed. SESAR2020 W1 PJ14-04-03 T05 expanded the development to improve the security functions, performed an initial assessment of the operational performance of the security functions and studied the behaviour of the system in long periods. As the result of Wave 1 maturity level of TRL4/V2 was achieved.
The present specification is related to the increase of the maturity to TRL6.

All these activities are in accordance with impact in SESAR 2020 architecture and its definition, meeting the requirements of PJ19 (Content Integration).

The TS/IRS is composed of different parts.

- Part I covers the main body of the Technical Specification / Interface Requirement Specification.
- Part III covers the Security Assessment Report (SeAR) that describes the security assessment work done for the SESAR Solution. Note that the Part III is confidential and not part of the solution data-pack.

Table of Contents

Abstract 4
1 Executive summary 7
2 Introduction 8
2.1 Purpose of the document 8
2.2 Scope 8
2.3 Intended readership 9
2.4 Background 9
2.5 Structure of the document 12
2.6 Glossary of terms 12
2.7 Acronyms and Terminology 13
3 SESAR Solution Impacts on Architecture 18
3.1 Target Solution Architecture 18
3.2 Changes imposed by the SESAR Solution on the baseline Architecture 25
3.3 Analysis of security functions 25
4 Technical Specifications 28
4.2 Functional architecture overview (general introduction for all solutions) 41
4.3 Functional and non-Functional Requirements 57
5 Recommendation for Implementation 84
6 Assumptions 85
7 References and Applicable Documents 86
7.1 Applicable Documents 86
7.2 Reference Documents 87
Appendix A Service Description Document (SDD) 88

List of Tables

Table 1: Glossary 13
Table 2: Acronyms and terminology 17
Table 3: SESAR Solution PJ.14-W2-84c Scope and related Functional Blocks/roles & Enablers 18
Table 5: SESAR Solution PJ.14-W2-84c Operational Improvement Steps 18
Table 5: List of Capability Configuration required for the SESAR Solution 25

EUROPEAN PARTNERSHIP
Co-funded by the European Union

Table 6: List of changes due to the SESAR Solution 25

List of Figures

Figure 3-1: Operational view / use case for surveillance security functions 19

Figure 4-1 Target Threat Classification..... 28

Figure 4-2 System Threat Classification 28

Figure 4-3: Security threat distribution in the surveillance systems..... 42

Figure 4-4: Generic ATC-architecture security function..... 42

Figure 4-5 Resource Connectivity Model NSV-1 45

Figure 4-6 Resource Infrastructure view NSV-2 46

Figure 4-7 Resource Orchestration View 47

Figure 4-8 Resource Connectivity Model NSV-2 49

Figure 4-9: System Interfaces Diagram 53

EUROPEAN PARTNERSHIP

Co-funded by the European Union

1 Executive summary

PJ.14-W2-84c intends to develop a set of requirements for security functions in Ground Surveillance Systems (ADS-B /WAM). These security functions are defined in the present technical specification (Final TS/IRS) in terms of functionality for security threat detection, interfaces / interoperability and performance in terms of integrity, time-to-alarm, continuity and accuracy. In previous SESAR activities, work was focused on the feasibility to detect and indicate threats at sensor level and subsequently on the determination of a security threat detection performance. In this project, the team will focus on maturing the previous work to a pre-industrial prototype of a ground surveillance sensor with proven security performance able to forward detect security threats along the surveillance chain.

The present document describes the security threats from EUROCONTROL GEN-SUR SEC document (Ref. [17]), defines security threat detection and threat handling requirements and provides security threat detection performance needs. The security functions provided by the secured surveillance are intended to make the information provided by the surveillance sensors – with special focus on ADS-B – more trustworthy. ADS-B systems with security features are seen as solution for high density airspace allowing to gain operational benefits like high nominal accuracy, high update rate and provision of additional information by using ADS-B as independent surveillance layer. This functionality increases safety through increased security. In this context it shall be noted that the solution has no negative safety impact, in case of solutions degradation/unavailability. Degradation/unavailability are handled like with any other sensor mainly through (internal) redundancy and fall-back processes.

Within PJ.14-W2-84c it is intended to achieve a maturity level of TRL6.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

2 Introduction

This project is part of the SESAR 2020 Wave 2 Multi Annual Program for the period 2020-2022. It is part of the Industrial Research & Validation phase, developed under the SJU Private Public Partnership.

Communications, Navigation and Surveillance (CNS) systems provide the invisible and often unappreciated infrastructure which is essential for Air Traffic Management. CNS enables efficient navigation and safe separation in all phases of flight.

In Surveillance, solutions will be developed to enhance, harmonize and integrate cooperative and emerging non-cooperative sensors, advanced multi-sensors data fusion capabilities, security related functionality together with the methods and tools for Surveillance Performance Monitoring.

The solutions target Maturity TRL6 at the end of Wave 2.

PJ.14-W2-84c will

- Substantiate material driving the security function performance requirements and assessment methods.
- Implement security target threat validation information in the related prototypes technical specifications.
- Perform validation for TRL6 maturity of the prototypes.

2.1 Purpose of the document

The objective of the document is to provide functional, performance and interface requirements related to SESAR 2020 PJ.14-W2-84c.

This document aims at following the recommendations of previous SESAR projects (SESAR1 15.4.6 D08 [16] and SESAR2020 Wave 1 PJ14-04-03 T05 [23]) and at creating new requirements associated to new threats or new functions for the threat detection and information distribution.

New information developed within the Wave 2 is added.

2.2 Scope

This TS/IRS covers functional, non-functional and interface requirements related to SESAR2020 PJ.14-W2-84c.

This is the TS/IRS document for PJ.14-W2-84c achieving TRL6, once verification and validation activities have been finalised executing the defined Exercises (Thales exercises):

- EXE1: – TRL6, Validation of Integrity, Continuity, Time-to-Alert and Accuracy of Secured Surveillance Systems; 22-08-2022

Co-funded by the European Union

This document addresses new security functionalities for ground surveillance sensors of different nature, with the aim to detect, and report the existence of them to system users.

Information on security performance values is provided.

The document gives a more detailed description of the analysed threats and describes their associated requirements for threat detection and reporting.

Most of the threats covered by this document have been extracted from the GEN-SUR Security Risk Assessment document [17], developed by EUROCONTROL. The threats original numeration, defined on the GEN-SUR-SEC [17], has been kept throughout this document.

This document uses as input the corresponding document from Wave 1 [23] expanded for the Wave 2 for the TRL6 Validation:

- The key addition is the use of the ASTERIX target validation message ASTERIX CAT 246. This message was defined as a result of the TRL4 work where the lack of a standardised interface to report target validation information became apparent. The ASTERIX CAT 246 is still prototypic. The number was provided by the ASTERIX management group for the purpose of definition of a prototype. The specification for ASTERIX CAT 246 was prepared by DFS and is given in this document.
- The second relevant change is related to specific security performance requirements which have been established based on the results of the TRL4 validation in Wave 1.

2.3 Intended readership

The audience of this document includes:

- SESAR 2020 Wave 2 Surveillance solutions within Solution 84
- SESAR 2020 PJ 19: Content integration;
- SESAR 2020 PJ 20: Master Plan maintenance;
- EUROCAE WG51-SG4: Composite ADS-B/WAM System;
- Other EUROCAE groups involved in surveillance activities;
- EUROCONTROL GEN-SUR SEC;
- ASTERIX Maintenance Group

Any other SJU project that may require the information included in this document for their activities.

2.4 Background

The following on-going and past activities have contributed to the definition of the high-level security requirements for surveillance sensors.

2.4.1 SESAR1 15.04.06 Project

SESAR 15.04.06 project focused on the development and testing of means to detect and indicate ADS-B threats, in order to further improve the security of ADS-B.

The project started with a security risk assessment for ADS-B ("ADS-B Threat Analysis Report" [14]), based on the GEN-SUR Security Risk Assessment document [17] developed by EUROCONTROL.

After the analysis for potential ADS-B security threats, the project established their associated high-level technical requirements. These requirements were used afterwards as basis for the implementation on the ADS-B Security Ground Sensor prototypes, developed separately by the project partners INDRA and THALES.

In general the related risks can be divided in those related on individual targets (one or few) and those affecting the entire surveillance sensor (all target information is affected). With respect to target threats it can be distinguished between spoofing, modification of provided data or target suppression. The system related threats are related to RF interference (Jamming), degradation of timing or overload conditions. The threats will be discussed in detail in sect. 4.1.

The developed functionality was related to the identification of basic threat detection means and their implementation.

During the Prototype Verification a range of internal tests were performed in order to assess the efficiency of threat detection mechanism by the INDRA and THALES security prototypes.

The lessons learnt during the project led in a number of recommendations regarding additional Ground Sensor prototype functionalities and reporting features, regarding threat mitigation, regarding additional tests and tools and related to extending the study of security topics beyond the ADS-B scope. These recommendations were made by 15.04.06 project in order to be developed further in detail in the SESAR 2020 programme.

2.4.2 GEN-SUR-SEC: EUROCONTROL Generic Surveillance Security Requirements

The GEN-SUR Security Risk Assessment document [17] developed by EUROCONTROL presents an approach for security risk assessment on a generic surveillance system that is supporting an ATS Surveillance Service in a given sector. As it was aforementioned, the document considers a generic surveillance system, which means that WAM, Primary and Secondary Surveillance Radar (including Mode S) and ADS-B are considered and that various combinations of these techniques are addressed in the document.

The generic assessment presented in the document establishes a framework that can be reused to derive local surveillance risk assessments and risk treatments.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

The document performs firstly a Threat Scenario Evaluation and a Threat Scenario Likelihood Evaluation, followed by an Impact Assessment at sector level as well as a Risk assessment at sector level.

2.4.3 SESAR2020 Wave I Solution PJ14-04-03 T05

The project concentrated on the development of threat detection means to detect the threats identified in SESAR1 project 15.04.06 and the implementation of functionality to report detected threats in an interoperable manner and by proprietary means.

The interoperable forwarding of security information was achieved by rising specific flags in the target ASTERIX reports for target related threats and the provision of specific information on system related threat detections in ASTERIX CAT 25.

Special focus was laid on the determination of a threat detection performance as basis for a later operational use. The threat detection performance is defined by the probability of threat detection and time to detection (integrity of the security function), probability of false alarm (continuity of the security function) and the accuracy.

As a result, the feasibility of a performance in support of the work conducted by ATC for aircraft separation was demonstrated.

During the work performed in PJ14-04-03 T05 it became apparent that a mechanism to forward more information on detected target threats is lacking. At that time only flags indicating invalid targets could be set but no further information could be provided. With the further clarification of validation needs it was concluded that a separate transponder validation message is needed by which threat detection information can be forwarded in an interoperable, sensor independent, manufacturer independent manner through the entire surveillance chain.

2.4.4 EUROCAE WG51 SG4

The document ED-142A (“Technical Specification for Wide Area Multilateration (WAM) Systems” [18]), developed within EUROCAE WG51 SG4, specifies the minimum performance requirements for a Wide Area Multilateration (WAM) System that is part of a system providing airspace situational awareness to air traffic controllers and other users within the European Air Navigation Region.

The document ED-129B (“Technical Specification for an ADS-B Ground System” developed within EUROCAE WG51 SG4, specifies the minimum performance requirements for a "SUR Sensor" element of an infrastructure supporting *ATS Surveillance Service*(s), such as the Approach Control and Area Control Services within the European Air Navigation Region.

2.4.5 Document update

The present document is based on the final TS/IRS of PJ14-04-03 T05 [23] and PJ.14-W2-84c Initial TS/IRS [24], and expanded for:

- ASTERIX CAT 246
- Performance requirements for secured surveillance functions.

2.5 Structure of the document

This document is structured as follows:

- Chapter 1: Executive summary
- Chapter 2: Introduction
- Chapter 3 : SESAR solution impacts on architecture
- Chapter 4 : Technical specifications
- Chapter 5 : Implementation options
- Chapter 6: Assumptions
- Chapter 7: References and applicable documents
- Appendix A: Service Description Document
- Appendix B: ASTERIX CAT 246 Transponder Validation Message

2.6 Glossary of terms

Term	Definition	Source of the definition
ACAS	An aircraft system based on secondary surveillance radar (SSR) transponder signals which operates independently of ground-based equipment to provide advice to the pilot on potential conflicting aircraft that are equipped with SSR transponders	*ICAO Doc 4444*
ADS-B	A means by which aircraft, aerodrome vehicles and other objects can automatically transmit and/or receive data such as identification, position and additional data, as appropriate, in a broadcast mode via a data link	*ICAO Annex 10*
Aircraft Address	A unique combination of 24 bits available for assignment to an aircraft for the purpose of air-ground communications, navigation and surveillance	*ICAO Doc 4444*
MLAT System	A group of equipment configured to provide position derived from the	*ICAO Doc 4444*

Co-funded by the European Union

	secondary surveillance radar (SSR) transponder signals (replies or squitters) primarily using time difference of arrival (TDOA) techniques. Additional information, including identification, can be extracted from the received signals.	
SSR	A surveillance radar system which uses transmitters / receivers (interrogators) and transponders	*ICAO Annex 10*

Table 1: Glossary

2.7 Acronyms and Terminology

Term	Definition
ACAS	Airborne Collision Avoidance System
ADA	Age of Duplication Address
ADD	Architecture Description Document
ADS-B	Automatic Dependent Surveillance - Broadcast
AERR	Age of Error
AMG	ASTERIX Maintenance Group
ASA	Aircraft Surveillance Application
ASTERIX	All-purpose structured EUROCONTROL surveillance information exchange
ATM	Air Traffic Management
ATC	Air Traffic Control
ATS	Air Traffic Services
AVAL	Age of Validation
BAD	Barometric Altitude Deviation
CAT	Category
CBA	Cost Benefit Analysis
CC	Capability Configuration

EUROPEAN PARTNERSHIP

Co-funded by the European Union

CNS	Communications, Navigation and Surveillance
CPR	Compact Position Reporting
CPS	Characters Per Second
CWP	Controller's Working Position
DAA	Detect and Avoid
DERR	Duration of Error
DF	Downlink Format
DVAL	Duration Since Last Validation Status Change
EAS	Element Action Status
EATMA	European ATM Architecture
E-ATMS	European Air Traffic Management System
ELE	ASTERIX Element
ENs	Enablers
ENVAR	Environmental Assessment Report
ER	En-Route
ECV	Error Code Value
ERR	Error
ETP	Error Type
EVAcq	Enhanced Visual Acquisition
FAA	Federal Aviation Administration
FRD	Functional Requirements Documents
GPS	Global Positioning System
GS	Ground Station
HF	High Frequency
HPAR	Human Performance Assessment
ICAO	International Civil Aviation Organization
IER	Information Exchange Requirement

EUROPEAN PARTNERSHIP

Co-funded by the European Union

IRS	Interface Requirements Specification
ISRM	Information Services Reference Model
ITP	In-Trail Procedure
LVC	Low Visibility Conditions
MID	Message Identification Number
MLAT	Multilateration
MOPS	Minimum Operational Performance Standards
MSSCs	Minimum Set of Security Controls
NAF	NATO Architecture Framework
NCS	Non Cooperative Surveillance
NSOV	NAF Service Oriented View
NOV	NAF Operational View
NSV	NAF System View
OSED	Operational Service and Environment Definition
PAS	Plot Action Status
POI	Performance Operational Improvement
QoS	Quality of Service
RA	Resolution Advisory
REQ	Requirement
REP	Repetition Factor
RF	Radio Frequency
RFI	Radio Frequency Interference
RPAS	Remotely Piloted Aircraft System
SAC	System Area Code
SAR	Safety Assessment Report
SDD	Service Description Document
SDPs	Software Defined Perimeter

Co-funded by the European Union

SeAR	Security Assessment Report
SESAR	Single European Sky ATM Research Programme
SFV	Security Function Value
SIC	System Identification Code
SID	Service Identification
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SNMP	Simple Network Management protocol
SPR	Safety and Performance Requirements
SS	Secure Surveillance
SSS	Secure Sensor Surveillance
SSR	Secondary Surveillance Radar
SUR	Surveillance
TA	Traffic Advisory
TCAS	Traffic Collision Avoidance System
TCN	Track Chain Number
TCNDA	Track Chain Number for Duplicate Address
TCO	Transition Concept of Operations
TMA	Terminal Manoeuvring Area
TOD	Time of Day
TRL	Technology Readiness Level
TS	Technical Specification
TSAA	Traffic Situation Awareness with Alerts
TVALP	Technical Validation Plan
UAP	User Application Profile
UAS	Unmanned Aircraft System
V&V	Validation and Verification

EUROPEAN PARTNERSHIP

Co-funded by the European Union

VMC	Visual Meteorological Conditions
VSA	Visual Separation on Approach
VST	Validation Status
VTP	Validation Type
WAM	Wide Area Multilateration

Table 2: Acronyms and terminology

EUROPEAN PARTNERSHIP

Co-funded by the European Union

3 SESAR Solution Impacts on Architecture

3.1 Target Solution Architecture

3.1.1 SESAR Solution(s) Overview

PJ.14-W2-84c: Secured Surveillance Systems (Single and Composite Systems)

SESAR Solution ID and Title	Functional Blocks/Role impacted by the SESAR Solution (from EATMA)	Enabler ID (from EATMA)	Enabler Title (from EATMA)	Enabler coverage
PJ.14-W2-84c Secured Surveillance Systems (Single and Composite)	Composite Surveillance	CTE-S09	Secured composite surveillance	**Fully**

Table 3: SESAR Solution PJ.14-W2-84c Scope and related Functional Blocks/roles & Enablers

Development of secured surveillance systems (focus on cooperative and cooperative dependent sensors) enabling the operational use of security functions.
Scope covers the sensor based radio frequency related threat detection and validation capabilities, performance assessment and identification of interoperable detection forwarding mechanisms by a specific ASTERIX target validation message (ASTERIX CAT 246).

OI Step		OI description	Open CR
POI-0059-SUR		Secured Surveillance Systems (Single and Composite)	
	EN code	EN description	Open CR
	CTE-S09	Secured surveillance	
	EN code	EN description	Open CR
	SVC-064	Security Threats Detection (Surveillance)	CR 06754 Create Enabler SVC-064 for Security Threats Detection (PJ.14-W2-84c)

Table 4: SESAR Solution PJ.14-W2-84c Operational Improvement Steps

Co-funded by the European Union

3.1.1.1 Deviations with respect to the SESAR Solution(s) definition

No deviations have been identified.

3.1.1.2 Relevant Use Cases

ADS-B is envisaged as future surveillance backbone / allowing the use of ADS-B as own/independent surveillance layer also in high density airspace. The expected use of this solution is primarily in En-Route and TMA environments with potential application as well to airport environment. In consequence the focus will be laid to En-Route and TMA environment.

One of the main issues to be solved for ADS-B is related to potential security issues, namely validating the correctness of information provided by the aircraft prior to its use in ATC.

This solution aims to provide a system that is capable of resolving the potential ADS-B security related issues and enable a secure concept for its use in ER and TMA environment. It can also be applied to airport environments.

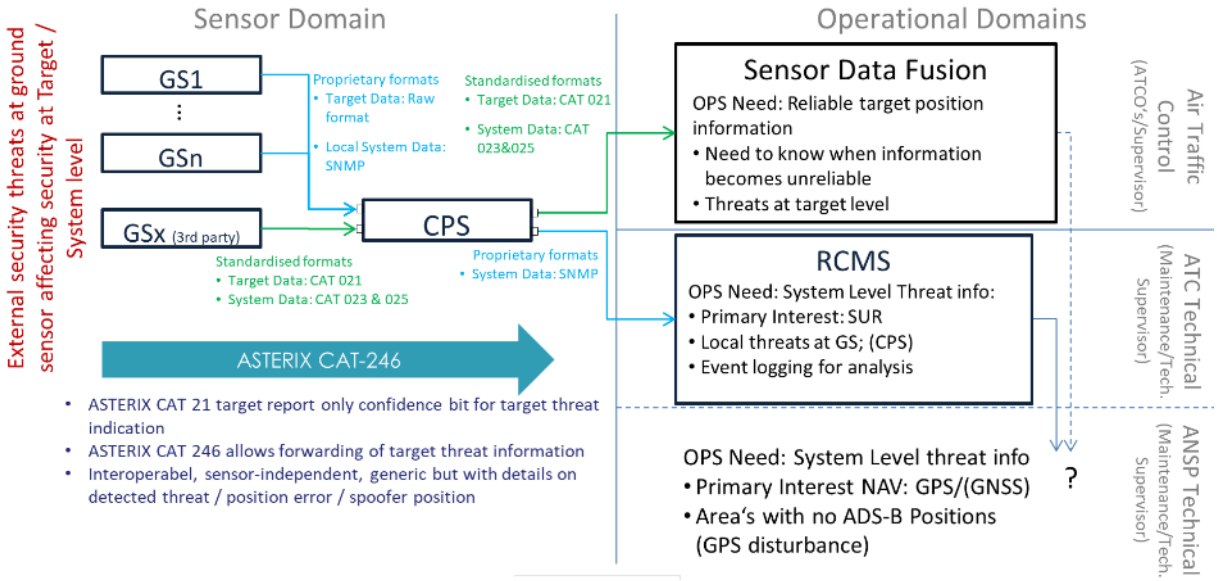


Figure 3-1: Operational view / use case for surveillance security functions

Ground surveillance sensors (ADS-B or MLAT) consist in most cases of several GS which provide data to a central processing where

- Target location
- System status information

is generated.

These information need to be forwarded to downstream processing. In most cases the following can be stated for the information forwarding chain:

- GS data to CPS: is typically performed in proprietary formats allowing to leverage network use and data to be provided. When 3rd party equipment is used ASTERIX will be used instead.
- CPS to Tracker: is performed via a ASTERIX target report message (CAT021 for ADS-B / CAT020 for multilateration)

EUROPEAN PARTNERSHIP
Co-funded by the European Union

The maintenance interfaces use in most cases proprietary formats (i.e. SNMP)

The operational use of ground surveillance sensors can be generalized as follows:

- SUR serves primary use: Target location via tracking system to controllers CWP who ensures aircraft separation
- Maintenance interface to technicians who supervise system status and perform corrective actions in case of system status degradations

With respect to RF threats entering the surveillance chain at the sensor the following operational needs can be identified:

- ATCO is not interested in security at all – he needs a ”clean“ display & reliable target positions
- But may need to be informed when information becomes unreliable in order to adapt operation (for instance target position reporting by VHF)
- Tech Supervisor may be interested in security issues when he can do something against
- Needs to be informed about system level threats
- May use system logs for event analysis
- Then there is a potential add on: provide information to other services, example: GNSS status from ADS-B and Multilateration systems
- A severe limitation to forward security related information will be overcome with ASTERIX CAT-246 target validation message since it allows to forward detailed information on threats detected for a target.
- Specific information needs for the different stakeholders
- When considering interfaces: interoperability of different equipment needs to be ensured

In addition following considerations are applicable:

In high density airspace typically multiple surveillance layers (min. 2) will be used. There is always a primary sensor.

It is reasonable to assume validation in downstream ATC processing: In large/complex ATC structures central validation of suspicious targets. The central validation is then able to collect all relevant information and to perform an appropriate action, e.g. removal of false targets or flagging of unreliable targets such the ATCO workload will be kept within allowable limits.

In this context the task of the sensor is:

- Detect target and system related RF threats
- At sensor level specific detection is feasible since full RF related information is available

Co-funded by the European Union

- In downstream this information is lost – target information is more compressed

Mitigation action:

- Forward information on target threat detections to downstream validation
- Provide system status via ASX23/25 and SNMP

Purpose of security function: confirm correctness (integrity) of (ADS-B) target data – especially position and essential secondary surveillance data (like emergency status).

From a high level perspective the following impact on the operation will result from potential RF-security threats.

	Threat	Description	Operational Impact	Performance parameter
	Modified Data	existing target with unreliable (position) data	Detected: Increased ATCO workload Not Detected: Separation violation	Integrity
	Spoofed Target	Non-existing target	Detected: Increased ATCO workload Not Detected: separation violation	Integrity
	Suppression	Invisible existing target	separation violation	Integrity
	Interference (Jamming) 1090 & 1030 MHz	Provision of all target data degraded	Increased ATCO workload	Availability
	Processing	Provision of all target data degraded	Increased ATCO workload	Availability
	Timing	Position accuracy degraded	Increased ATCO workload	Accuracy
	GPS	Position accuracy degraded & Impact to other services (NAV)	Procedure switch Increased ATCO workload	Accuracy

Co-funded by the European Union

General distinction for security threats:

- threats affecting single or few targets -> target threats
- Threats affecting all targets & the system in general -> system threats

On target level following threats have been identified

- Data modification – meaning the modification of the ADS-B data of a target leading to potentially unreliable position data for the respective target
- Spoofing – refers to the generation of false or non-existing targets
- Suppression – refers to suppressing existing targets such that its position data will not be processed – invisible target

The operational impact depends on whether the threat will be detected by the air traffic controller or not

- The more severe case results when the threat is not detected by the controller
- Then aircraft separation violations may result

Consequently in terms of a performance parameter the impact of a separation violation can be expressed as integrity violation.

On the system threat side one can identify the following threats

- Radio frequency interference (RFI) on primarily on 1090 MHz but also on 1030 MHz if interrogations of the aircraft transponder are considered: depending on the interference level the data reception will be degraded
- Timing (especially via GPS)
- GPS meaning the position determination process using GPS

The impact will in every case result in increased ATCO workload since the sensor does not provide data and either redundant equipment has to be used or different separation procedures, like voice comm with position reporting have to be applied

- Processing: like overload situations. In this case the entire target data processing will be degraded.
- In case of GPS positioning also switching to other procedures using other navigation means need to be considered.
- It needs to be mentioned that the hazard identification refers to the surveillance and not to the navigation. For navigation typically a separate assessment needs to be performed as the operational impact differs.

The impact of the system threats in terms of performance parameters is

Co-funded by the European Union

- Availability in case of RFI and threats to the sensor data processing
- Accuracy in case of timing and GPS

In general it can be stated for all threats that the criticality depends on the airspace. In high density airspace the risks resulting from the threats are higher.

In summary the use cases can be described in short as follows:

Operational Use Case	Description

System Process	Description
[NSV-4] T05 - Use of Secure Surveillance at TMA	Provide information on detected system threats. Provide information on detected target threats.

System Process	Description
[NSV-4] T05 - Use of Secure Surveillance at TMA & Enroute	Inform Downstream equipment about detected RF-Security threats with a specified performance

3.1.1.3 Applicable standards and regulations

This list of standards and regulations that are applicable to the SESAR Solution 14.04.03:

- EUROCAE ED-142A Technical Specification for Wide Area Multilateration (WAM) systems
- EUROCAE ED-129B Technical Specification for a 1090 MHz Extended Squitter ADS-B Ground System
- EUROCONTROL Specification for Surveillance Data Exchange ASTERIX Part 14 Category 20 Multilateration Target Reports, Ed. 1.9.
- EUROCONTROL Specification for Surveillance Data Exchange ASTERIX Part 12 Category 21 ADS-B Target Reports, Ed. 2.4.
- EUROCONTROL Specification for Surveillance Data Exchange ASTERIX Part 26 Category 025 CNS/ATM Ground System Status Reports Ed.1.1.
- Draft Specification for Surveillance Data Transponder Validation Report ASTERIX CAT 246 Ed. 0.12.06 (draft developed as part of PJ.14-W2-84c in Wave 2)

3.1.2 Capability Configurations required for the SESAR Solution

T05 - Secured Surveillance				
CC	**Op Env**	**Capability**	**Node**	**Stakeholder**

APP ACC (PJ14-W2-84c)	TA-High Complexity; TA-Low Complexity; TA-Medium Complexity; TA-Very High Complexity; Terminal Airspace;	Air Traffic Demand Provision (airspace); Airspace Reservation Design; Airspace Reservation Management; Arrival Sequencing; Collaborative Network Management; Collaborative Trajectory Planning; Messaging; Trajectory Conformance Monitoring; Trajectory Information Synchronisation; Trajectory Revision in Execution;	Airspace Management; En-Route/Approach ATS;	Civil ATS Approach Service Provider; Military ATS Approach Service Provider;
Communication Infrastructure	Airport; En-Route; Network; Terminal Airspace;	Air/ground connectivity provision based on terrestrial infrastructure; Network connectivity provision for aeronautical communications on the airport surface;		Civil CNS Service Provider; Military CNS Service Provider;
ER ACC (PJ.14-W2-84c)	En-Route;		Air Traffic Flow and Capacity Management; Airspace Management; Airspace Organisation; En-Route/Approach ATS;	Civil ATS En-Route Service Provider; Military ATS En-Route Service Provider;
ER ACC (PJ.14-W2-84c)	En-Route;		Air Traffic Flow and Capacity Management; Airspace Management; Airspace Organisation; En-Route/Approach ATS;	Civil ATS En-Route Service Provider; Military ATS En-Route Service Provider;
Surveillance Infrastructure	En-Route;			Civil CNS Service

Co-funded by the European Union

En-Route (PJ.14-W2-84c)				Provider; Military CNS Service Provider;
Surveillance Infrastructure En-Route (PJ.14-W2-84c)	En-Route;			Civil CNS Service Provider; Military CNS Service Provider;
Surveillance Infrastructure TMA (PJ14-W2-84c)	Terminal Airspace;			Civil CNS Service Provider; Military CNS Service Provider;

Table 5: List of Capability Configuration required for the SESAR Solution

3.2 Changes imposed by the SESAR Solution on the baseline Architecture

Enabler	Element type	Element name	Impact	Change
CTE-S09	Secured surveillance			
	Sys	Secure Surveillance	Introduce	
SVC-064 (create CR)	Security Threats Detection (Surveillance)			
	Service	SecurityThreatsDetection	Introduce	

Table 6: List of changes due to the SESAR Solution

3.3 Analysis of security functions

The scope of the surveillance security functions addressed herein is related to threats entering the system via the RF interface. Threats are related to system level or target level, where on system level overload (denial of service) and system timing can be affected and on target level the threats are related to jamming, spoofing or suppressing single targets (for more details on security threats, one can refer to section 4.1).

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Network security and physical security are not different compared to other systems and thus are not specifically addressed herein.

The intention of the surveillance security functions is to ensure correctness of the information provided to an air traffic controller who is responsible to ensure aircraft separation. The term correctness is related to a security performance expressed by integrity, continuity and accuracy. Due to this nature the security functions are a mean to ensure the safety of the air traffic management (security for safety).

3.3.1 Security in ADS-B systems

The ADS-B is a cooperative & dependent system. Due to its RF-interface and modulation scheme it is vulnerable to be interfered as any other RF-based system. In addition, target reports may be modified or even supressed in a relatively easy way. Taking into account that ADS-B is a crucial piece of the surveillance infrastructure in the coming years, this system needs to be secure against any type of threat entering from the outside via the RF signal and also from the network side the latter is separately covered by cyber-security

Implementing new security functionalities can afford the detection and implementation of different threats similar to working together with a multilateration system.

This PJ.14-W2-84c provides analysis of the potential threats of this system, explaining how to detect and report them. Note that the definition of mitigation means is out of scope of this solution.

The responsibility of the security function at ADS-B ground sensor level is primarily to detect and report an existing threat condition. Enhancements towards a mitigation for a “clean” aerial situation display at CWP needs the involvement of additional validation means either at the ground sensor or further processing steps which typically are part of the downstream ATC data processing chain.

Aspects of threat validation in network-based processing and against other sensors are covered in section 3.3.3.

3.3.2 Security in multilateration systems (WAM/MLAT)

Multilateration systems can be less affected than ADS-B, due to they use independent surveillance, but they can be also threatened by noise, jamming, overpowering, etc.

It is noted that the passive mode in the multilateration systems can potentially be spoofed where active multilateration through interrogation can provide additional security.

3.3.3 Security in composite surveillance

The security in composite surveillance needs to be a sum of the different security features of the systems that are part of it.

During the previous activities, it was proven that composite WAM+ADS-B system improves the security level of isolate systems (e.g. by identifying spoofed targets). ADS-B data – such as position,

EUROPEAN PARTNERSHIP

Co-funded by the European Union

identification or altitude information – was validated using multilateration, proving the resilience of the composite surveillance.

The availability of additional data within the composite systems can be used to support optional means to provide additional security mitigation techniques in a cost effective manner.

It shall also include security aspects related to integrated CNS concept, one point failure, etc.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

4 Technical Specifications

4.1 Threats classification

In SESAR 15.04.06 project, different threats were developed and studied. The list of threats has been established with the aim of studying the integrity and performance values that can be achieved by the system for their detection.

The threat ID's follow the classification in GEN-SUR-SEC [17].

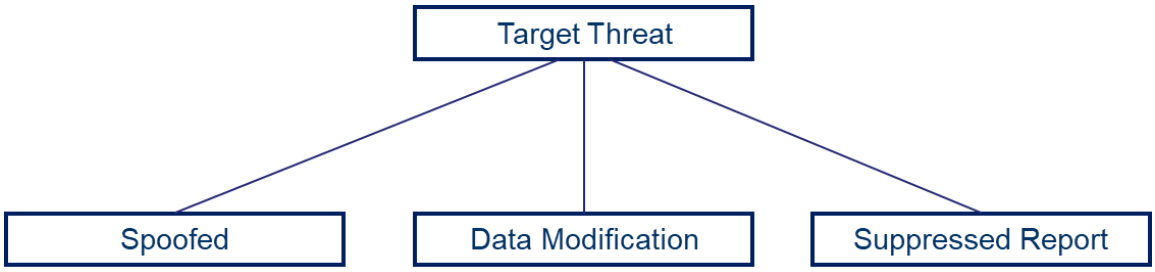


Figure 4-1 Target Threat Classification

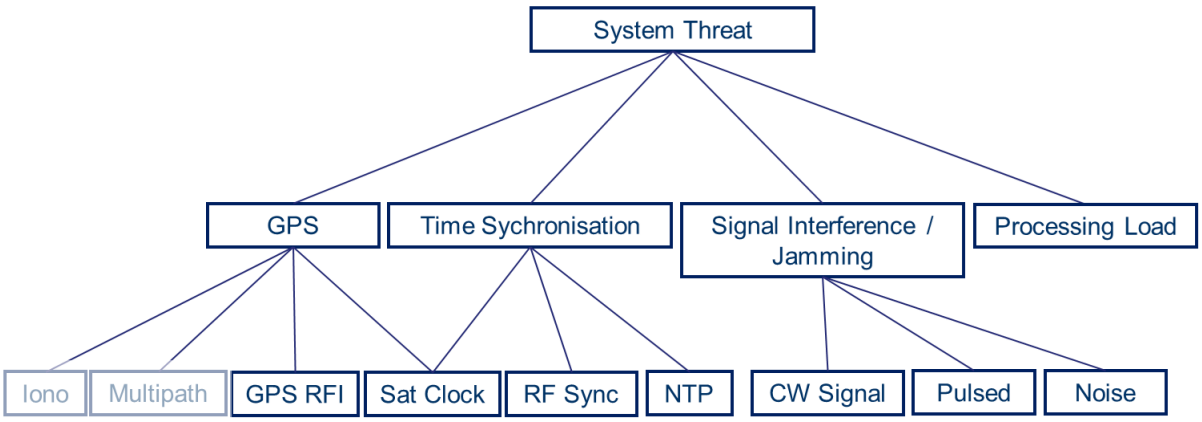


Figure 4-2 System Threat Classification

4.1.1 Threats at signal level

Co-funded by the European Union

4.1.1.1 Overpowering system by noise

THREAT 14: Overpowering 1090 MHz by noise from the ground

The target of this threat is to saturate the receiver by noise on 1090 MHz from ground, in order to mask a large number of real aircraft.

The relevant threat parameters are:

- Minimum noise level.
- Minimum duration of interference.

THREAT 15: Overpowering 1090 MHz by noise from airborne

The target of this threat is to saturate the receiver by noise on 1090 MHz from airborne, in order to mask a large number of real aircraft.

The relevant threat parameters are:

- Minimum noise level.
- Minimum duration of interference.

THREAT 17: Overpowering 1090 MHz by massive fake 1090 MHz SSR messages

This applies in the generation of multitude valid non ADS-B messages (non DF17, DF18 and DF19 with unique or different ICAO addresses) and classic (non-Mode S) SSR messages that may disturb the reception performances of the system.

The relevant threat parameters are:

- Minimum noise level.
- Increase of received messages compared to usual values (%)
- Minimum duration of interference.

4.1.1.2 Jamming

THREAT 16A: Sending massive fake ADS-B messages, non-similar to a real aircraft in the sector (different 24-bit ICAO address)

The objective is to overload the ADS-B sensor. These fake messages are only partial and could not be assembled as fake SUR reports in addition to the real aircraft.

Co-funded by the European Union

Threat 16A is based on the following concepts:

- Generation of (in some cases massive) fake ADS-B messages, which not affect to the behaviour of real existing targets in the ADS-B ground sensor's reception area.
- The ADS-B messages do not reach the CWP display, but some real aircrafts could be lost.
- All types of ADS-B message transmission sequences and data modifications are possible.
- Received ADS-B messages studied in this case will not normally coincide with existing ICAO addresses received by the ground sensor. This will result in an increase of the number of messages received by the system but should not affect the existing tracks except by cases random coincidence.

The relevant threat parameters are:

- Overload level in terms of number of messages.
- Increase of received messages compared to usual values (%)
- Minimum duration of interference.

4.1.2 Threats at ADS-B content level

4.1.2.1 Modification of existing targets

THREAT 16B: Sending some fake ADS-B messages, similar to a real aircraft in the sector (same 24-bit ICAO address) but with falsified content

The objective is to modify existing track data.

Threat 16B is based on:

- Generation of fake ADS-B messages, which affect only the behaviour of real existing targets in the ADS-B ground sensor reception area.
- The ADS-B messages (modified target data) could reach the CWP display.
- All types of ADS-B message transmission sequences and data modifications are possible.
- It is important to distinguish the analysis on the ADS-B messages data contents and the time of ADS-B message emission.
- In this way, different, similar or a mix of ADS-B messages types and subtypes could be transmitted, with falsified or valid data contents.
- ADS-B messages could be emitted synchronous or asynchronous to real standard ADS-B transponder transmissions.

Co-funded by the European Union

Threat 16B addresses only ADS-B position and/or altitude messages that cause no target position jump.

The relevant threat parameters are:

- Messages/content received.
- Increase of received messages compared to usual values (%)
- Minimum duration of interference.

THREAT 16C: Sending massive fake ADS-B messages, similar to a real aircraft in the sector (same 24-bit ICAO address) but with falsified content

The objective is to overload the ADS-B sensor using modified existing track data.

Threat 16C is based on:

- Generation of massive fake ADS-B messages, which affect the behaviour of real existing targets in the ADS-B ground sensor reception area.
- The ADS-B messages could reach the CWP display, but also some real aircraft could be lost.
- All types of ADS-B message transmission sequences and data modifications are possible.

Threat 16C covers the case of massive fake ADS-B messages, which degrades or overloads the ADS-B ground sensor processing performance.

The relevant threat parameters are:

- Overload level in terms of number of messages.
- Increase of received messages compared to usual values (%)
- Minimum duration of interference.

THREAT 25A: Sending some fake ADS-B messages, similar to a real aircraft in the sector (same 24-bit ICAO address)

The prime objective is to duplicate the real aircraft, by one or several spoofed tracks, sent with or without delay.

Threat 25A is based on:

- Generation of some fake ADS-B target reports (spoofed), which are duplicating the aircraft address of existing targets. Only those ADS-B messages are taken into consideration, which could be associated to real existing targets in the ADS-B ground sensor reception area.
- The spoofed ADS-B targets could not reach the CWP display (duplicate indicated), but also

Co-funded by the European Union

duplicated real targets could lost.

- The threat scenario could consist of real target recordings, which are afterwards later retransmitted with or without modifications of the original target data, or user simulated ADS-B target movements.
- In most of the cases, the target duplication implies related target position jumps.
- The generated ADS-B message scenario shall fulfil the necessary requirements for the subsequent ADS-B ground sensor target generation.

This threat 25A is focused on the position, however some variation exists, e.g. the case of the spoofed aircraft alternating the aircraft emergency status, but are not covered.

The relevant threat parameters are:

- Overload level in terms of number of messages.
- Messages/content received.
- Minimum duration of interference.
- Minimum distance between fake and real targets.

4.1.2.2 Duplicating tracks

THREAT 16C: Sending massive fake ADS-B messages, similar to a real aircraft in the sector (same 24-bit ICAO address) but with falsified content

The objective is to overload the ADS-B sensor using modified existing track data. These fake messages could not be assembled as fake SUR reports in addition to the real aircraft.

Threat 16C is based on:

- Generation of massive fake ADS-B messages, which affect the behaviour of real existing targets in the ADS-B ground sensor reception area.
- The ADS-B messages could reach the CWP display, but also some real aircraft could be lost.
- All types of ADS-B message transmission sequences and data modifications are possible.

Threat 16C covers the case of massive fake ADS-B messages, which degrades or overloads the ADS-B ground sensor processing performance.

The relevant threat parameters are:

- Overload level in terms of number of messages.

Co-funded by the European Union

- Increase of received messages compared to usual values (%)
- Minimum duration of interference.

THREAT 25A: Sending some fake ADS-B messages, similar to a real aircraft in the sector (same 24-bit ICAO address)

The prime objective is to duplicate the real aircraft, by one or several spoofed tracks, sent with or without delay

Threat 25A is based on:

- Generation of some fake ADS-B target reports (spoofed), which are duplicating the aircraft address of existing targets. Only those ADS-B messages are taken into consideration, which could be associated to real existing targets in the ADS-B ground sensor reception area.
- The spoofed ADS-B targets could not reach the CWP display (duplicate indicated), but also duplicated real targets could lost.
- The threat scenario could consist of real target recordings, which are afterwards later retransmitted with or without modifications of the original target data, or user simulated ADS-B target movements.
- In most of the cases, the target duplication implies related target position jumps.
- The generated ADS-B message scenario shall fulfil the necessary requirements for the subsequent ADS-B ground sensor target generation.

This threat 25A is focused on the position, however some variation exists, e.g. the case of the spoofed aircraft alternating the aircraft emergency status, but are not covered.

The relevant threat parameters are:

- Overload level in terms of number of messages.
- Messages/content received.
- Minimum duration of interference.
- Minimum distance between fake and real targets.

THREAT 25C: Sending massive fake ADS-B messages, similar to real aircraft in the sector (same 24-bit ICAO address)

The prime objective is to duplicate the real aircraft, by massive spoofed tracks.

Threat 25C is based on:

Co-funded by the European Union

- Generation of massive fake ADS-B target reports (spoofed), which are duplicating the aircraft address of existing targets. Only those ADS-B messages are taken into consideration, which could be associated to real existing targets in the ADS-B ground sensor reception area.
- The spoofed ADS-B targets could not reach the CWP display (duplicate indicated), but duplicated real targets could be lost, and also some real not duplicated aircrafts could be lost.
- The threat could consist of scenarios with addresses the duplication of many targets.
- In most of the cases the target duplication implies related target position jumps.
- There are, however, constellations in which the position difference is below the position jump detection threshold.
- The generated ADS-B message scenario shall fulfil the necessary requirements for the subsequent ADS-B ground sensor target generation.

The relevant threat parameters are:

- Overload level in terms of number of messages.
- Messages/content received.
- Minimum duration of interference.
- Minimum distance between fake and real targets.

4.1.2.3 Delaying real tracks and re-injecting again.

THREAT 25A: Sending some fake ADS-B messages, similar to a real aircraft in the sector (same 24-bit ICAO address)

The prime objective is to duplicate the real aircraft, by one or several spoofed tracks, sent with or without delay.

Threat 25A is based on:

- Generation of some fake ADS-B target reports (spoofed), which are duplicating the aircraft address of existing targets. Only those ADS-B messages are taken into consideration, which could be associated to real existing targets in the ADS-B ground sensor reception area.
- The spoofed ADS-B targets could not reach the CWP display (duplicate indicated), but also duplicated real targets could lost.
- The threat scenario could consist of real target recordings, which are afterwards later retransmitted with or without modifications of the original target data, or user simulated ADS-

Co-funded by the European Union

B target movements.

- In most of the cases, the target duplication implies related target position jumps.
- The generated ADS-B message scenario shall fulfil the necessary requirements for the subsequent ADS-B ground sensor target generation.

This threat 25A is focused on the position, however some variation exists, e.g. the case of the spoofed aircraft alternating the aircraft emergency status, but are not covered.

The relevant threat parameters are:

- Overload level in terms of number of messages.
- Messages/content received.
- Minimum duration of interference.
- Minimum distance between fake and real targets.

4.1.2.4 Simulation of non-real ADS-B targets

THREAT 24A: Sending some fake ADS-B messages, non-similar to a real aircraft in the sector (different 24-bit ICAO address)

The objective is to add spoofed tracks in addition to the real aircraft.

Threat 24A is based on

- Generation of some fake ADS-B target reports. Only those ADS-B messages are taken into consideration, which fulfil all necessary requirements for the subsequent target report generation by the ADS-B ground sensor. This threat is only based on the continuous presence of the spoofed ADS-B targets.
- Covers only ADS-B messages of targets that did not exist in the current ADS-B ground sensor reception area.
- The spoofed ADS-B targets could reach the CWP display, no real aircrafts are lost.
- This threat case comprises scenarios with a minor number of ADS-B targets.
- In principle, all kind of target behaviours are possible. The targets could replicate a usual aircraft, vehicle behaviour pattern on ground and/or air, or they could emit noticeable mutated target data accumulations with an unusual pattern.
- It is important to distinguish the analysis on the data contents and the time of message emission. The relevant ADS-B messages could be emitted continuous or unsteady.
- This Threat 24A only relates to position (horizontal or vertical).

EUROPEAN PARTNERSHIP

Co-funded by the European Union

The relevant threat parameters are:

- Overload level in terms of number of messages.
- Messages/content received.
- Minimum duration of interference.

THREAT 24B: Sending massive fake ADS-B messages, non-similar to a real aircraft in the sector (all different 24-bit ICAO address)

Threat 24B is based on:

- Generation of massive fake ADS-B target reports. Only those ADS-B messages are taken into consideration, which fulfil all necessary requirements for the subsequent target report generation by the ADS-B ground sensor. Threat 24B covers only ADS-B messages of spoofed targets that did not exist in the current ADS-B ground sensor reception area.
- The objective is to add spoofed tracks in addition to the real aircraft.
- The massive spoofed ADS-B targets could reach the CWP display, but also real aircrafts could be lost.
- Continuous presence of the spoofed ADS-B targets.

The relevant threat parameters are:

- Overload level in terms of number of messages.
- Messages/content received.
- Minimum duration of interference.

THREAT 25B: Sending some fake ADS-B messages, all with the same 24-bit ICAO address (but different from real aircraft)

Threat 25B is based on:

- Generation of some fake ADS-B target reports (spoofed), which are duplicating the aircraft address of not existing (spoofed) targets.
- Only those ADS-B messages are taken into consideration, which could not be associated to real existing targets in the ADS-B ground sensor reception area.
- The objective is to add spoofed tracks in addition to the real aircraft.
- The generated scenario covers duplicated faked ADS-B targets.

- The spoofed ADS-B targets could not reach the CWP display (duplicate indicated).
- The focus of threat 25B is on the position of targets.

The relevant threat parameters are:

- Overload level in terms of number of messages.
- Messages/content received.
- Minimum duration of interference.

THREAT 25D: Sending massive fake ADS-B messages, all with the same 24-bit ICAO address (but different from real aircraft)

The objective is to add massive spoofed tracks in addition to the real aircraft.

Threat 25D is based on:

- Generation of massive fake ADS-B target reports (spoofed), which are duplicating the aircraft address of not existing (spoofed) targets. Only those ADS-B messages are taken into consideration, which could be not associated to real existing targets in the ADS-B ground sensor reception area.
- The generated scenario covers only duplicated faked (spoofed) ADS-B targets.
- The spoofed ADS-B targets could not reach the CWP display (duplicate indicated), but some real not duplicated aircraft could be lost.

The relevant threat parameters are:

- Overload level in terms of number of messages.
- Messages/content received.
- Minimum duration of interference.

4.1.2.5 Frustrate track initiation

THREAT 16F: Suppression of ADS-B targets

It´s possible to frustrate track initiation in ADS-B sensors by different methods, introducing false information to the system. With the use of composite sensors this can be detected and reported as WAM track will be correctly initiated, while non-successful track initiations for ADS-B will take place for the same ICAO address. This threat was not included in the study of SESAR1 15.04.06 project.

The relevant threat parameters are:

Co-funded by the European Union

- CPR initialization tries

Note: This threat 16F is not included in the GEN SUR document at the moment of the creation of this document.

4.1.3 Threats at WAM content level

THREAT 16D: Sending some fake replies, similar to a real aircraft in the sector (same 24-bit ICAO address) but with falsified content

The objective is to modify existing track data; therefore, these fake replies could not be assembled as fake SUR reports in addition to the real aircraft.

Threat 16D applied for WAM addresses the modification of the following content:

- Aircraft ID.
- Mode A.
- Mode C.
- Emergency/alert.

The relevant threat parameters are:

- Increase of received replies compared to usual values (%)
- Minimum duration of interference.
- Replies/content received.

Note: This threat 16D is not included in the GEN SUR document at the moment of the creation of this document.

THREAT 16E: Sending massive fake replies, similar to a real aircraft in the sector (same 24-bit ICAO address) but with falsified content

The objective is to overload the WAM sensor using modified existing track data. These fake replies could not be assembled as fake SUR reports in addition to the real aircraft.

Threat 16E applied for WAM addresses the modification of the following content:

- Aircraft ID.
- Mode A.
- Mode C.

Co-funded by the European Union

- Emergency/alert.

The relevant threat parameters are:

- Overload level in terms of number of replies.
- Increase of received replies compared to usual values (%)
- Minimum duration of interference.
- Replies/content received.

Note: This threat 16E is not included in the GEN SUR document at the moment of the creation of this document.

4.1.4 Time Synchronisation

4.1.4.1 GPS RFI related to ADS-B

The reception of the GPS signals can be disturbed due RF-interference in vicinity of the receiver. The range of disturbance depends on the properties of the interfering signal (i.e. modulation, power, polarization …). The impact on the GPS receiver depends on these characteristics. It may vary from degraded accuracy of airborne position reports to loss of GPS signal reception.

GPS RFI can adversely affect the accuracy of positions reported by ADS-B targets, if the interference source is in the vicinity of the airborne receiver. Airborne certification will ensure that no misleading information is provided (accuracy reports are bounded by integrity reports).

THREAT 20: Overpowering a single or multiple SUR Sensor (excluding WAM) GPS frequency with noise (loss) to affect GPS timing, done from the ground (low power)

Threat 20 is based on the generation of noisy band signals that may affect to the L1 and L2 band.

May affect multiple sectors if the sensors support multiple sectors.

The relevant threat parameters are:

- Minimum noise level.
- Minimum duration of interference.

4.1.4.2 GPS RFI related to WAM

THREAT 19: Overpowering a single or multiple WAM Ground Station GPS frequency with noise (loss) to affect GPS timing, done from the ground (low power)

Co-funded by the European Union

The relevant threat parameters are:

- Minimum noise level.
- Minimum duration of interference.

The effect of this threat depends on ground station timing solution (GPS only or an alternative mechanism).

4.1.4.3 GPS based timing in ATC SUR

THREAT 20A: Affecting the GPS timing of the ATC SUR Processing by sending overpowering the GPS signal (jamming)

The target of this threat is to affect the capacity by stopping/degrading the ATC SUR Processing.

The relevant threat parameters are:

- Minimum noise level.
- Minimum duration of interference

THREAT 20B: Affecting the timing of the ATC Processing by sending fake GPS signal – drifting the signal

The target of this threat is to create incident/accident through first partial track loss then ultimately total loss of tracks.

Note: In most cases a time-differential principle is applied in ATC-Sur. In this case a spoofed GPS signal will be easily detected before any hazardous condition will result. Thus this threat will not be further considered in the scope of PJ.14-W2-84c.

THREAT 21: Overpowering a single or multiple WAM Ground Station GPS frequency with spoofed GPS signal to affect timing (Misleading)

The effect of this target depends on ground station timing solution (GPS only or else).

Note: In most cases a time-differential principle is applied in ATC-Sur. In this case a spoofed GPS signal will be easily detected before any hazardous condition will result. Thus, this threat will not be further considered in the scope of PJ.14-W2-84c.

Co-funded by the European Union

THREAT 22: Overpowering a single or multiple SUR Sensor (excluding WAM) GPS frequency with spoofed GPS signal to affect timing (Misleading)

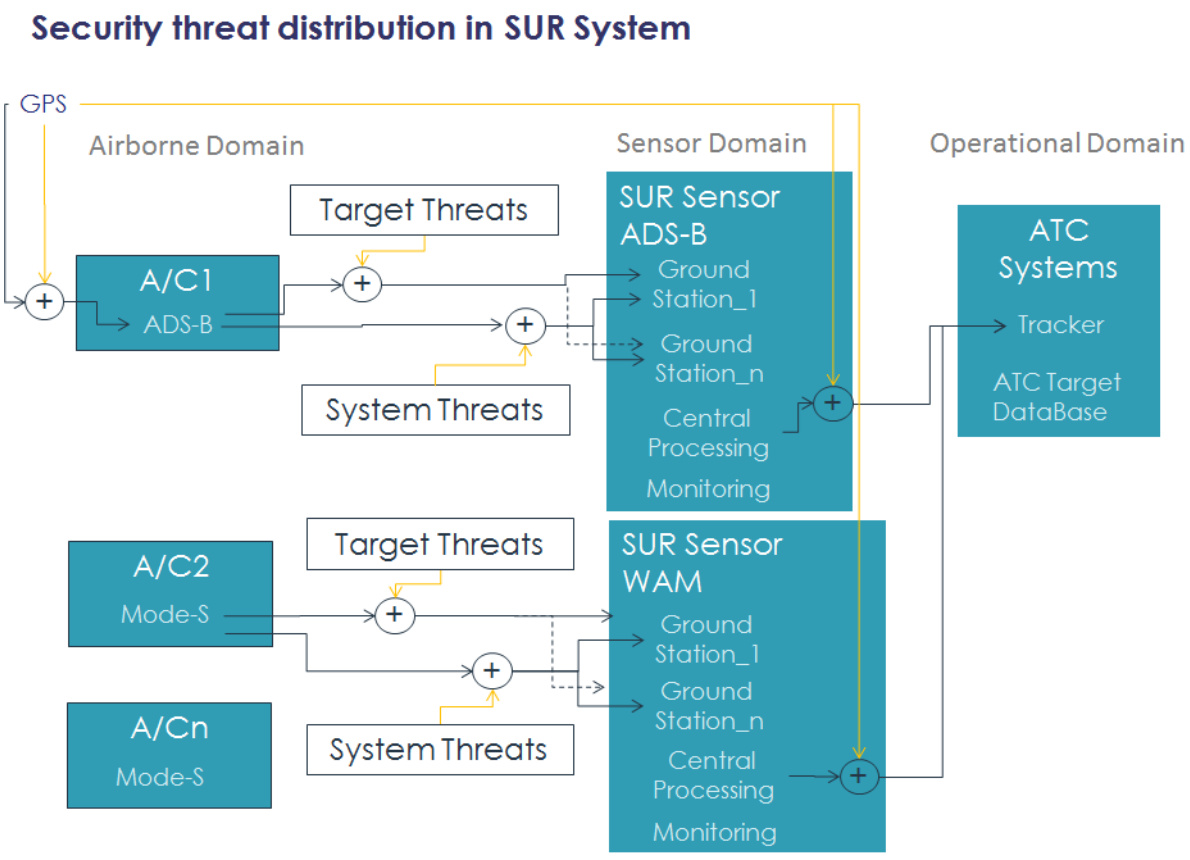
This threat may affect multiple sectors if the sensors support multiple sectors.

Note: In most cases a time-differential principle is applied in ATC-Sur. In this case a spoofed GPS signal will be easily detected before any hazardous condition will result. Thus, this threat will not be further considered in the scope of PJ.14-W2-84c.

In addition to above mentioned intentional influences on the timing, also unintentional influences exist – in most cases caused by a satellites internal malfunction. Such malfunction can lead to very large timing errors and thus adversely affect the accuracy / integrity of WAM and MLAT systems. Such satellite malfunctions are rare events (approx. 1.5 times per year).

4.2 Functional architecture overview (general introduction for all solutions)

The Figure 4-3 below explains the threats distribution in a surveillance system composed by ADS-B and WAM ground stations. As can be seen, target and system threats can be interfered independently in different aircrafts and surveillance techniques.



EUROPEAN PARTNERSHIP

Co-funded by the European Union

Figure 4-3: Security threat distribution in the surveillance systems

In the following figure, it is represented a generic ATC security infrastructure where the validation can occur at different stages. The following aspects must be taken into account:

- Sensors responsibility is to detect and flag threat conditions: At the sensor the full RF information is available. This enables the detection of anomalies. More details on the detection will be given below. Centralized functions are capable to validate sensor data and to remove invalid targets. The validation function may be split.
- The CPS provides the ADS-B system output and hence the security function.
- Technical system control & status functions ensure that detected component or system related threats will be mitigated. This involves removal of faulty components / sensors and annunciation on the technical displays.

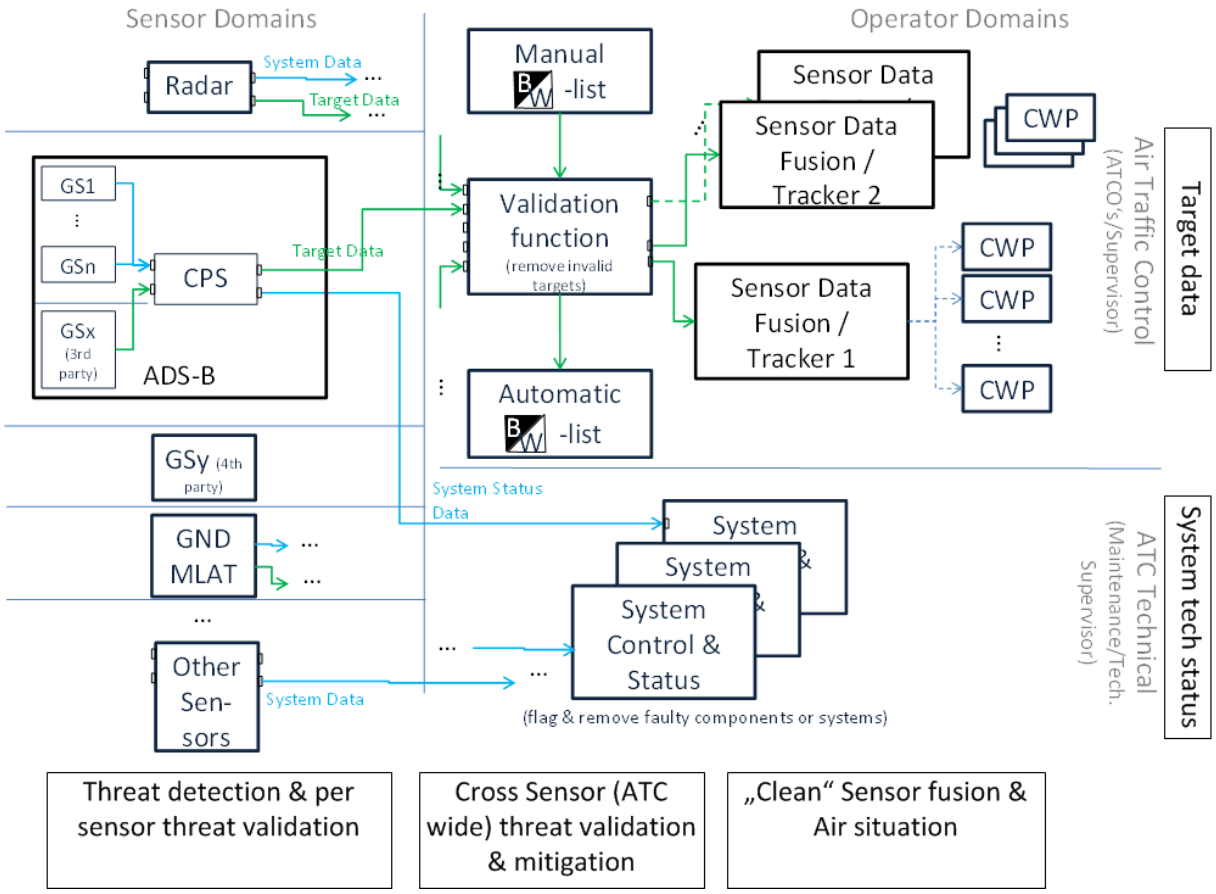


Figure 4-4: Generic ATC-architecture security function

As identified in sect. 3.1.1.2 the purpose of the security function is to confirm ADS-B target data – especially position. The raw received ADS-B signal consists of the carrier pulse-position modulated with the Mode S pulses over time. By the signal processing chain the contained position data are decoded.

EUROPEAN PARTNERSHIP
Co-funded by the European Union

Based on raw data alone the correctness of data cannot be verified. Data decoding needs to be performed. But from data alone it cannot be ensured that content is correct – it could be spoofed, what is not identifiable based on data content.

Security functions at target level therefore can apply a two staged approach consisting of:

1. Target threat detection: to detect anomalies related to the identified security threats, detection of non-confident targets

2. Target threat validation: threat confirmation

Detection of threats at target level is related to spoofing; data modification or target suppression. It is based on the detection of non-standard behavior and checks on reasonableness against physical constraints.

In order to work reliably, the threat detection needs to assume:

- that the transponders implemented in air vehicles conform to the applicable standards (RTCA DO-260x)

- Air vehicles move within certain physical constraints

The applied checks for target threat detection are extremely helpful in conformance monitoring. So the use for conformance monitoring can be seen as by-product of the security functions.

The validation of identified threats is performed based on physical measurements. Within the sensor additional HW-based measurements of target RF signals physical properties will be performed. The measured quantity needs to be related to position in known manner (like TDOA between two spatially distributed GS). Through these measurements a deviation between the reported ADS-B position and the measured position metric will result. The measured position related metric can be used to indicate the location of the RF-source (i.e. attacker position).

The principle of the security function of a ground sensor with independent validation is as shown:

- Use of data for the anomaly detection

- Use of RF-signals physical properties to verify the position and validate the threat

From those a mitigation action can be derived. From a sensor perspective the mitigation is forwarding detailed target validation information by the ASTERIX CAT-246. The ASTERIX CAT-246 solves the issue of not being able to provide detailed target threat information by the ASTERIX target reports (i.e. CAT-21 for ADS-B, where there is only one bit allowing to inform of a low target confidence level). Since it is intended to standardize the CAT-246 the interoperability of target validation information can be ensured.

The ASTERIX CAT-246 allows to forward following information in a reliable manner:

- Information on detected position deviation for the respective target
- Information on data inconsistencies for the respective targets
- Information of information non-compliance of the respective targets

EUROPEAN PARTNERSHIP

Co-funded by the European Union

The ASTERIX CAT-246 is defined such that it is not limited to ADS-B, but can be used for any surveillance sensor. Furthermore the definition provides flexibility such that it can be forwarded to different downstream instances. For instance a tracker can receive the sensor target validation data by the ASTERIX CAT-246, enrich it with further information available in the tracker and output it to the further processing. This allows accommodating different potential validation infrastructures (i.e. central validation instance vs. distributed, etc.). The validation infrastructure is expected to draw final conclusion on the target report data. In case of spoofing through generation of false targets this could be the removal of the identified false target reports. However, the detailed definition of the resulting final action is out of scope of the sensor based threat detection and thus not further detailed here.

The described approach allows establishing performance figures since the security functions performance parameters (integrity, continuity, accuracy) can be linked to position information.

With a target validation capable ADS-B sensor it is seen to allow the use of ADS-B as an independent surveillance layer also in high density airspace. This allows gaining of operational benefits like:

- High accuracy surveillance – accuracy independent of range
- High update rate
- Additional target information
- Low lifecycle cost

In the following sections, EATMA information developed within PJ.14-W2-84c is exposed.

Role	Functional Block	Function
[NSV-4] T05 - Use of Secure Surveillance at TMA		
	Secure Sensor Surveillance	Security threat detection; Surveillance data acquisition; System Security threat report generation; Target Security threat report generation;

4.2.1 Resource Connectivity view (one section per NSV-1)

Resource Connectivity Model describes the use of Secure Surveillance in a TMA environment for cooperative (ADS-B and WAM) sensors:

The same is valid for ER environment.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

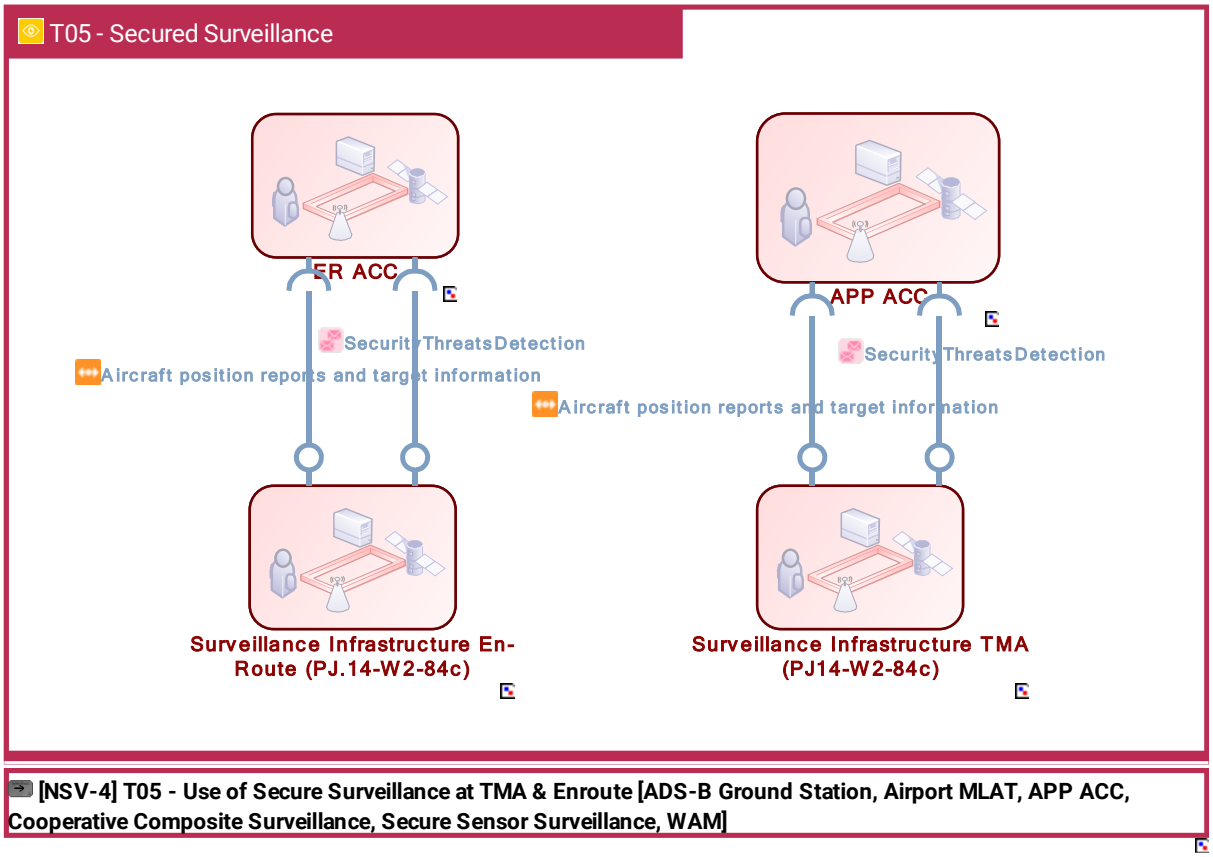


Figure 4-5 Resource Connectivity Model NSV-1

4.2.1.1 Resource Infrastructure view (of the NSV-2)

EUROPEAN PARTNERSHIP
Co-funded by the European Union

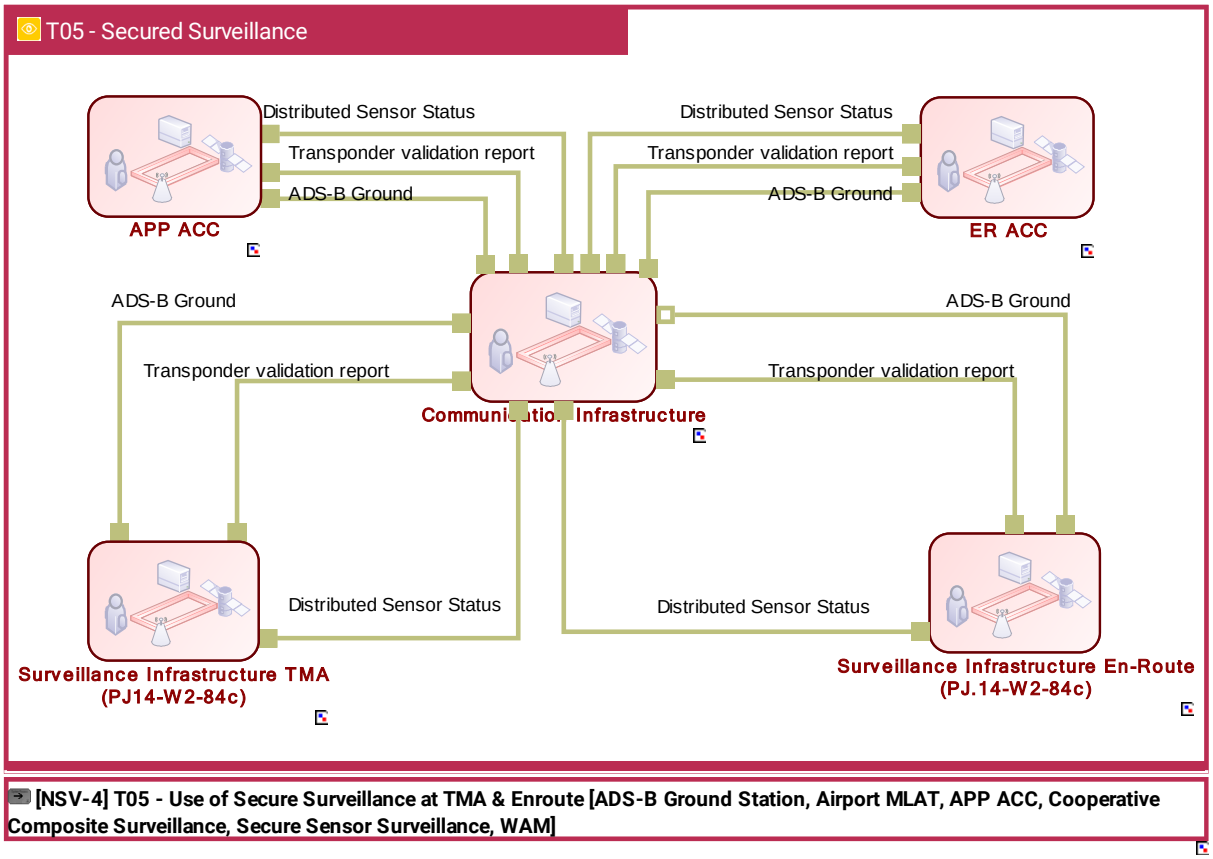


Figure 4-6 Resource Infrastructure view NSV-2

4.2.1.2 Resource Orchestration view (all NSV-4s linked to the NSV-1)

This use case describes the Secure Surveillance operation at TMA for cooperative (ADS-B and WAM) sensors:

The same is valid for ER environment.

The primary focus for PJ.14-W2-84c is on En-Route and TMA. However, the application to airport environment is covered in the reflexion.

Since PJ.14-W2-84c puts a strong focus on ADS-B with the background of enabling the use of ADS-B as independent surveillance layer in high density airspace (as is the case in ECAC), the En-route and TMA environments are of a high interest. The solution is expected to provide the largest benefits for cost efficient surveillance (CEF3) when applied to this environment. The application of PJ.14-W2-84c to airport environment is feasible and is part of the considerations performed in PJ.14-W2-84b in the context of Multiple Remote Tower surveillance sensor and surveillance for small and regional airports.

Co-funded by the European Union

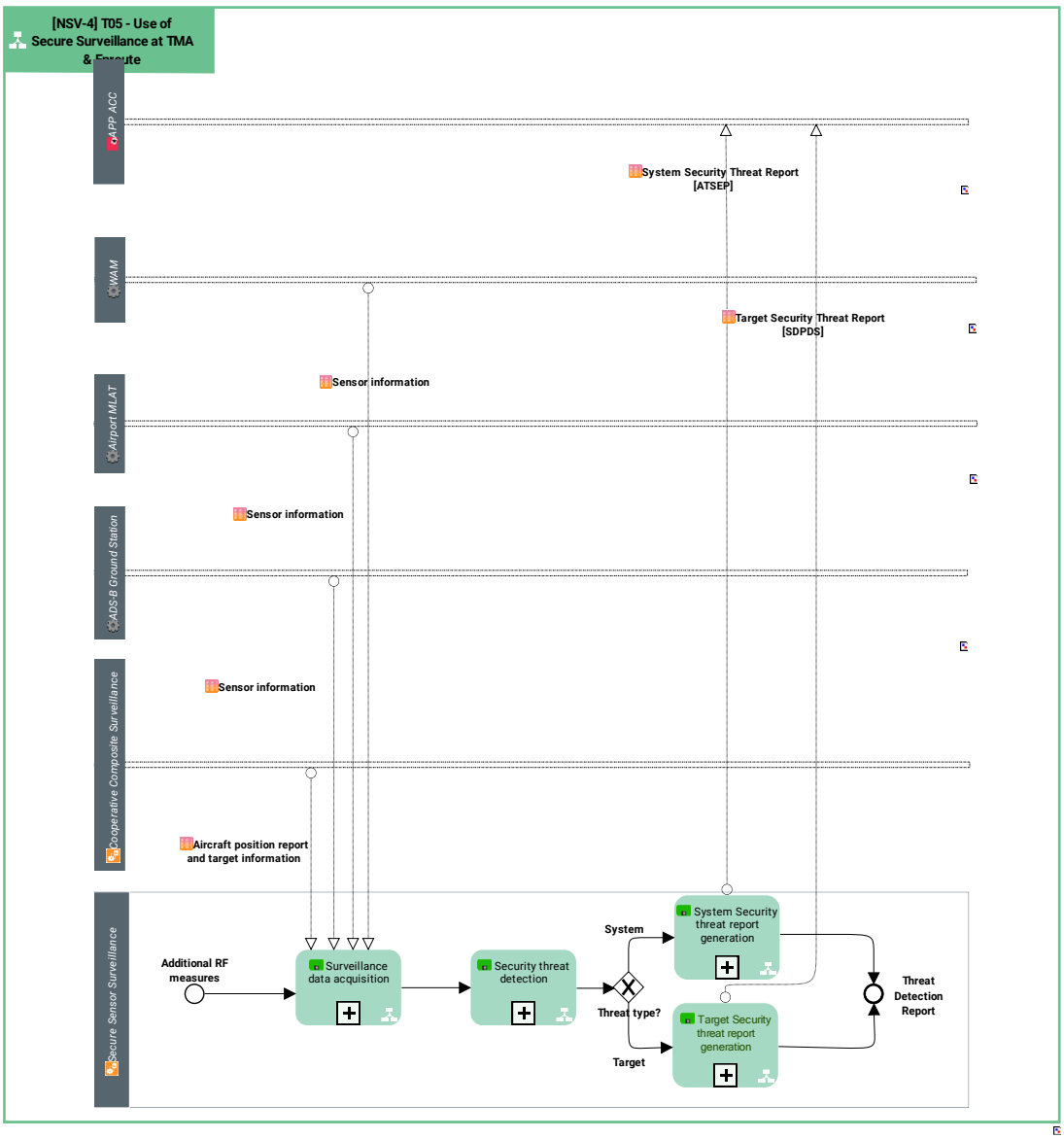


Figure 4-7 Resource Orchestration View

System/Role	Functional Block	Function
Secure Surveillance	Secure Sensor Surveillance	Security threat detection; Surveillance data acquisition; System Security threat report generation; Target Security threat report generation;

Function	Description
Security threat detection	This function receives surveillance data and detects RF security threats.
Surveillance data acquisition	This function receives data from the surveillance sensors via the TCP/IP network. This function uses standard service protocols in order to connect to the system LAN to acquire surveillance data that will be provided in standard ASTERIX format and in proprietary protocols. Surveillance data received from different sensors, locally or remotely connected, shall be available in a system LAN. Surveillance data will be provided in standard ASTERIX format. In particular: · ASTERIX Cat 10 for SMR target reports; · ASTERIX Cat 10 for MLAT target reports; · ASTERIX Cat 20 for MLAT target reports; · ASTERIX Cat 21 for ADS-B target reports; · ASTERIX Cat 48 for Radar target reports. Security threat information is provided in draft ASTERIX format: · ASTERIX Cat 246 for Target Validation.
System Security threat report generation	This functions generates system security threat reports intended for ATSEP.
Target Security threat report generation	This functions generates target security threat reports intended for secure surveillance chain.

4.2.2 Resource Composition

Infrastructure connectivity model for TMA cooperative sensors (ADS-B and WAM):

EUROPEAN PARTNERSHIP

Co-funded by the European Union

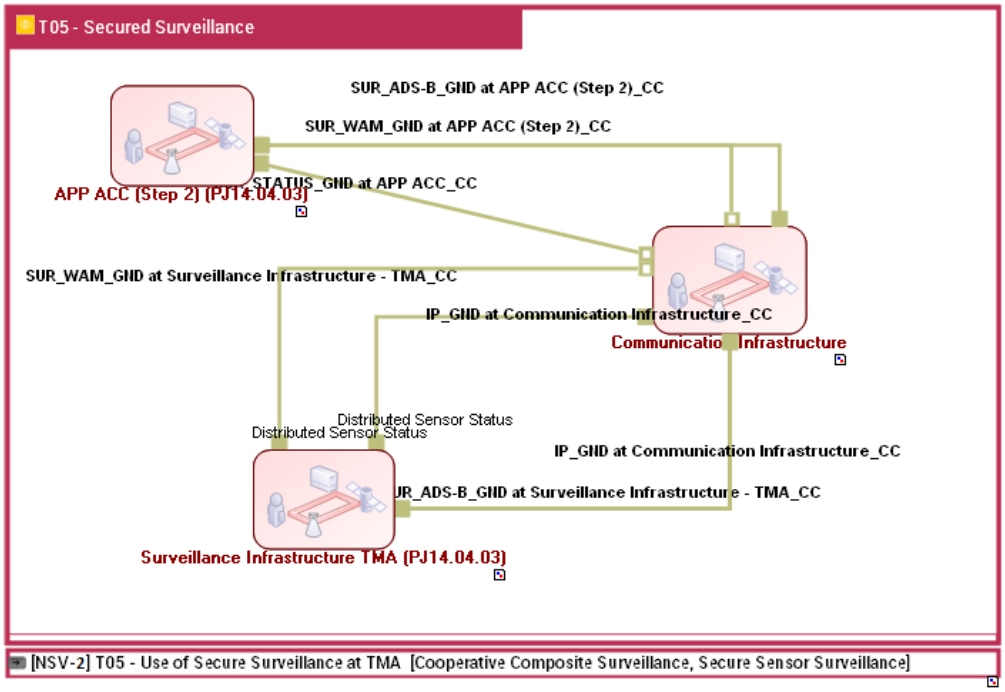
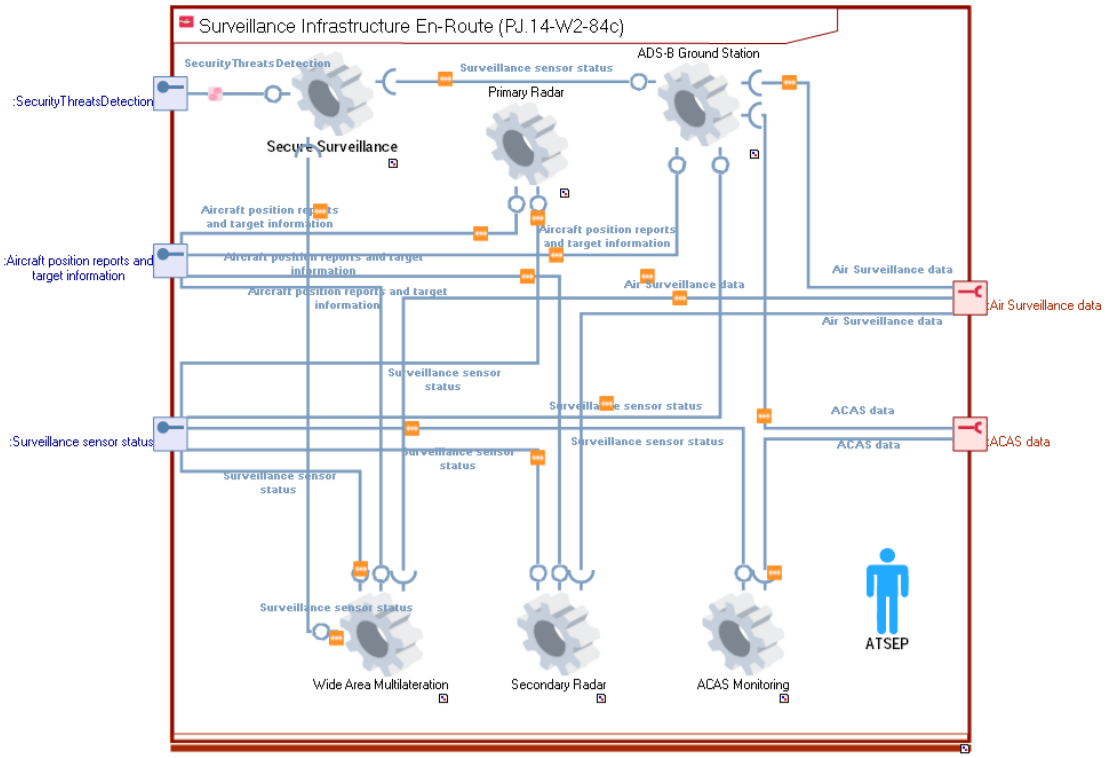


Figure 4-8 Resource Connectivity Model NSV-2

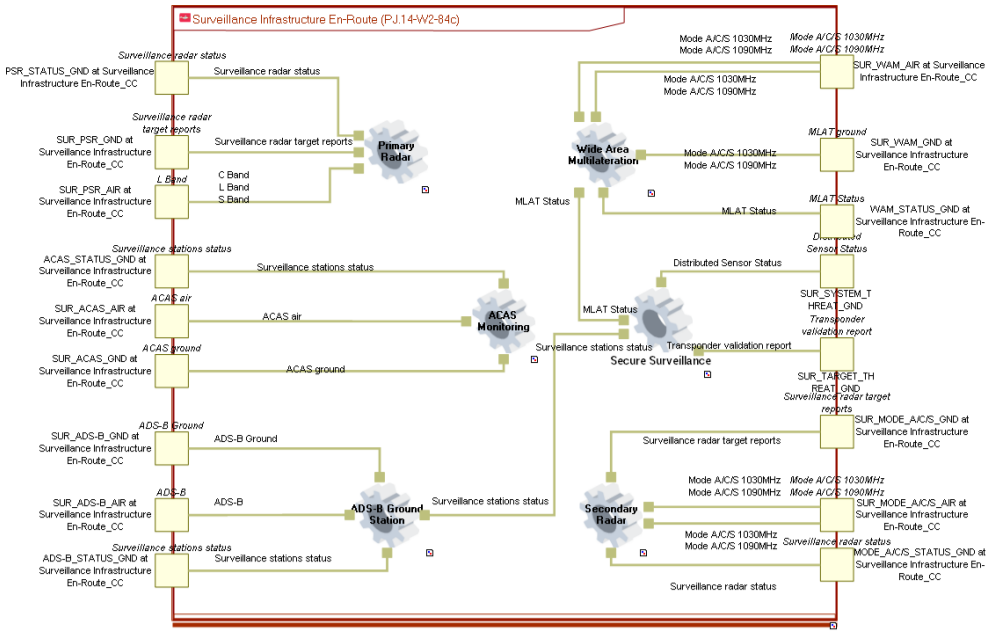
4.2.2.1 Surveillance Infrastructure En-Route (PJ14-W2-84c)

4.2.2.1.1 Structure



4.2.2.1.2 Infrastructure

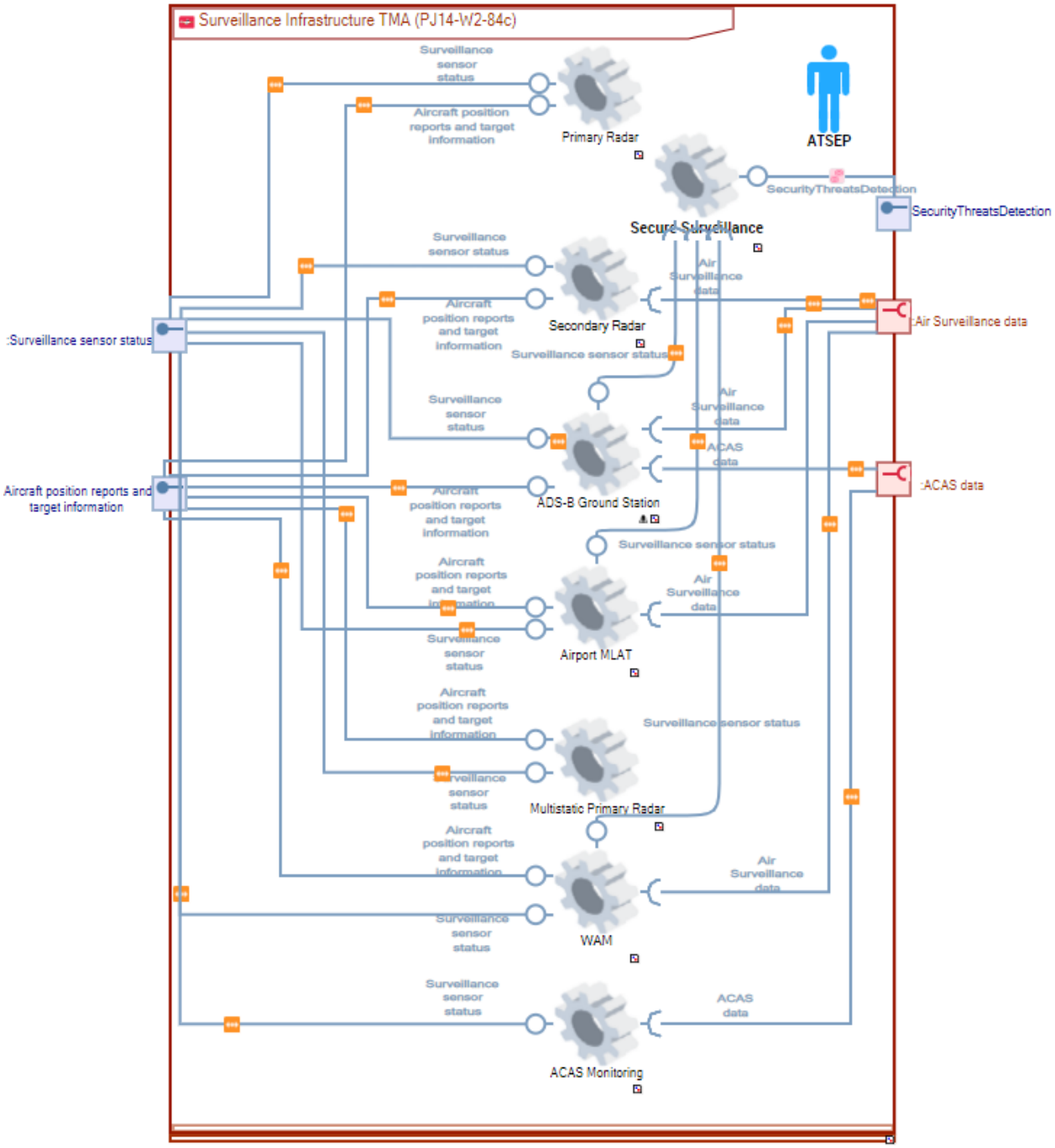
EUROPEAN PARTNERSHIP
Co-funded by the European Union



4.2.2.2 Surveillance Infrastructure TMA (PJ14-W2-84c)

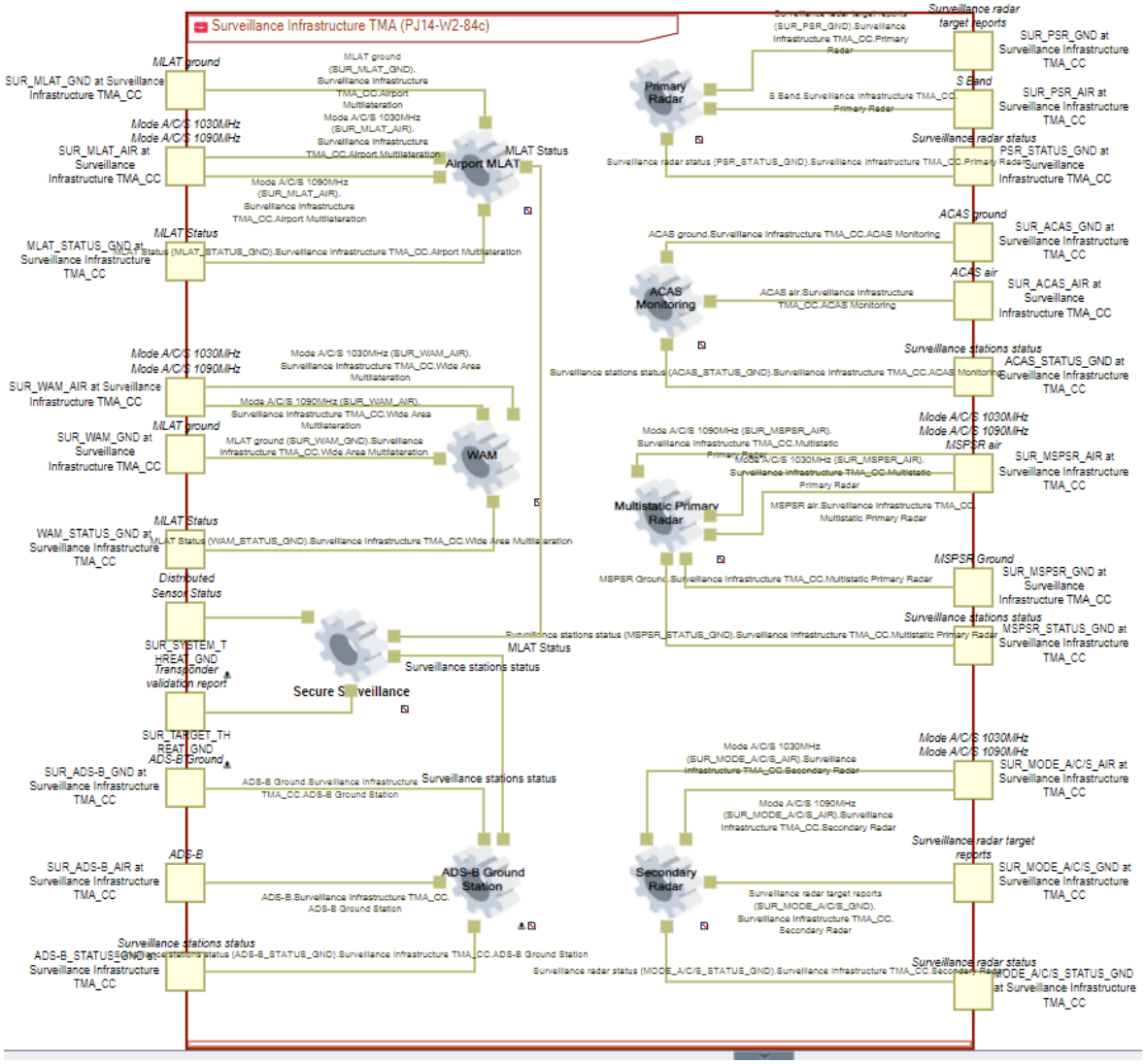
4.2.2.2.1 Structure

EUROPEAN PARTNERSHIP
Co-funded by the European Union



4.2.2.2.2 Infrastructure

EUROPEAN PARTNERSHIP
Co-funded by the European Union



4.2.2.3 Secure Surveillance Technical System

Secure Surveillance Technical System acquires the surveillance sensor information (ASTERIX Cat 10, 20, 21, 48, 246), and provides system and target security threat reports.

4.2.2.3.1 Composition

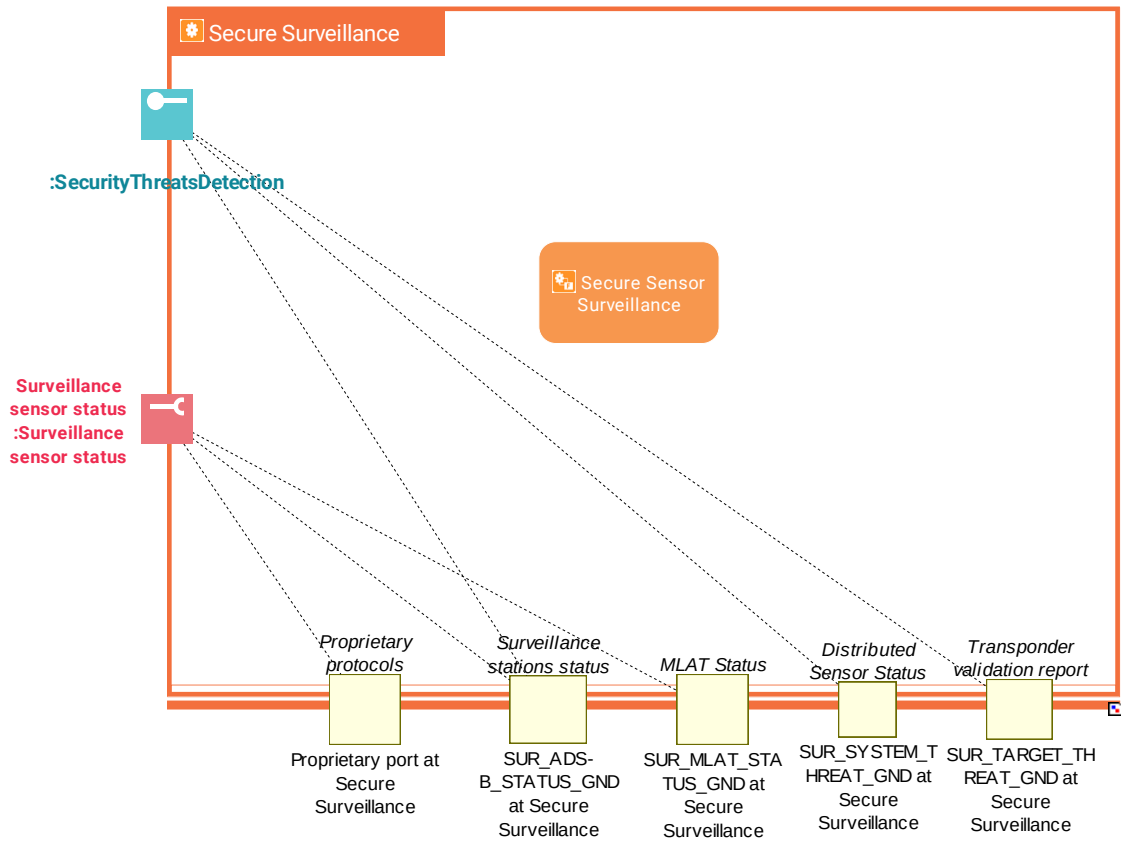


Figure 4-9: System Interfaces Diagram

4.2.3 Service view

4.2.3.1 Service description

Service	Service description
SecurityThreatDetection	Detection and reporting of security threats that might affect surveillance chain. Consists of two interfaces: • SystemThreatDetection • TargetThreatDetection

4.2.3.2 Service Provisioning

Interaction	Consumer CC	Consumer System	Provider CC	Provider System
Aircraft position reports and target information	ER ACC	En-Route / Approach ATC;	Surveillance Infrastructure En-Route (PJ.14-W2-84c)	Secondary Radar; ADS-B Ground Station; Wide Area Multilateration; Primary Radar;

Co-funded by the European Union

Interaction	Consumer CC	Consumer System	Provider CC	Provider System
SecurityThreatsDetection	APP ACC	En-Route / Approach ATC;	Surveillance Infrastructure TMA (PJ14-W2-84c)	Secure Surveillance;
Aircraft position reports and target information	APP ACC	En-Route / Approach ATC;	Surveillance Infrastructure TMA (PJ14-W2-84c)	Multistatic Primary Radar; ADS-B Ground Station; Secondary Radar; Airport MLAT; WAM; Primary Radar;
SecurityThreatsDetection	ER ACC	En-Route / Approach ATC;	Surveillance Infrastructure En-Route (PJ.14-W2-84c)	Secure Surveillance;

4.2.3.3 Service Realization

4.2.3.3.1 Interaction Aircraft position reports and target information

System Port: IP_GND at Communication Infrastructure_CC

Protocol Stack	Protocol
IP	

System Port: SUR_ADS-B_GND at APP ACC_CC

Protocol Stack	Protocol
ADS-B Ground	
	Asterix Cat21
	UDP
	IP

System Port: IP_GND at Communication Infrastructure_CC

Protocol Stack	Protocol
IP	

System Port: SUR_ADS-B_GND at Surveillance Infrastructure TMA_CC

Protocol Stack	Protocol
ADS-B Ground	
	Asterix Cat21
	UDP
	IP

EUROPEAN PARTNERSHIP

Co-funded by the European Union

4.2.3.3.2 Interaction Aircraft position reports and target information

Interaction SecurityThreatsDetection

Service Interface Definition	
SystemThreatDetection	
Standard	**MEP, Security Configuration, Interface Bindings**
Asterix Cat21	ECTL Standard SUR.ET1.ST05.2000-STD-12-01
Asterix Cat25	

Service Interface Definition	
TargetThreatDetection	
Standard	**MEP, Security Configuration, Interface Bindings**
Asterix Cat 246	

4.2.3.3.3 Interaction SecurityThreatsDetection

System Port: IP_GND at Communication Infrastructure_CC

Protocol Stack	Protocol
IP	

System Port: SUR_ADS-B_GND at APP ACC_CC

Protocol Stack	Protocol
ADS-B Ground	
	Asterix Cat21
	UDP
	IP

System Port: IP_GND at Communication Infrastructure_CC

Protocol Stack	Protocol
IP	

System Port: SUR_ADS-B_GND at Surveillance Infrastructure TMA_CC

Protocol Stack	Protocol
ADS-B Ground	
	Asterix Cat21
	UDP
	IP

System Port: IP_GND at Communication Infrastructure_CC

Protocol Stack	Protocol

EUROPEAN PARTNERSHIP

Co-funded by the European Union

IP	

System Port: SUR_SYSTEM_THREAT_GND

Protocol Stack	Protocol
Distributed Sensor Status	
	Asterix Cat25
	IP
	UDP

System Port: SUR_SYSTEM_THREAT_GND

Protocol Stack	Protocol
Distributed Sensor Status	
	Asterix Cat25
	IP
	UDP

System Port: IP_GND at Communication Infrastructure_CC

Protocol Stack	Protocol
IP	

System Port: IP_GND at Communication Infrastructure_CC

Protocol Stack	Protocol
IP	

System Port: SUR_TARGET_THREAT_GND

Protocol Stack	Protocol
Transponder validation report	
	Asterix Cat 246
	UDP
	IP

System Port: SUR_TARGET_THREAT_GND

Protocol Stack	Protocol
Transponder validation report	
	Asterix Cat 246
	UDP
	IP

Co-funded by the European Union

System Port: IP_GND at Communication Infrastructure_CC

Protocol Stack	Protocol
IP	

Service Interface Definition	
SystemThreatDetection	
Standard	**MEP, Security Configuration, Interface Bindings**
Asterix Cat21	ECTL Standard SUR.ET1.ST05.2000-STD-12-01
Asterix Cat25	

Service Interface Definition	
TargetThreatDetection	
Standard	**MEP, Security Configuration, Interface Bindings**
Asterix Cat 246	

4.2.3.3.4 Interaction SecurityThreatsDetection

Service Interface Definition	
SystemThreatDetection	
Standard	**MEP, Security Configuration, Interface Bindings**
Asterix Cat21	ECTL Standard SUR.ET1.ST05.2000-STD-12-01
Asterix Cat25	

Service Interface Definition	
TargetThreatDetection	
Standard	**MEP, Security Configuration, Interface Bindings**
Asterix Cat 246	

4.3 Functional and non-Functional Requirements

4.3.1 General Requirements

[REQ]

Identifier	REQ-14.84c-TS-GENR.0001

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Title	Mode A/C/S threats detection
Requirement	The surveillance sensor **shall** apply security functions capable to detect security threats related to the transmission of Mode A/C and Mode-S Extended Squitter data at 1090 MHz (ADS-B).
Status	<Validated>
Rationale	The surveillance sensor has to cover transmissions of civil aircraft equipped with a Mode S transponder.
Category	<Security>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-GENR.0002
Title	GPS L1 threats detection
Requirement	The surveillance sensor **shall** apply security functions capable to detect security threats related to the reception of information provided by GPS on L1 frequency.
Status	<Validated>
Rationale	The L1 frequency it is the only considered due to the following: First, L2 is modulated with the military chip signal, which is not available to civil users (included aeronautics). Thus, receivers apply semi-codeless processing to get the signal. The signal is extremely noise and very weak and thus not desirable to be used. Second, L2 is not a frequency in the protected aeronautical radio range. Any interferences may happen in L2 and one has no legal mean to/responsible to ensure freedom of interference. Due to that, for aeronautical applications L2 is in general not considered (exception SBAS RIMS, but there are specific arguments and it is expectable that with broader availability of L5 SBAS will switch to L5).

Co-funded by the European Union

	In summary L2 is generally not to be considered for aeronautical use.
Category	<Security>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-GENR.0003
Title	Target threats detection
Requirement	The security function **shall** be capable of detecting threat conditions related to specific targets, as well as ADS-B sensor system wide security threats.
Status	<Validated>
Rationale	The threats can be classified to affect either the entire system or a single or few targets. Threats can be further subdivided as at signal or content level in the next categorization: - Threats at signal level: - Threats at ADS-B content level: - Threats at WAM content level - Time Synchronisation
Category	<Security>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Co-funded by the European Union

Identifier	REQ-14.84c-TS-GENR.0004
Title	Threat classification (ADS-B)
Requirement	The ADS-B security function **shall** be capable of detecting the following threat conditions: - Overpowering of system by noise (Threat 14, Threat 15, Threat 17) - Jamming (Threat 16A) - Modification of existing targets (Threat 16B, Threat 16C) - Duplicated tracks (Threat 16C, Threat 25A, Threat 25C) - Modified target data (Threat 25A) - Delayed and re-injected real tracks (Threat 25A) - Simulation of non-real targets (Threat 24A, Threat 24B, Threat 25B, Threat 25D) - Frustrate track initiation (Threat 16F) - Time synchronisation interference (Threat 20)
Status	<Validated>
Rationale	In SESAR 15.04.06 project, different threats were developed and studied. The list of threats has been established with the aim of studying the integrity and performance values that can be achieved by the system for their detection. The threat ID's follow the classification in GEN-SUR-SEC.
Category	<Security>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-GENR.0005

Co-funded by the European Union

Title	Threat classification (WAM)
Requirement	The WAM security function **shall** be capable of detecting the following threat conditions: - Overpowering of system by noise (Threat 15, Threat 17) - Jamming (Threat 16A) - Modification of existing targets (Threat 16D, Threat 16E) - Time synchronisation interference (Threat 19)
Status	<Validated>
Rationale	In SESAR 15.04.06 project, different threats were developed and studied. The list of threats has been established with the aim of studying the integrity and performance values that can be achieved by the system for their detection. The threat ID's follow the classification in GEN-SUR-SEC.
Category	<Security>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-GENR.0006
Title	Satellite clock threats
Requirement	The surveillance security function **shall** be capable of detecting satellite clock threats (Threat 20A, Threat 20B, Threat 21, Threat 22).
Status	<Validated>

Rationale	In SESAR 15.04.06 project, different threats were developed and studied. The list of threats has been established with the aim of studying the integrity and performance values that can be achieved by the system for their detection. The threat ID's follow the classification in GEN-SUR-SEC.
Category	<Security>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-GENR.0007
Title	System threat detection function
Requirement	The system **shall** provide means to enable/disable each system threat detection function individually.
Status	<Validated>
Rationale	To ensure that a malfunction of one of the functions of the system does not affect the general operation of the whole system.
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-GENR.0008
Title	Threat reporting
Requirement	The system **shall** be able to report automatically the indication of the Security threat detection.
Status	<Validated>
Rationale	Detection and reporting of threats need to be automatic
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

EUROPEAN PARTNERSHIP

Co-funded by the European Union

4.3.2 Threats Detection

[REQ]

Identifier	REQ-14.84c-TS-TDET.0001
Title	Target flags
Requirement	The system shall be able to indicate the detection of a security threat results which could be associated to targets by raising an indicator/flag in ASTERIX CAT 21 and providing detailed information of the detected threat in ASTERIX CAT 246 (Target Validation Message) Additional information may be provided through dedicated protocols (SNMP). *Note: The category number of ASTERIX CAT246 may change later.*
Status	<Validated>
Rationale	ASTERIX used to distribute generic information. Simple Network Management Protocol (SNMP) used to provide the exchange of detail information.
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-TDET.0002
Title	Detection of rise in received targets (ADS-B)
Requirement	The ADS-B sensor **shall** be able to detect a sudden rise of received number of targets. *Note: The sensor compares units.* *Single unit: Number of received targets over a particular period of time. (User defined threshold).*

EUROPEAN PARTNERSHIP

Co-funded by the European Union

	The background is to detect spoofing conditions at the sensor level.
Status	<Validated>
Rationale	Detection method for Threats. Detection
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

Co-funded by the European Union

4.3.3 External Interface

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0001
Title	ASTERIX outputs
Requirement	The surveillance sensor **shall** support following outputs: - ADS-B target data Output Channel ASTERIX CAT 021 - ADS-B and/or WAM System Output Status ASTERIX CAT 025 - WAM target data Output Channel ASTERIX CAT 020 - ASTERIX target validation message ASTERIX CAT 246
Status	<Validated>
Rationale	Editions currently in use are the following: - ASTERIX CAT021 Edition 2.4 - ASTERIX CAT025 Edition 1.1 - ASTERIX CAT020 Edition 1.9 - ASTERIX CAT246 Edition 0.12.06
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0002
Title	ASTERIX outputs (optional)
Requirement	The surveillance sensor **should** support following outputs: - Surface Movement Radar Outputs ASTERIX CAT 010 - WAM/MLAT System Output Status ASTERIX CAT 019

Co-funded by the European Union

	- System Output Status ASTERIX CAT 023
Status	<Validated>
Rationale	Editions currently in use are the following: - ASTERIX CAT010 Edition 1.1 - ASTERIX CAT019 Edition 1.3 - ASTERIX CAT023 Edition 1.2
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0003
Title	Flag in field I021/040
Requirement	The ADS-B security function **shall** flag detected targets in ASTERIX CAT 021, "Target Report Descriptor" field I021/040, first extension field, by setting the confidence level to "Report suspect" bits-3/2 (CL) to "1".
Status	<Validated>
Rationale	In the ASTERIX CAT 021 the confidence level is set to "Report suspect" meaning that the target is possible under threat condition. The information about the threat itself is contained in the 025 CAT reports for system related threats. For target related threats there is no standard compliant mean to forward detection details. A new system independent ASTERIX category could support the forwarding of such information.
Category	<Functional>

EUROPEAN PARTNERSHIP

Co-funded by the European Union

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0004
Title	Flag in field I020/030
Requirement	The WAM security function **shall** flag detected targets in ASTERIX CAT 020, "Warning/Error Conditions" field I020/030 by setting Code 15 Transponder anomalies
Status	<Validated>
Rationale	Initial analysis of WAM related security threats has shown that WAM is very robust with respect to target related security threats. The initial analysis showed the need to forward detected threats at target level resulting from some Mode A/C/S code vulnerabilities covering the target data modification threat. Thus, the transponder related error code 15 is chosen to flag the respective detection. Not yet considered are ADS-B / WAM comparison and other threats. Additional error codes, are **optionally** applied: - Code 3 split plot to flag modified target data (for instance due ADS-B – WAM position comparison); - Code 10 for spoofed targets.
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09

Co-funded by the European Union

<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0018
Title	Validation information in ASTERIX CAT 246
Requirement	The surveillance security function **shall** provide information on detected target threats in ASTERIX CAT 0246 as follows: - Data Modification (threat 16B) is indicated by I246/200 with the ASTERIX Element providing information on the type of modification - Target Suppression (threat 16F) is indicated by I246/100 ERR = 1 with ELE to indicate no position, PAS to indicate no target report is provided in ASTERIX CAT21 - Spoofing with Position Jump as per MOPS is indicated by I246/200 ((+ I246/210)) ELE to indicate position; PAS to indicate no CAT21 plot; EAS=2; VTP = 0 - Spoofing (threat 24A, 25A) with Horizontal speed anomaly is indicated by I246/200 + I246/220 with PAS=3; ELE=3; VST=2; VTP=1 - Spoofing (threat 24A, 25A) with Position anomaly is indicated by I246/110 with ELE=1, PAS=1, EAS=1, VST=2, VTP=1 - Spoofing (threat 24A, 25A) with Altitude anomaly is indicated by I246/110 with ELE=2, PAS=1, EAS=1, VST=2, VTP=1 - Spoofing (threat 24A, 25A) with Vertical speed anomaly is indicated by I246/200 ELE=12, PAS=1, VST=2, EAS=1, VTP=1 - Spoofing showing up as non-conforming transponder is indicated by I246/100 ERR = 2 - Spoofing (threat 24A, 25A) with an erroneous position validated with a squitters triggered by the ground sensor is indicated by I246/200 + I246/210 X-East; y-North; If no valid squitter: max. rng, max. std.dev ELE=1; PAS=1; EAS=1; VST=2; VTP=1 - Spoofing (threat 24A, 25A) with an erroneous position validated with the squitters received by the ground sensor is indicated by I246/110 + I246/120, … - Target duplication (threat 24B) is indicated by I246/300. Additional information on the target characterisation (position, speed) may be provided by I246/200. Note 1: Non-compliant aircraft transponders can cause triggers by the ground sensor security detectors. Note 2: A validated erroneous position refers to quantification of the position error within the ground sensor through an independent measurement. In these cases, the information on the position of the spoofer will be provided by the CAT 246.

Co-funded by the European Union

Status	<Validated>
Rationale	ASTERIX used to distribute target threat information
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0005
Title	Flag in field I025/105 I
Requirement	The security function **shall** flag detected system threats in ASTERIX CAT 025 as follows: - **System** wide related time synchronisation threats leading to invalid time source is flagged by I025/105 Code 2
Status	<Validated>
Rationale	ASTERIX used to distribute generic information. A time source is considered as valid when either externally synchronized or running on a local oscillator within the required accuracy of UTC. *Code 2 of data item I025 / 105 of the ASTERIX category 025 is the one, according to the specification, that must be flagged In case of* 'Time Source Invalid'.
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09

Co-funded by the European Union

<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0006
Title	Flag in field I025/105 II
Requirement	The security function **shall** flag detected system threats in ASTERIX CAT 025 as follows: - **System** wide time synchronisation threats leading to coasting of the time reference are flagged by I025/105 Error Code 3
Status	<Validated>
Rationale	ASTERIX used to distribute generic information. A time source is considered as valid when either externally synchronized or running on a local oscillator within the required accuracy of UTC. Code 3 of data item I025 / 105 of the ASTERIX category 025 is the one, according to the specification, that must be flagged in case of '*Time Source Coasting '* of the system.
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0007
Title	Flag in field I025/105 III
Requirement	The security function **shall** flag detected system threats in ASTERIX CAT 025 as follows:

Co-funded by the European Union

	- **System** wide data processor overload is flagged by I025/105 Error code 5
Status	<Validated>
Rationale	ASTERIX used to distribute generic information *Code 5 of data item I025 / 105 of the ASTERIX category 025 is the one, according to the specification, that must be flagged In case of* 'Data Processor Overload'.
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0008
Title	Flag in field I025/105 IV
Requirement	The security function **shall** flag detected system threats in ASTERIX CAT 025 as follows: - **System** wide ground interface data communications overload is flagged by I025/105 Error code 6
Status	<Validated>
Rationale	ASTERIX used to distribute generic information *Code 6 of data item I025 / 105 of the ASTERIX category 025 is the one, according to the specification, that must be flagged In case of* 'Ground Interface Data Communications Overload'.
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c

Co-funded by the European Union

<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0009
Title	Flag in field I025/105 V
Requirement	The security function **shall** flag detected system threats in ASTERIX CAT 025 as follows: - **System** wide interference at 1090 MHz shall is flagged by I025/105 Error Code 32
Status	<Validated>
Rationale	ASTERIX used to distribute generic information. Error codes in the range from 32 to 255 of the data item I025/105 are available for specification by the system manufacturers. They are not standardized and shall be described for each applicable case. Therefore, the Code 32 in this project is defined to flag all detected threats related to 'System wide interference at 1090 MHz'
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0010
Title	Flag in field I025/105 VI

Co-funded by the European Union

Requirement	The security function **shall** flag detected system threats in ASTERIX CAT 025 as follows: - **System** wide GPS interference at L1 is flagged by I025/105 Code 35
Status	<Validated>
Rationale	ASTERIX used to distribute generic information. Error codes in the range from 32 to 255 of the data item I025/105 are available for specification by the system manufacturers. They are not standardized and shall be described for each applicable case. Therefore, the Code 35 in this project is defined to flag all detected threats related to 'System wide GPS interference at L1'.
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0011
Title	Flag in field I025/120
Requirement	The security function **shall** flag detected system threats in ASTERIX CAT 025 as follows: - **GS** related interference at 1090 MHz is flagged by I025/120 Error Code 16
Status	<Validated>
Rationale	ASTERIX used to distribute generic information. Error codes in the range from 16 to 63 of the data items I025/120 are available for specification by the system manufacturers. They are not standardized and shall be described for each applicable case. Therefore, the Code 16 in this project is defined to flag all detected threats related to 'GS related interference at 1090 MHz' of the system.

Co-funded by the European Union

Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0012
Title	Flag in field I025/120 II
Requirement	The security function **shall** flag detected system threats in ASTERIX CAT 025 as follows: - **GS** related excessive processor load is flagged by I025/120 Code 17
Status	<Validated>
Rationale	ASTERIX used to distribute generic information. Error codes in the range from 16 to 63 of the data item I025/120 are available for specification by the system manufacturers. They are not standardized and shall be described for each applicable case. Therefore, the Code 17 in this project is defined to flag all detected threats related to 'GS related excessive processor load' of the system.
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0013

Co-funded by the European Union

Title	Flag in field I025/120 III
Requirement	The security function **shall** flag detected system threats in ASTERIX CAT 025 as follows: - **GS** related processor overload is flagged by I025/120 Code 18
Status	<Validated>
Rationale	ASTERIX used to distribute generic information. Error codes in the range from 16 to 63 of the data items I025/120 are available for specification by the system manufacturers. They are not standardized and shall be described for each applicable case. Therefore, the Code 18 in this project is defined to flag all detected threats related to 'GS related processor overload' of the system.
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0014
Title	Flag in field I025/120 IV
Requirement	The security function **shall** flag detected system threats in ASTERIX CAT 025 as follows: - **GS** related time synchronisation threats leading to coasting of the time reference are flagged by I025/120 Error Code 19
Status	<Validated>

Co-funded by the European Union

Rationale	ASTERIX used to distribute generic information. Error codes in the range from 16 to 63 of the data items I025/120 are available for specification by the system manufacturers. They are not standardized and shall be described for each applicable case. Therefore, the Code 19 in this project is defined to flag all detected threats related to 'GS related time synchronisation threats leading to coasting of the time reference' of the system
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0015
Title	Flag in field I025/120 V
Requirement	The security function **shall** flag detected system threats in ASTERIX CAT 025 as follows: - **GS** related time synchronisation threats leading to invalid time source are flagged by I025/120 Code 20
Status	<Validated>
Rationale	ASTERIX used to distribute generic information. Error codes in the range from 16 to 63 of the data items I025/120 are available for specification by the system manufacturers. They are not standardized and shall be described for each applicable case. Therefore, the Code 20 in this project is defined to flag all detected threats related to 'GS related time synchronisation threats leading to invalid time source' of the system.
Category	<Functional>

Co-funded by the European Union

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0016
Title	Flag in field I025/120 VI
Requirement	The security function **shall** flag detected system threats in ASTERIX CAT 025 as follows: - **GS** related interference at GPS L1 is flagged by I025/120 Error Code 21
Status	<Validated>
Rationale	ASTERIX used to distribute generic information. Error codes in the range from 16 to 63 of the data item I025/120 are available for specification by the system manufacturers. They are not standardized and shall be described for each applicable case. Therefore, the Code 21 in this project is defined to flag all detected threats related to 'GS related interference at GPS L1' of the system.
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-EXIN.0017
Title	Storage of information

Co-funded by the European Union

Requirement	The system **shall** store all Security configuration parameters in a persistent memory.
Status	<Validated>
Rationale	If a network error or system crash occurs (intentional or fortuitous), users need to know that the application will be available when their systems recover in the same conditions in which it was configured before the event.
Category	<Functional>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

EUROPEAN PARTNERSHIP

Co-funded by the European Union

4.3.4 Performance

[REQ]

Identifier	REQ-14.84c-TS-PERF.0001
Title	Continuity of security function
Requirement	The Continuity of security function per threat – **probability of false alarm** – shall be compliant with the operational impact. Note: the operational impact depends on multiple factors like the embodiment of the SUR sensor in the SUR chain and the kind of threat and its impact on the capability to ensure safe aircraft separations which furthermore depends on the type of airspace and number of flights. This requires to perform an individual analysis per threat per sensor. The following can be assumed to fulfil the performance needs in high density En-route airspace: - the max. acceptable total alarm rate is 1/h - N targets / d = 2500 - n detectors = 20 - n ground station = 10 performing the security assessment in parallel - one assessment interval (epoch) is 30 s This leads to a probability of false alarm per epoch, per target, per ground station and per detector of ~ 2 x 10E-8. Depending on the embodiment in the architecture and actual design hence an individual sensor threat detection false alarm probability of 1 x 10E-4/epoch is acceptable
Status	<Validated>
Rationale	As there are no reference values concerning this parameter, the final intention of this requirement is to determine the performance values acceptable for Secured Surveillance in relation with the 'Continuity of Security Function'. The Continuity of the Security Function Value should be defined per operational volume after a first analysis of the values of the system under no threats operation. This parameter is directly related to the integrity of Security Function value.
Category	<Functional>, <Performance>

Co-funded by the European Union

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-PERF.0002
Title	Integrity of security function
Requirement	The Integrity of security function per threat – **probability of missed detection** – **shall** be compliant with the operational impact. Note: the operational impact depends on multiple factors like the embodiment of the SUR sensor in the SUR chain and the kind of threat and its impact on the capability to ensure safe aircraft separations which furthermore depends on the type of airspace and number of flights. This requires to perform an individual analysis per threat per sensor. Assuming for a high density airspace total acceptable risk of a missed detection of a security threat 1x10E-7/h based on the consideration that aircraft are ACAS equipped and furthermore considering that a target is simultaneously observed by at least two ground stations (due redundancy, for 99.9% of the time) and assuming a prior probability of the existence of a security threat of 0.01 (this would translate to a security threat of ~15 minutes every day and hence is a conservative assumption) a probability of threat detection of ~1x10E-2 is needed. It also needs to be taken into account that certain threats may be unknown. With the conservative assumption that the implemented means detect only 10% of the potential threats the implemented detectors need to achieve a detection probability of ~1-1x10E-3. A driving factor for a real world probability of threat detection is the probability of update / the probability to receive the affected messages and also the Bit-error rate during reception.
Status	<Validated>
Rationale	The Integrity of the Security Function Value should be defined per operational volume after a first analysis of the values of the system under no threats operation. This parameter is directly related to the Continuity of Security Function value.
Category	<Functional>, <Performance>

EUROPEAN PARTNERSHIP

Co-funded by the European Union

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-PERF.0003
Title	Time to alarm
Requirement	The time to alarm per threat **shall** be compliant with the operational impact. Note: the operational impact depends on multiple factors like the embodiment of the SUR sensor in the SUR chain and the kind of threat and its impact on the capability to ensure safe aircraft separations which furthermore depends on the type of airspace and number of flights. This requires to perform an individual analysis per threat per sensor. Depending on the type of threat values between 30 s and 60 s may be needed to ensure safe operation.
Status	<Validated>
Rationale	As there are no reference values concerning this parameter, the final intention of this requirement is to determine the performance values acceptable for Secured Surveillance in relation with the 'Time to alarm'. The Time to Alarm Value should be defined as a maximum value of time for the prototype to generate the appropriate alarm from the moment when the Threat is introduced.
Category	<Functional>, <Performance>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09

Co-funded by the European Union

<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

[REQ]

Identifier	REQ-14.84c-TS-PERF.0004
Title	Accuracy of security function
Requirement	The accuracy per threat (max thresholds) **shall** be compliant with the operational impact. Note 1: Accuracy is related to the nominal behaviour of the threat detectors. Note 2: Accuracy relates primarily to measurable values. For status values by a data broadcast the accuracy is related to the digit of the value itself.
Status	<Validated>
Rationale	As there are no reference values concerning this parameter, the final intention of this requirement is to determine the performance values acceptable for Secured Surveillance in relation with the 'Accuracy of security function'. The Accuracy of the Security Function Value should be defined per operational volume after a first analysis of the values of the system under no threats operation. This value definition will be related to the values of continuity of security function and Integrity of Security Function.
Category	<Functional>, <Performance>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<SATISFIES>	<SESAR Solution>	PJ.14-W2-84c
<SATISFIES>	<Enabler>	CTE-S09
<ALLOCATED_TO>	<Functional block>	Secure Sensor Surveillance

EUROPEAN PARTNERSHIP

Co-funded by the European Union

5 Recommendation for Implementation

The security functions specified in the previous section are related to ADS-B ground segment level and WAM/MLAT systems. Implementation in SESAR is performed in line with the specification aiming on determination of the security functions performance in preparation of future operational use. Thus, the implementation may include additional “debug” outputs and potential limitations in the detection capabilities compared to future operational systems.

Furthermore, the current implementation aims to ensure the feasibility of threat detection by the security function and determining according performance figures as part of the validation.

The validation process is explained more in detail in the Technical Validation Plan (TVALP, ref. [25]). That validation process consists in the analysis of the security functions developed by the project member Thales. They are implemented in accordance with the technical specifications defined in this document. The process ensures that each solution (each ground system) complies with the requirements defined.

The manufacturer uses a composite system to implement the security function. These composite systems consist of various ADS-B+WAM ground stations.

Furthermore, it has to be considered that although a composite system is used the security functions are aimed to support also each sensor mode individually. The focus of the security function is to ensure correctness of ADS-B information.

Hence the implementation of the security function is feasible on ADS-B only (ensuring ADS-B can be used as own surveillance layer), composite ADS-B + WAM and partially WAM (the vulnerability of the latter is much lower).

In addition, the security function could be implemented in other types of composite surveillance (e.g. ADS-B+Mode S radar) but is out of scope of this project.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

6 Assumptions

It is assumed that:

- The primary concern of the research on the security functions within SESAR is related to threats on the RF-interfaces. Physical security (like access control etc.) and network security do not deviate from existing systems.
- The surveillance sensors role in security threat mitigation is related to the detection and reporting of threat conditions.
- Threat validation is part of validation functions in composite surveillance and downstream ATC-processing.
- The foremost interest of the downstream processing is information on the validity of target reports. It does not need details on causes of a threat detected at target level.

At the current stage the definition of mitigation means is not part of this solution. The security function at sensor level is limited to detection and reporting of threat conditions. This allows an ATC system integrator to apply individual mitigation means according to the actual operational needs. Such mitigations could be filtering out suspicious targets, forwarding the information to dedicated instance, etc. The actual operational needs may differ between the different ANSPs so that they are not specified in a generic way.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

7 References and Applicable Documents

7.1 Applicable Documents

Content Integration

[1] EATMA guidance material and report, Dec 2019.

[2] EATMA Community pages.

Content Development

[3] Concept of Operations, Dec 2019.

System and Service Development

[4] Report of the progress on standardisation of Services, Information and Terminology, Oct 2019.

Performance Management

[5] Performance Framework, Dec 2019.

Validation

[6] Validation Strategy, Dec 2019.

[7] Validation Targets W2, Jun 2020.

System Engineering

[8] System Engineering - Methodology for the V&VP, V&VI and Demonstration Platform development, Jun 2019.

Safety

[9] SESAR Safety Reference Material, Dec 2018.

[10] Guidance to Apply SESAR Safety Reference Material, Dec 2018.

Human Performance

[11] Human Performance - Guidance Reference Material, Aug 2020.

Environment Assessment

[12] ENV - Guidance Reference Material, Dec 2019.

Security

[13] SecRAM, Sep 2017

7.2 Reference Documents

[14]SESAR 15.04.06 D02 ADS-B Security – Threat Analysis Report

[15] SESAR 15.04.06 D03 ADS-B GS Security Requirements and share between INDRA and THALES

[16] SESAR 15.04.06 D08 Final Report on ADS-B Security

[17] EUROCONTROL – GEN-SUR Safety And Performance Requirements Document On A Generic Surveillance System Supporting Air Traffic Control Services

[18] EUROCAE ED-142A Technical Specification for Wide Area Multilateration (WAM) systems

[19]EUROCAE ED-129B Technical Specification for a 1090 MHz Extended Squitter ADS-B Ground System

[20]EUROCONTROL Specification for Surveillance Data Exchange ASTERIX Part 14 Category 20 Multilateration Target Reports

[21]EUROCONTROL Specification for Surveillance Data Exchange ASTERIX Part 12 Category 21 ADS-B Target Reports

[22]EUROCONTROL Specification for Surveillance Data Exchange ASTERIX Part 26 Category 025 CNS/ATM Ground System Status Reports

[23]SESAR2020 D12.2.070 TS-IRS Initial Technical Specification for PJ14-04-03 Task 05

[24]SESAR 2020 PJ.14-W2-84c - D12.3.110 Initial TS-IRS Part I

[25]SESAR2020 D12.1.130 TVALP Technical Validation Plan for PJ14-04-03 Task 05

[26]SESAR2020 D12.1.150 TVALR Technical Validation Report for PJ14-04-03 Task 05

Appendix A Service Description Document (SDD)

This Appendix included in the TS/IRS Template is not applicable for this document

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix B ASTERIX CAT 246 Transponder Validation Report

The message is still a draft. It is implemented as a prototype to validate the message.

The current version is Edition 0.12.06.

The message specification is provided within this section.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

This document has not been approved by the ASTERIX Maintenance Group (AMG).

CAT 246
Transponder Validation Report

by Dr. Klaus Pourvoyeur / DFS

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Abstract 4
1 Executive summary 7
2 Introduction 8
2.1 Purpose of the document 8
2.2 Scope 8
2.3 Intended readership 9
2.4 Background 9
2.4.1 SESAR1 15.04.06 Project 10
2.4.2 GEN-SUR-SEC: EUROCONTROL Generic Surveillance Security Requirements 10
2.4.3 SESAR2020 Wave I Solution PJ14-04-03 T05 11
2.4.4 EUROCAE WG51 SG4 11
2.4.5 Document update 11
2.5 Structure of the document 12
2.6 Glossary of terms 12
2.7 Acronyms and Terminology 13
3 SESAR Solution Impacts on Architecture 18
3.1 Target Solution Architecture 18
3.1.1 SESAR Solution(s) Overview 18
3.1.2 Capability Configurations required for the SESAR Solution 23
3.2 Changes imposed by the SESAR Solution on the baseline Architecture 25
3.3 Analysis of security functions 25
3.3.1 Security in ADS-B systems 26
3.3.2 Security in multilateration systems (WAM/MLAT) 26
3.3.3 Security in composite surveillance 26
4 Technical Specifications 28
4.1 Threats classification 28
4.1.1 Threats at signal level 28
4.1.2 Threats at ADS-B content level 30
4.1.3 Threats at WAM content level 38
4.1.4 Time Synchronisation 39
4.2 Functional architecture overview (general introduction for all solutions) 41
4.2.1 Resource Connectivity view (one section per NSV-1) 44
4.2.2 Resource Composition 48
4.2.3 Service view 53
4.3 Functional and non-Functional Requirements 57
4.3.1 General Requirements 57
4.3.2 Threats Detection 64
4.3.3 External Interface 66
4.3.4 Performance 80
5 Recommendation for Implementation 84
6 Assumptions 85

EUROPEAN PARTNERSHIP
Co-funded by the European Union

7 References and Applicable Documents 86
7.1 Applicable Documents 86
7.2 Reference Documents 87
Appendix A Service Description Document (SDD) 88
Appendix B ASTERIX CAT 246 Transponder Validation Report 89
1. DESCRIPTION 93
i. General Purpose Description 93
1.1.1 Target Identification 93
1.1.2 Error Code 93
1.1.3 Source Location Validation 94
1.1.4 Data Validation 95
ii. Status and Type Modelling 95
iii. Duplicate Mode-S Address 98
2. ITEMS 99
2.1 Description of Standard Data Items 99
2.1.1 Data Item I246/000, Message Type 99
2.1.2 Data Item I246/010, Data Source Identifier 100
2.1.3 Data Item I246/015, Service Identification 100
2.1.4 Data Item I246/050, Message Identification 101
2.1.5 Data Item I246/070, Time of Day 101
2.1.6 Data Item I246/080, Target Address 103
2.1.7 Data Item I246/081, Address Type 103
2.1.8 Data Item I246/082, Airport Identification 105
2.1.9 Data Item I246/090, Track / Chain Number 106
2.1.10 Data Item I246/100, Error Code 107
2.1.11 Data Item I246/110, Source Location Validation Status 109
2.1.12 Data Item I246/120, Source Location Validation Deviation 111
2.1.13 Data Item I246/200, Data Validation Status 113
2.1.14 Data Item I246/210, Horizontal Position Data Deviation 115
2.1.15 Data Item I246/220, Horizontal Velocity Data Deviation 116
2.1.16 Data Item I246/230, Barometric Altitude Data Deviation 117
2.1.17 Data Item I246/300, Duplicate Address List 118
2.2 Standard User Application Profile 120

EUROPEAN PARTNERSHIP
Co-funded by the European Union

1. DESCRIPTION

i.General Purpose Description

Within the surveillance chain, each component has a different capability for the provision of validation information regarding a specific transponder. A sensor is the only component to be able to make a statement on the high frequency (HF) properties of the transmission channel. The advantage an SDPS has is that, it is connected to different input sources. Enabling a possibility for dependent validation approach, where these different input sources can be intercompared.

The purpose of the CAT 246 transponder validation report is to provide a container for the provision of validation information regarding the behaviour of a specific transponder. As the plot is moving along the surveillance chain, beginning with its generation to its final processing by the SDPS providing the situation awareness, the CAT 246 report is designed to collect information provided by multiple systems. In addition to the provision of a specific validation result, a design goal for CAT 246 was to be able to preserve meta data (data describing data) e.g. the system identification which conducted a specific validation.

1.1.1 Target Identification

A standard mean of target identification can be obtained via the 24-bit address of a Mode-S frame. The 24-bit ICAO address is mandatory for aircraft equipped with a Mode-S transponder. But, a transponder on a ground vehicle can transmit either a 24-bit ICAO address or a unique local surface vehicle address. In case a local surface address is sued, it can only be assumed that it is taken care (hopefully successful), that the surface vehicle address is unique for a specific airport but not that such an address is unique regarding several airports. To address this circumstance, a CAT 246 transponder validation report is able to provide an airport identification as four-letter ICAO code. An anonymous address lags the identification, whether it is an ICAO or a surface vehicle address.

Although the 24-bit ICAO address should be unique, this is not a certainty. In case of a Mode-S address conflict, a target within CAT 246 can be uniquely identified by the track / chain number of an SDPS and/or a sensor. The advantage of the track / chain number in comparison to the 24-bit address is its uniqueness, but this uniqueness last only until the track /chain is terminated und reused again. Regarding an SDPS, a track service end message is generated to indicate that a track is terminated by the SDPS. Unlike an MLAT plot, an ADS-B plot is not capable to provide a track termination message.

1.1.2 Error Code

CAT 246 is capable to collect the last 255 error codes of a specific transponder. The collection shall be done regarding the age of the error message and not regarding its first occurrence.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

1. Error Code System Identification

Each system in the surveillance chain can encounter different types of errors. This information may be crucial for a final decision on the validity of an ADS-B report. CAT 246 is designed to collect error messages along the surveillance chain. Within CAT 246, each provided error message identifies the system declaring the error via a SAC/SIC. The system forwarding the error message may operate on a different SAC/SIC with respect to the system, which originally generated the error message.

2. Duration of an Error

The duration of an error indicates how long the error continuously lasted since its first occurrence.

3. Age of an Error

The age of an error indicates when the error was last detected by the system reporting the error. An age of zero indicates, that the presence of the error has been currently confirmed.

4. Error Code Value

The error code value gives a rough indication on the nature of the error. Details regarding a specific error code value can be obtained from the log files of the corresponding system, which generated the initial report regarding this error code.

An ADS-B sensor might be able to detect an ADS-B squitter message but may not be able to generate a position solution. So, no plot report is generated for this missing position solution, and therefore this constellation cannot be indicated via CAT 021.

1.1.3 Source Location Validation

5. Source Location Validation Status

The goal of source location validation is to validate the signal source of a squitter message, containing specific data. For a specific ASTERIX element like horizonal position, horizontal velocity or barometric altitude CAT 246 provides information with respect to the origin of the data content. The content of the squitter message is not validated regarding this validation procedure. From a measurement perspective, the validation is based on time difference of arrival as well as angle of arrival measurements.

A squitter message may contain several data item, e.g. horizontal position and barometric altitude are parts of the same ADS-B squitter message.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

CAT 246 is designed to relieve the systems downstream from the necessity to take into account which data items are broadcasted together in a squitter message e.g. in ADS-B horizonal position and barometric altitude are part of the same squitter message. A slight drawback of this approach is, that information is partially doubled.

For an ADS-B position squitter, the data content is supposed to be identical to the source location of the squitter message.

6. Source Location Validation Deviation

The source location validation deviation provides the calculated deviation of the provided position in comparison to the location of the data source. To get rid of a specific measurement constellation, the source location deviation is expressed in local Cartesian coordinates centred around the supposed aircraft position.

Standard deviation of the validation result is expressed in the very same local Cartesian coordinate system as the deviation itself.

1.1.4 Data Validation

To conduct the validation of a specific data element, the data provided by a specific surveillance system under test e.g. ADS-B is compared with the data gained from another independent surveillance system e.g. Mode-S radar. The reference system must not be capable to form a complete surveillance layer by its own. A non-directed Mode-S interrogation is e.g. enough to validate the Callsign-in-flight of a target.

A statement on the validation status declaring a plot as valid or invalid can only be done regarding a specific threshold, which might be different depending on a specific surveillance service.

Therefore CAT 246 is capable to provide

- Horizontal Position Data Deviation
- Horizontal Velocity Data Deviation
- Barometric Altitude Data Deviation

Due to the domination of quantisation noise regarding barometric altitude of either 25 ft or 100 ft, no statement is made regarding the assumed accuracy.

ii.Status and Type Modelling

Co-funded by the European Union

1. Airborne / Ground Status

The airborne / ground status enables to distinguish the behaviour of a transponder between being airborne or moving on the ground. For a transponder of a ground vehicle only a ground status is meaningful.

2. Report Generation Status

The report generation of CAT 246 transponder validation reports can be triggered by the following circumstances:

- A periodic report is generated after a constant time since the last periodic event of a transponder validation report for a specific target.
- A plot driven report is generated for a currently processed plot by the validation instance. Plot driven report generation can be limited e.g. to the technology currently under validation.
- An event driven report is generated if a change in a specific information (e.g. validation status, validation type, presence of an error code or a change of the duplicate address list) has occurred since the last report output.

3. Plot Action Status

The plot action status is a binary decision, whether the plot is provided or filtered to be processed by a component down the surveillance chain. However, complex the decision is, in the end it comes down to this binary decision.

For a component which has not the purpose to provide plots to another component e.g. a conventional SDPS, the plot action status shall be set to no information.

4. Element Action Status

Instead of completely filtering a plot, in case of a detected anomaly regarding a specific ASTERIX element, only the identified suspicious element might be removed from the ASTERIX report. The element action status

By removing specific elements from an ASTERIX report, care must be taken to maintain a consistent ASTERIX report to be processed down the surveillance chain e.g. removing a data age, but remaining the declaration that the age of this very same element is zero is a contradiction.

Co-funded by the European Union

5. Validation Status

The validation status consists of the states; no information, valid, and invalid. The state transition diagram for the validation status is given in Fig. 1.

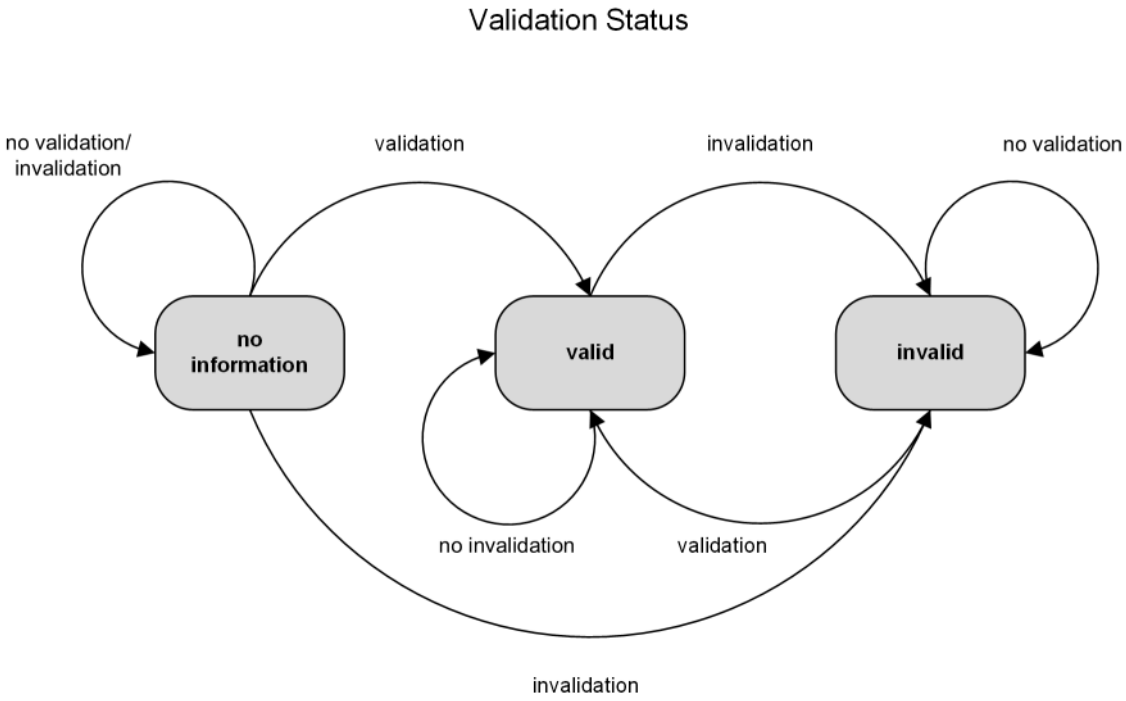


Fig. 1: State transition diagram for the validation status.

A transition from the status valid or invalid back to no information occurs only after a re-start of the validation without persistent data storage e.g. by the track termination of a SDPS regarding a specific 24-bit Mode-S address.

6. Validation & Error Type

The validation Type or Error Type describes on which the current validation or error declaration is based on and consists of the following states: no information, current plot, current track/chain, and current address. The state transition for validation type is given Fig. 2.

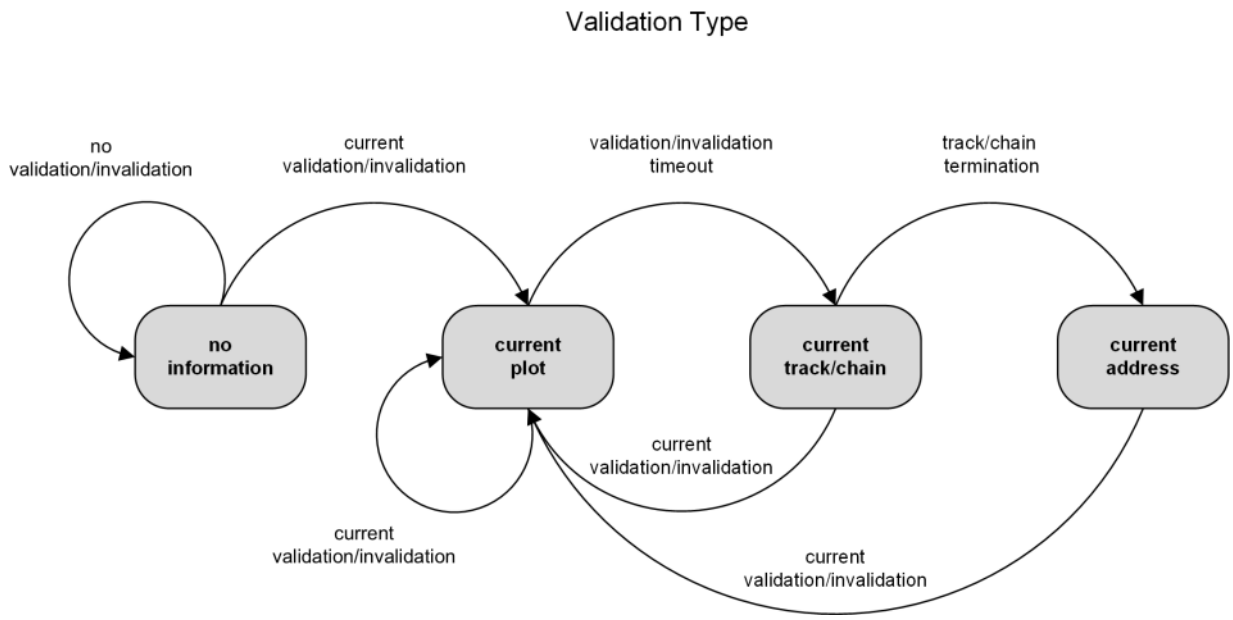


Fig. 2: State transition diagram for the validation type.

iii.Duplicate Mode-S Address

CAT 246 is able to provide the information to which the target of a CAT 246 report currently is or previously was in conflict. CAT 246 is capable to collect the last 255 error duplicate Mode-S address conflicts. The collection shall be done based on the age of the conflict not based on its first occurrence.

Mode-S radar or MLAT are not capable to provide information on the address type via ASTERIX; only ADS-B has a dedicated ASTERIX element based on the address type (ATP). For a surface vehicle address, a conflict is only present, if both targets are dedicated to the same airport. Therefore, the constellations for declaring a duplicate Mode-S address conflicts are the following:

- ICAO with ICAO
- ICAO with unknown
- Unknown with unknown
- Unknown with surface vehicle
- Surface vehicle with surface vehicle of the same airport

EUROPEAN PARTNERSHIP
Co-funded by the European Union

2. ITEMS

2.1 Description of Standard Data Items

2.1.1 Data Item I246/000, Message Type

Definition: This data item conveys the report type and whether the output is periodically updated, plot driven or asynchronous depending upon external events.

Format: One-octet fixed length data item.

Structure:

Octet no. 1

8	7	6	5	4	3	2	1
AG		RG		0	0	0	0

bits-8/7 (AG) Airborne / Ground
= 0 No information
= 1 Airborne
= 2 Ground

bits-6/5 (RG) Report Generation
= 0 No information
= 1 Periodic report
= 2 Plot driven report
= 3 Event driven report

bits-4/1 Spare bit(s) set to zero

EUROPEAN PARTNERSHIP
Co-funded by the European Union

2.1.2 Data Item I246/010, Data Source Identifier

Definition: Identification of the data source from which the data is received.

Format: Two-octet fixed length data item.

Structure:

Octet no. 1								Octet no. 2							
16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
SAC								SIC							

bits-16/9 (SAC) System Area Code

bits-8/1 (SIC) System Identification Code

2.1.3 Data Item I246/015, Service Identification

Definition: Identification of the service provided to one or more users.

Format: One-octet fixed length data item.

Structure:

Octet no. 1							
8	7	6	5	4	3	2	1
SID							

bits-8/1 (SID) Service Identification

EUROPEAN PARTNERSHIP

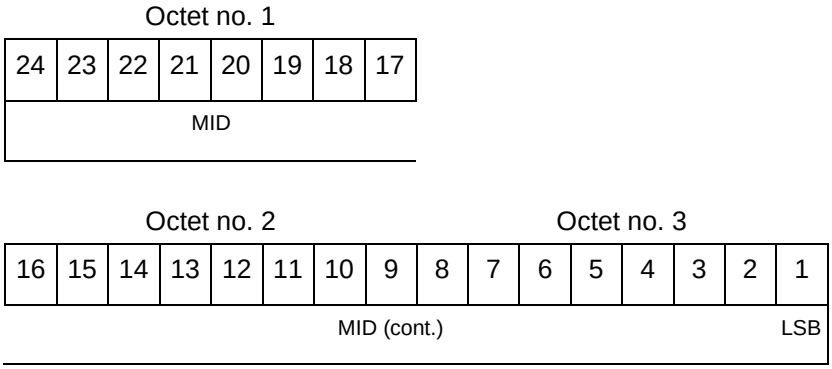
Co-funded by the European Union

2.1.4 Data Item I246/050, Message Identification

Definition: A unique identifier (until round robin) of the ASTERIX message report.

Format: Three-octet fixed length data item.

Structure:



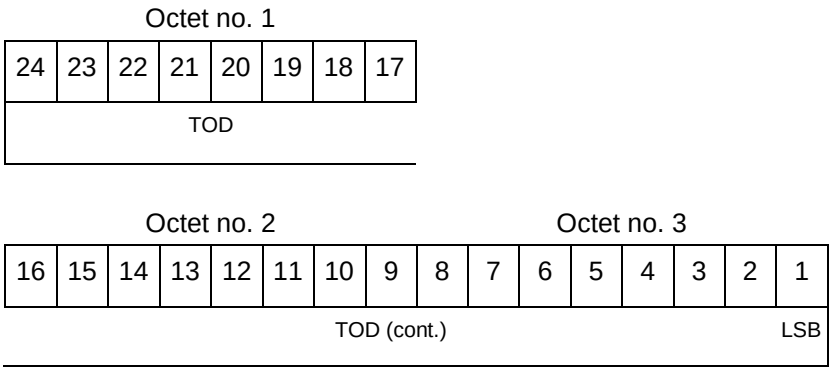
bits-24/1	(MID)	Message Identification Number max. value: 16,777,215

2.1.5 Data Item I246/070, Time of Day

Definition: Absolute time stamping for applicability of the ASTERIX report expressed as UTC.

Format: Three-octet fixed length data item.

Structure:



bits-24/1	(TOD)	Time of Day
bit-1	(LSB)	= 1/128 s

EUROPEAN PARTNERSHIP

Co-funded by
the European Union

2.1.6 Data Item I246/080, Target Address

Definition: Target identification by means of the 24-bit target address.

Format: Three-octet fixed length data item.

Structure:

Octet no. 1

24	23	22	21	20	19	18	17
ADR							

Octet no. 2 Octet no. 3

16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
ADR (cont.)															

bits-24/1 (ADR) 24-bit target address

Note 1: This Data Items is only a unique identifier in case of unique 24-Bit Mode S Address.

Note 2: In case of Mode S address conflict, the target is designated additionally by the track / chain number.

2.1.7 Data Item I246/081, Address Type

Definition: Address type of the 24-bit target address.

Format: One-octet fixed length data item.

Structure:

Octet no. 1

8	7	6	5	4	3	2	1
0	0	0	0	0	ATP		

bits-8/4 Spare Bits

bits-3/1 (ATP) Address Type
= 0 No information

EUROPEAN PARTNERSHIP

Co-funded by the European Union

= 1 24-bit ICAO address
= 2 Anonymous address
= 3 Surface vehicle address

EUROPEAN PARTNERSHIP
Co-funded by the European Union

2.1.8 Data Item I246/082, Airport Identification

Definition: Airport identification for surface vehicle as four-letter ICAO code in ASCII representation.

Format: Four-octet fixed length data item.

Structure:

Octet no. 1 Octet no. 2

32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
CHR1								CHR2							

Octet no. 3 Octet no. 4

16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
CHR3								CHR4							

bits-32/25 (CHR1) First letter of ICAO code for airports

bits-24/17 (CHR2) Second letter of ICAO code for airports

bits-16/9 (CHR3) Third letter of ICAO code for airports

bits-8/1 (CHR4) Fourth letter of ICAO code for airports

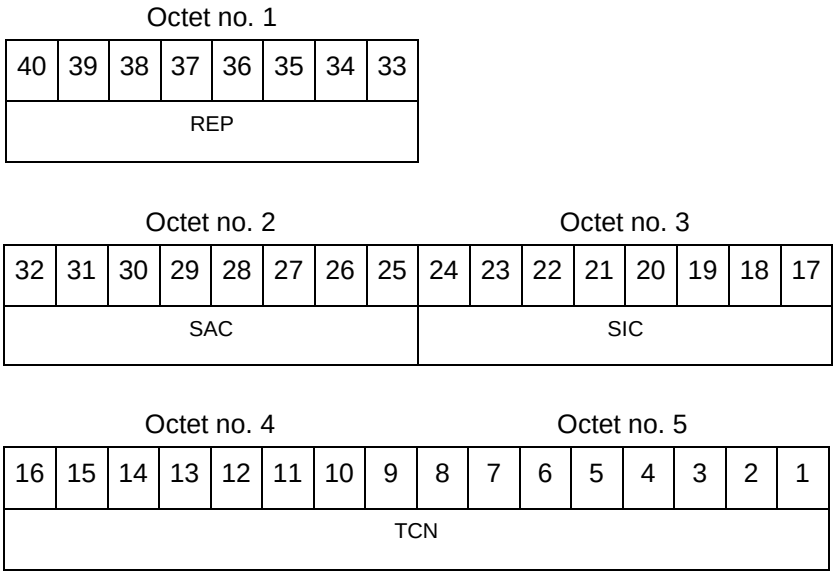
EUROPEAN PARTNERSHIP
Co-funded by the European Union

2.1.9 Data Item I246/090, Track / Chain Number

Definition: Track / Chain Number of report referring to a chainer output by an SDPS and/or a sensor. Any additional information is to be taken from the plot / track report.

Format: Repetitive data item starting with a one-octet field repetition indicator (REP) followed by at least one status report of 4-octet.

Structure:



bits-40/33	(REP)	Repetition factor
bits-32/25	(SAC)	System Area Code of the SDPS
bits-24/17	(SIC)	SDPS System Identification Code of the SDPS
bits-16/1	(TCN)	Track / Chain Number max. value = 65,536

Note: This Data Items enables to identify a specific target in case of multiple identical 24-bit transponder addresses, without the necessity to transmit redundant data.

EUROPEAN PARTNERSHIP
Co-funded by the European Union

2.1.10 Data Item I246/100, Error Code

Definition: Error code provided by the system.

Format: Repetitive data item starting with a one-octet field repetition indicator (REP) followed by at least one status report of 9-octet.

Structure:

Octet no. 1

80	79	78	77	76	75	74	73
REP							

Octet no. 2 Octet no. 3

72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57
SAC								SIC							

Octet no. 4 Octet no. 5

56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41
ERR								PAS		0	0	0	0	ETP	

Octet no. 6 Octet no. 7

40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25
D_ERR															LSB

Octet no. 8 Octet no. 9

24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9
A_ERR															

Octet no. 10

8	7	6	5	4	3	2	1
A_ERR (cont.)							LSB

bits-80/73 (REP) Repetition factor

bits-72/65 (SAC) System Area Code of the system declaring the error

bits-64/57	(SIC)	System Identification Code of the system declaring the error
bits-56/49	(ERR)	Error Code Value = 0 No information = 1 No position solution = 2 Non-conformance behaviour = 3 Position Deviation = 4 Data Deviation = 5 Missing Data = 6 …
bits-48/47	(PAS)	Plot Action Status = 0 No information = 1 Plot provided = 2 Plot filtered
bits-46/43		Spare bits
bits-42/41	(ETP)	Error Type 0 = No information 1 = Current plot 2 = Current track / chain 3 = Current address
bits-40/25	(D_ERR) (LSB)	Duration of Error = 0.25 s
bits-24/1	(A_ERR) (LSB)	Age of Error = 0.25 s

EUROPEAN PARTNERSHIP
Co-funded by the European Union

2.1.11 Data Item I246/110, Source Location Validation Status

Definition: Source Location Validation Status.

Format: Repetitive data item starting with a one-octet field repetition indicator (REP) followed by at least one status report of 9-octet.

Structure:

Octet no. 1

80	79	78	77	76	75	74	73
REP							

Octet no. 2 Octet no. 3

72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57
SAC								SIC							

Octet no. 4 Octet no. 5

56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41
ELE								PAS		EAS		VST		VTP	

Octet no. 6 Octet no. 7

40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25
D_VAL															LSB

Octet no. 8 Octet no. 9

24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9
A_VAL															

Octet no. 10

8	7	6	5	4	3	2	1
A_VAL (cont.)							LSB

bits-80/73 (REP) Repetition factor

bits-72/65 (SAC) System Area Code of the system conducting the source location validation

EUROPEAN PARTNERSHIP
Co-funded by the European Union

bits-64/57	(SIC)	System Identification Code of the system conducting the source location validation
bits-56/49	(ELE)	ASTERIX Element = 1 Horizontal position = 2 Barometric altitude = 3 Horizontal velocity = 4 Target identification = 5 Mode-3/A = 6 MOPS = 7 NICp = 8 NACp = 9 NUCp = 10 Priority Status (Special Emergency) = 11 …
bits-48/47	(PAS)	Plot Action Status = 0 No information = 1 Plot provided = 2 Plot filtered
bits-46/45	(EAS)	Element Action Status = 0 No information = 1 Element provided = 2 Element filtered
bits-44/43	(VST)	Validation Status = 0 No information = 1 Valid = 2 Invalid
bits-42/41	(VTP)	Validation Type 0 = No information 1 = Current plot 2 = Current track / chain 3 = Current address
bits-40/25	(D_VAL) (LSB)	Duration since last Validation Status change = 0.25 s
bits-24/1	(A_VAL) (LSB)	Age of Validation = 0.25 s

EUROPEAN PARTNERSHIP
Co-funded by the European Union

2.1.12 Data Item I246/120, Source Location Validation Deviation

Definition: Source Location Validation Deviation and Precision.

Format: Repetitive data item starting with a one-octet field repetition indicator (REP) followed by at least one status report of 11-octet.

Structure:

Octet no. 1

96	95	94	93	92	91	90	89
REP							

Octet no. 2 Octet no. 3

88	87	86	85	84	83	82	81	80	79	78	77	76	75	74	73
SAC								SIC							

Octet no. 4

72	71	70	69	68	67	66	65
ELE							

Octet no. 5 Octet no. 6

64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49
DX															LSB

Octet no. 7 Octet no. 8

48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33
DY															LSB

Octet no. 9 Octet no. 10

32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
SD_DX											LSB	SD_DY			

Octet no. 11 Octet no. 12

16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
SD_DY (cont.)							LSB	CoSD_DXY							LSB

EUROPEAN PARTNERSHIP
Co-funded by the European Union

bits-96/89	(REP)	Repetition factor
bits-88/81	(SAC)	System Area Code of the system calculating the position deviation and precision
bits-80/73	(SIC)	System Identification Code of the system calculating the position deviation and precision
bits-72/65	(ELE)	ASTERIX Element = 1 Horizontal position = 2 Barometric altitude = 3 Horizontal velocity = 4 …
bits-64/49	(DX) (LSB)	Deviation in X for horizontal source location, in two's compliment = 1 m
bits-48/33	(DY) (LSB)	Deviation in Y for horizontal source location, in two's compliment = 1 m
bits-32/21	(SD_DX) (LSB)	Standard deviation of horizontal source location deviation in X = 1 m
bits-20/9	(SD_DY) (LSB)	Standard deviation of horizontal source location deviation in Y = 1 m
bits-8/1	(CoSD_DXY) (LSB)	Correlation of horizontal source location deviation of X and Y component, in two's compliment = $1/2^7$

EUROPEAN PARTNERSHIP
Co-funded by the European Union

2.1.13 Data Item I246/200, Data Validation Status

Definition: Data Validation Status regarding consistency with another surveillance sensor, consistency with another ground station or consistency over time.

Format: Repetitive data item starting with a one-octet field repetition indicator (REP) followed by at least one status report of 9-octet.

Structure:

Octet no. 1

80	79	78	77	76	75	74	73
REP							

Octet no. 2 Octet no. 3

72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57
SAC								SIC							

Octet no. 4 Octet no. 5

56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41
ELE								PAS		EAS		VST		VTP	

Octet no. 6 Octet no. 7

40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25
D_VAL															LSB

Octet no. 8 Octet no. 9

24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9
A_VAL															

Octet no. 10

8	7	6	5	4	3	2	1
A_VAL (cont.)							LSB

bits-80/73 (REP) Repetition factor

bits-72/65	(SAC)	System Area Code of the system declaring the error
bits-64/57	(SIC)	System Identification Code of the system declaring the error
bits-56/49	(ELE)	ASTERIX Element = 1 Horizontal position = 2 Barometric altitude = 3 Horizontal velocity = 4 Target identification = 5 Mode-3/A = 6 MOPS = 7 NICp = 8 NACp = 9 NUCp = 10 Priority Status (Special Emergency) = 11 Downlink Format = 12 Vertical Velocity
bits-48/47	(PAS)	Plot Action Status = 0 No information = 1 Plot provided = 2 Plot filtered
bits-46/45	(EAS)	Element Action Status = 0 No information = 1 Element provided = 2 Element filtered
bits-44/43	(VST)	Validation Status = 0 No information = 1 Valid = 2 Invalid
bits-42/41	(VTP)	Validation Type 0 = No information 1 = Current plot 2 = Current track / chain 3 = Current address
bits-40/25	(D_VAL) (LSB)	Duration since last Validation Status change = 0.25 s
bits-24/1	(A_VAL) (LSB)	Age of Validation = 0.25 s

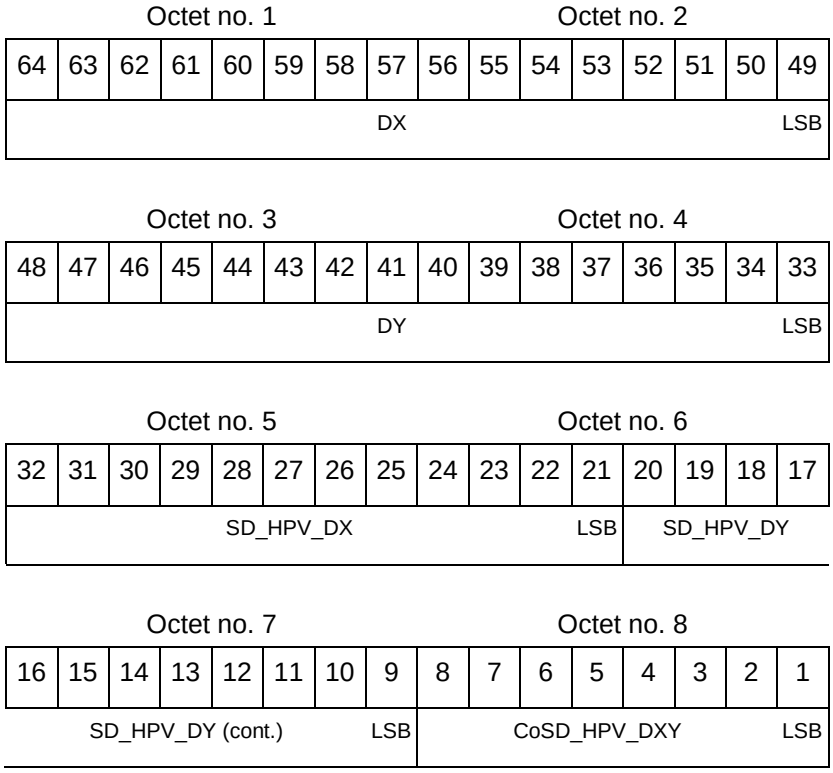
EUROPEAN PARTNERSHIP
Co-funded by the European Union

2.1.14 Data Item I246/210, Horizontal Position Data Deviation

Definition: Horizontal position deviation and precision between ADS-B and non ADS-B by a reference sensor or SDPS (ADS-B position minus non ADS-B position).

Format: Eight-octet fixed length data item.

Structure:



bits-64/49	(DX)	Deviation in X for horizontal position validation, in two's compliment (ADS-B measurement minus expected meas.)
	(LSB)	= 1 m
bits-48/33	(DY)	Deviation in Y for horizontal position validation, in two's compliment (ADS-B measurement minus expected meas.)
	(LSB)	= 1 m
bits-32/21	(SD_HPV_DX)	Standard deviation of Horizontal Position Deviation in X
	(LSB)	= 1 m
bits-20/9	(SD_HPV_DY)	Standard deviation of Horizontal Position Deviation in Y
	(LSB)	= 1 m

EUROPEAN PARTNERSHIP
Co-funded by the European Union

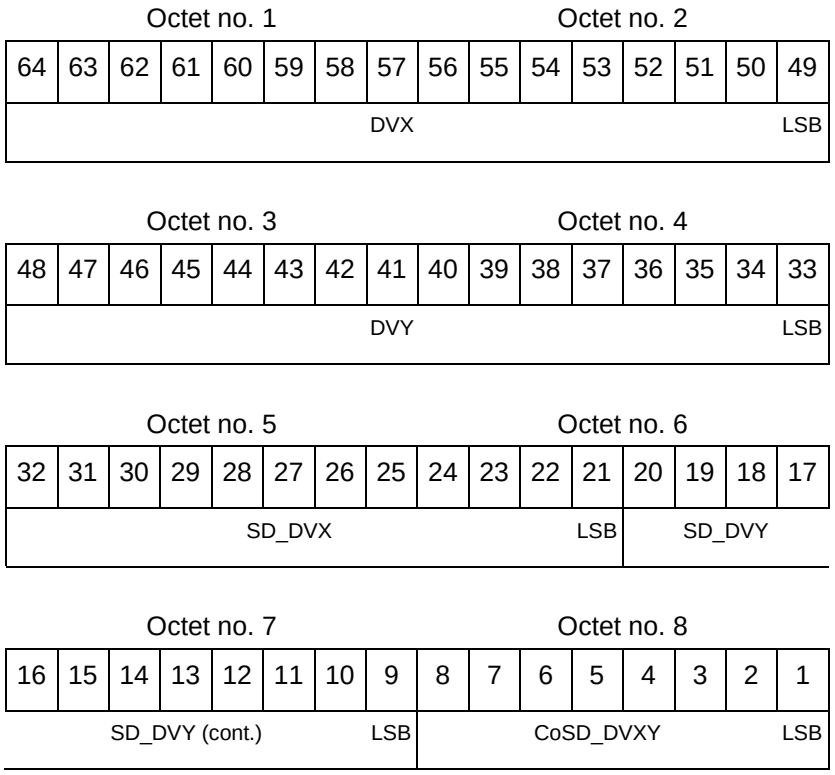
bits-8/1	(CoSD_HPV_DXY)	Correlation of Horizontal Position Deviation of X and Y component, in two's compliment
	(LSB)	= $1/2^7$

2.1.15 Data Item I246/220, Horizontal Velocity Data Deviation

Definition: Horizontal velocity deviation and precision between ADS-B and non ADS-B by a reference sensor or SDPS.

Format: Eight-octet fixed length data item.

Structure:



bits-64/49	(DVX)	Horizontal Velocity Deviation, in two's compliment. (ADS-B measurement minus expected meas.)
	(LSB)	= 0.1 m/s
bits-48/33	(DVY)	Horizontal Velocity Deviation in Y in two's compliment. (ADS-B measurement minus expected meas.)
	(LSB)	= 0.1 m/s

EUROPEAN PARTNERSHIP
Co-funded by the European Union

bits-32/21	(SD_DVX)	Standard deviation of Horizontal Velocity Deviation in X
	(LSB)	= 1 m
bits-20/9	(SD_DVY)	Standard deviation of Horizontal Velocity Deviation in Y
	(LSB)	= 1 m
bits-8/1	(CoSD_DVXY)	Correlation of Horizontal Velocity Deviation of X and Y component, in two's compliment
	(LSB)	= $1/2^7$

2.1.16 Data Item I246/230, Barometric Altitude Data Deviation

Definition: Barometric altitude deviation between ADS-B and non ADS-B

Format: Two-octet fixed length data item.

Structure:

	Octet no. 1								Octet no. 2							
	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
	BAD															LSB

bits-16/1	(BAD)	Barometric Altitude Deviation, in two's compliment
	(LSB)	= 6.25 ft

EUROPEAN PARTNERSHIP
Co-funded by the European Union

2.1.17 Data Item I246/300, Duplicate Address List

Definition: List of targets with the same 24-bit address identified by a track / chain number.

Format: Repetitive data item starting with a one-octet field repetition indicator (REP) followed by at least one status report of 10-octet.

Structure:

Octet no. 1

88	87	86	85	84	83	82	81
REP							

Octet no. 2 Octet no. 3

80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65
SAC								SIC							

Octet no. 4 Octet no. 5

64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49
TCN_DA															

Octet no. 6 Octet no. 7

48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33
D_DA															LSB

Octet no. 8 Octet no. 9

32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
A_DA															

Octet no. 10 Octet no. 11

16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
A_DA (cont.)							LSB	NCS	SSR	MDS	MLT	ADS	0	0	0

bits-88/81 (REP) Repetition factor

bits-80/73 (SAC) System Area Code of track / chain number

EUROPEAN PARTNERSHIP
Co-funded by the European Union

bits-72/65	(SIC)	System Identification Code of track / chain number
bits-64/49	(TCN_DA)	Track / chain number for Duplicate Address
bits-48/33 bit-33	(D_DA) (LSB)	Duration of Duplicate Address 0.25 s
bits-32/9 bit-9	(A_DA) (LSB)	Age of Duplicate Address 0.25 s
bit-8	(NCS)	Non cooperative Surveillance (NCS) support status 0 = has no NCS support 1 = has NCS support
bit-7	(SSR)	secondary surveillance radar support status (Mode-1/2/3/4/5/S or only Mode-3?) 0 = has no SSR support 1 = has SSR support
bit-6	(MDS)	Mode-S surveillance radar support status 0 = has no Mode-S surveillance radar support 1 = has Mode-S surveillance radar support
bit-5	(MLT)	MLAT/WAM support status 0 = has no MLAT/WAM support 1 = has MLAT/WAM support
bit-4	(ADS)	ADS-B/C support status 0 = has no ADS-B/C support 1 = has ADS-B/C support
bits-3/1		Spare Bits set to zero

EUROPEAN PARTNERSHIP

Co-funded by the European Union

2.2 Standard User Application Profile

The following UAP shown in Table 7 shall be used for the transmission of target reports and service messages:

Table 7: Standard UAP

FRN	Data Item	Information	Length in Octets
1	I246/010	Data Source Identifier	2
2	I246/000	Message Type	1
3	I246/015	Service Identification	1
4	I246/050	Message Identification	3
5	I246/070	Time of Day	3
6	I246/080	Target Address	3
7	I246/081	Address Type	1
FX	-	Field Extension Indicator	-
8	I246/082	Airport Identification	4
9	I246/090	Track / Chain Number	1+4n
10	I246/100	Error Code	1+9n
11	I246/110	Source Location Validation Status	1+9n
12	I246/120	Source Location Validation Deviation	1+11n
13	I246/200	Data Validation Status	1+9n
14	I246/300	Duplicate Address List	1+10n
FX	-	Field Extension Indicator	-
15	I246/210	Horizontal Position Data Deviation	8
16	I246/220	Horizontal Velocity Data Deviation	8
17	I246/230	Barometric Altitude Data Deviation	2
18	SP	Special Purpose Field	1+
19	-	not used	-
20	-	not used	-
21	-	not used	-
FX	-	Field Extension Indicator	-

EUROPEAN PARTNERSHIP
Co-funded by the European Union

-END OF DOCUMENT-

Insert beneficiary's logos below, if required

Co-funded by
the European Union