Aviation resilience to GNSS frequency jamming and cyber threats

FINAL REPORT

DELIVERABLE(S): D1090 (TLP: AMBER)

AIRING

Prepared by: AIRING Team

Approved by: Luis J. Alvarez

Authorized by: Alberto de la Fuente

Code:	AIRING-GMV-FR
Version:	1.1
Date:	17/03/2023
Internal code:	GMV 20995/23 V2/23

DOCUMENT STATUS SHEET

Version	Date	Pages	Changes
1.0	22/02/2023	100	First version of the document
1.1	17/03/2023	98	Updated to implement the following RIDs (AIRING RIDs_REP15_v1.0_REVIEWED_v2.0): • RID 1: text updated in section §4.3.1 • RID 2: Figure 4-2 and Figure 4-3 shown in landscape format • RID 3: section §4.3.2 updated • RID 4: Table 4-17 updated; clarification added to section §4.6.1 • RID 5: Table 4-18 updated; section §4.6.1 added • RID 6: section §4.3.3 updated; section §4.6.2 added • RID 7: section §4.3.3 updated; section §4.6.2 added • RID 8: typo corrected • RID 9: Table 4-14 updated • RID 10: Figure 4-4 shown in landscape format • RID 11: Figure 4-5 shown in landscape format • RID 12: text updated in section §4.4 • RID 13: section §4.7 updated • RID 14: Management section removed

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

1. INTRODUCTION

1.1. PURPOSE

This is deliverable D1090 "Final Report", and it is the last outcome of WP1000

The document is split into two main parts:

- An executive summary (4.), which summarizes the results of the core tasks of the project
- Some annexes (5. to 8.), which provide additional details on the results of the core tasks of the project, as well as it summarizes other project tasks (e.g. DPA study, open field tests, operational tests, recommended support actions to the proposed roadmap, material to support the industrialization of the main research results of the project).

The project results represent the views of the users and the consortium. They do not necessarily represent the views of the European Commission and they do not commit the European Commission to implementing the results.

1.2. SCOPE

This is the second version of the document, and includes some changes in its structure

- A new section "Technologies implementation timeline" is added (see §4.6)
- One of the sections in the Annex, "Monitoring and Reporting", is removed

2. REFERENCES

2.1. APPLICABLE DOCUMENTS

The following documents, of the exact issue shown, form part of this document to the extent specified herein. Applicable documents are those referenced in the Contract or approved by the Approval Authority. They are referenced in this document in the form [XXX]:

Table 2-1: Applicable documents.

Ref.	Title	Code	Version	Date
[ITT]	Invitation to Tender: Aviation Resilience to GNSS Frequency Jamming and Cyber Threats	DEFIS/2020/OP/0006	-	27/08/20
[TS]	Tender Specifications: Aviation Resilience to GNSS Frequency Jamming and Cyber Threats	DEFIS/2020/OP/0006	-	27/08/20
[CNTR]	Service Contract: Aviation Resilience to GNSS Frequency Jamming and Cyber Threats	DEFIS/2020/OP/0006	-	03/03/21
[TP]	AIRING (Aviation Resilience to GNSS Frequency Jamming) Technical Proposal	GMV 12761/20 V1/20	1.0	16/10/20

2.2. REFERENCE DOCUMENTS

The following documents, although not part of this document, amplify or clarify its contents. Reference documents are those not applicable and referenced within this document. They are referenced in this document in the form [XXX]:

Table 2-2: Reference documents.

Ref.	Title	Code	Version	Date
[PMP]	Project Management Plan	AIRING-GMV-PMP	1.0	31/03/21
[REP01]	GNSS RFI scenarios, threats characterization and evolution	AIRING-GMV-REP-01	1.1	10/09/21
[REP02]	Risk Analysis for Aviation	AIRING-GMV-REP-02	2.1	27/01/23
[REP03]	State of the Art of GNSS RFI Detection, Mitigation and Localization Techniques	AIRING-GMV-REP-03	1.1	24/09/21
[REP05]	Evaluation of GNSS RFI detection, mitigation and localization techniques for aviation	AIRING-GMV-REP-05	1.1	02/11/21
[REP06]	GNSS RFI detection, mitigation and localization requirements	AIRING-GMV-REP-06	1.2	01/04/22
[REP08]	GNSS RFI test scenarios, test plan, and key performance indicators	AIRING-GMV-REP-08	1.1	11/03/22
[REP09]	Proposed labelling for airborne and ground equipment for GNSS RFI detection, mitigation and localization in aviation	AIRING-GMV-REP-09	2.1	27/01/23
[REP10]	GNSS RFI test procedures	AIRING-GMV-REP-10	1.3	19/09/22
[REP11]	GNSS RFI reporting, operational concept, database and API definition and specification for Aviation	AIRING-GMV-REP-11	1.1	02/05/22
[REP12]	GNSS RFI operational mitigation, contingency plans, and preventive measures for Aviation	AIRING-GMV-REP-12	1.1	30/03/22
[REP14]	GNSS RFI Experimentation results	AIRING-GMV-REP-14	1.2	27/01/23

Ref.	Title	Code	Version	Date
[REP15]	Roadmap for implementation of GNSS RFI detection, mitigation and localization solutions for Aviation	AIRING-GMV-REP-15	1.1	15/03/23
[APRESTA]	APRESTA Architectural Design Document. GMV	GMV-APRESTA-AD	2.2	March 2020
[EOCVM]	European Operational Concept Validation Methodology. Volume I. EC and Eurocontrol	-	3.0	Feb 2010
[EOCVMA]	European Operational Concept Validation Methodology. Volume II Annexes. EC and Eurocontrol	-	3.0	Feb 2010
[MOPS]	Minimum Operational Performance Standard for Galileo / Global Positioning System / Satellite-Based Augmentation System Airborne Equipment. RTCA	ED-259A	0.16	23/11/22
[Doc 4444]	Air Traffic Management (ATM)	Doc 4444	Ed 16th	2016
[Doc 8071]	Manual on Testing of Radio Navigation Aids. Volume II Testing of Satellite-based Radio Navigation Systems	Doc 8071	Ed 5th Corr. 1	2007 30/04/08
[Doc 9849]	Global Navigation Satellite System (GNSS) Manual	Doc 9849	Ed 3rd	2017
[Doc9859]	Safety Management Manual. ICAO	Doc 9859	4th edition	2018
[ION]	Fernández-Hernández, Ignacio, Walter, Todd, Alexander, Ken, Clark, Barbara, Châtre, Eric, Hegarty, Chris, Appel, Manuel, Meurer, Michael, "Increasing International Civil Aviation Resilience: A Proposal for Nomenclature, Categorization and Treatment of New Interference Threats," Proceedings of the 2019 International Technical Meeting of The Institute of Navigation, Reston, Virginia, January 2019, pp. 389-407.	https://doi.org/10.33012/2019.16699	-	Jan 2019
[SKYBRA]	Safety Management. Probability of Occurrence. Skybrary. https://www.skybrary.aero/index.php/Risk_Assessment	-	-	-
[PBNHND]	European GNSS Contingency/Reversion Handbook for PBN Operations, PBN HANDBOOK No. 6, Eurocontrol.	-	-	2020
[SECRAM]	Security Risk Assessment methodology for SESAR 2020. SESAR Joint Undertaking	SecRAM	2.0	25/09/17
[EVAIR]	EVAIR Bulletin No 22 (2015 – 2019) https://www.eurocontrol.int/publication/eurocontrol-voluntary-atm-incident-reporting-evair-safety-bulletin-22	-	-	May 2021

3. TERMS, DEFINITIONS AND ABBREVIATED TERMS

3.1. DEFINITIONS

Concepts and terms used in this document and needing a definition are included in the following table:

Table 3-1 Definitions

Concept / Term	Definition

3.2. ACRONYMS

Acronyms used in this document and needing a definition are included in the following table:

Table 3-2 Acronyms

Acronym	Definition
A/C	Aircraft
A-PNT	Alternative Position, Navigation and Timing
AA	Aerodrome Authority
ADC	Analog-to-Digital Converter
ADS-B	Automatic Dependent Surveillance – Broadcast
AGC	Automatic Gain Control
AFIS	Aerodrome Flight Information Service
AHRS	Attitude and Heading Reference Systems
AIS	Aeronautical Information Service
AOC	Aircraft Operations Centre
ANF	Adaptive Notch Filter
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider
AO	Aerodrome Operator
AoA	Angle of Arrival
API	Application Programming Interface
APM	Absolute Power Monitoring
ARAIM	Advanced Receiver Autonomous Integrity Monitoring
ARINC	Aeronautical Radio, Incorporated
ASIC	Application-Specific Integrated Circuit
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATFCM	Air Traffic Flow and Capacity Management
ATM	Air Traffic Management
ATS	Air Traffic Service
ATSEP	Air Traffic Safety Electronics Personnel
ATSU	Air Traffic Services Unit
AU	Airspace User
BVLOS	Beyond Visual Line of Sight
C/N0	Carrier to Noise

Acronym	Definition
CAA	Civil Aviation Authority
CBA	Cost Benefit Analysis
CCH	Consistency Checks
CH	Chirp
CIS	Common Information Services
CNS	Communications, Navigation, Surveillance
COTS	Commercial Off-The-Shelf
CPDLC	Controller Pilot Data Link Communications
CPM	Correlation Peak Monitoring
CQI	Channel Quality Indicator
CRPA	Controlled Reception Pattern Antenna
CTR	Control Traffic Zone
CW	Constant Wave
CWP	Controller Working Position
D-ATIS	Digital Automatic Terminal Information Service
D3	Dispersion of Double Differences
DB	Database
DF	Dual Frequency
DFMC	Dual Frequency Multi Constellation
DLL	Delay Lock Loop
DME	Distance Measurement Equipment
DMPR	DME based Passive Ranging
DOA	Direction of Arrival
DPA	Dual-Polarized Antenna
DS	Digital Sum
DUT	Device Under Test
E-OCVM	European Operational Concept Validation Methodology
EAD	European AIS Database
EASA	European Aviation Safety Agency
EC	European Commission
ECAC	European Civil Aviation Conference
eDEM	Enhanced DME
EGNOS	European Geostationary Navigation Overlay Service
EIRP	Effective Isotropic Radiated Power
eLORAN	Enhanced LORAN
ESPRIT	Estimation of Signal Parameters via Rotational Invariant Techniques
ESSP	European Satellite Services Provider
ETSO	European Technical Standard Order
EU	European Union
EUR	Eurocontrol
EUROCAE	European Organization for Civil Aviation Equipment
EUSPA	EU Agency for the Space Programme
EVAIR	EUROCONTROL's Voluntary ATM Incident Reporting
FDE	Fault Detection and Exclusion

Acronym	Definition
FDOA	Frequency Difference of Arrival
FI	Flight Inspection
FLARM	Flight Alarm
FMS	Flight Management System
FPGA	Field Programable Gate Array
FRPA	Fixed Reception Pattern Antenna
FV	Flight Validation
G2G	Galileo Second Generation
GBAS	Ground Based Augmentation System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSC	European GNSS Service Centre
GSS	Galileo Sensor Station
GV	Ground Validation
H	Horizontal
HAPS	High Altitude Platform Station
HAPS	High Altitude Pseudo Satellite
HAS	High Accuracy Service
HMI	Human Machine Interface
HPL	Horizontal Protection Level
HTTP	Hypertext Transfer Protocol
HW	Hardware
IAF	Initial Approach Fix
ICAO	International Civil Aviation Organization
IFR	Instrument Flight Rules
IO	Input/Output
IQ	In Phase / Quadrature
ILS	Instrument Landing System
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
IPR	Intellectual Property Right
IRU	Inertial Reference Unit
ISL	Inter-Satellite Links
JSR	Jamming to Signal Ratio
JTIDS	Joint Tactical Information Distribution System
KPA	Key Performance Area
KPI	Key Performance Indicator
LDACS	L-band Digital Aeronautical Communications System
LEO	Low Earth Orbit
LHCP	Left Circular Polarization
LNAV	Lateral Navigation
LORAN	Long Range Navigation
LPV	Localizer Performance with Vertical guidance
MEO	Medium Earth Orbit

Acronym	Definition
MFMC	Multi-Frequency Multi-Constellation
MIL	Military
ML	Machine Learning
MLAT	Multilateration
MIDS	Multifunctional Information Distribution System
MOPS	Minimum Operational Performance Standards
MUSIC	Multiple Signal Classification
MVDR	Minimum Variance Distortionless Response Estimator
N/A	Not Applicable
NAV	Navigation
NFM	National Frequency Manager
NL	Noise-Lile
NM	Network Manager
NMA	Navigation Message Authentication
NOF	NOTAM Office
NOTAM	Notice To Airmen
NSA	National Safety Authority
OBP	On-Board Processing
OPS	Operations
OS	Open Service
OSNMA	Open Service Navigation Message Authentication
P&F	Precise and Fast
PB	Pulse Blanking
PBN	Performance Based Navigation
PL	Pulsed
PNT	Positioning, Navigation, and Timing
POS	Position
PPD	Personal Privacy Devices
PSR	Primary Surveillance Radar
PVT	Position, Velocity, Time
RAIM	Receiver Autonomous Integrity Monitoring
RbXO	Rubidium-Crystal Oscillator
RDS	Running Digital Sum
REST	Representational State Transfer
RF	Radio Frequency
RF	Radio to Fix
RFI	Radio Frequency Interference
RHCP	Right Circular Polarization
RID	Review Item Discrepancy
RIM	Robust Interference Mitigation
RIMS	Ranging Integrity Monitoring Stations
RINEX	Receiver Independent Exchange
RNAV	Radio Navigation
RNP	Required Navigation Performance

Acronym	Definition
RTF	Radiotelephony
SF	Single Frequency
SJU	SEAR Joint Undertaking
SP	Service Provider
RSS	Received Signal Strength
RTCA	Radio Technical Commission for Aeronautics
Rx	Receiver
SARPS	Standards and Recommended Practices
SBAS	Satellite Based Augmentation System
SCA	Spreading Code Authentication
SCP	Smoothed Concave Hexagonal Pulse
SDR	Software Defined Receiver
SESAR	Single European Sky ATM Research
SID	Standard Instrument Departure
SNPR	Signal-to-Noise Power Ratio
SSR	Secondary Surveillance Radar
SSR	Spoofing to Signal Ratio
STAR	Standard Instrument Arrival
STL	Satellite Time and Location
SUR	Surveillance
SV	Space Vehicle
SWAL	Software Assurance Level
SWIM	System Wide Information Management
SW	Software
SWX	Space Weather
TACAN	Tactical Air Navigation
TDOA	Time Difference of Arrival
TMA	Terminal Maneuvering Area
TRL	Technology Readiness Levels
TTRP	Time to Re-compute Position
Tx	Transponder
UAS	Unmanned Aerial System
UAT	Universal Access Transceiver
UTM	U-Space Traffic Management
VFR	Visual Flight Rules
VOR	Very High Frequency Omni-directional Range
VNAV	Vertical Navigation
VHF	Very High Frequency
WAM	Wide Area Multilateration

4. EXECUTIVE SUMMARY

The goal of the AIRING project is to define a roadmap for the implementation of new technical and operational safeguards (in the short-, mid- and long-term) to improve the resilience of GNSS use in Aviation against RFI threats (including jamming and spoofing), in a way that not only brings operational benefits in the short-run but also, and more importantly, prepare Aviation for the advent by 2030 of DFMC GNSS and a stronger dependency on GNSS to support the exclusive use of PBN navigation.

To define that roadmap the main activities performed in the AIRING project have been:

- To carry out a **security risk assessment** to estimate the level of operational risk expected in Aviation by 2030 (the reference timeframe), should no new technical or operational safeguards be put in place. The objectives of this security risk assessment are:
    - To define the baseline level of operational risk (in the *do-nothing* scenario)
    - To define the target level of operational risk (to be met at some point in the roadmap)
    - To identify the different types of safeguards that could be implemented, and the mechanisms through which those safeguards would reduce the operational risk
- To identify, through a review of the state-of-the-art, the candidate technologies that could be implemented in space, on-board an aircraft (or another aerial vehicle, e.g. UAS), or on ground to act as technical safeguards against GNSS RFIs. Those technologies can be classified as:
    - **Detection**: to enable an equipment (e.g. a GNSS receiver) to detect an RFI
    - **Mitigation**: to enable GNSS receivers to operate despite the presence of RFIs
    - **Localization**: to allow an equipment or system to help in locating the source of an RFI
    - **Reversion**: to provide non-GNSS PNT services (in case of loss of GNSS)

  Other supporting, but key, technologies are those that help in **assessing the impact** of RFIs, and those that facilitate the **exchange of information** pertaining to RFIs among stakeholders.
- To analyze, taking into account different criteria (including the maturity of the technology, the expected performances, the complexity of the technology, the impact on the aircraft, the cost for the implementation, and a system-wide approach), the different technologies, and then to **recommend** the implementation of a sub-set of those **technologies** to help achieving the target level of operational risk.
- To carry out a **quantitative assessment of** the **effectiveness** performances of most of the selected on-board and ground technologies, through the execution of an extensive number of laboratory tests, plus several live demonstrations, in which different DUTs (implementing one or several of those technologies) were subject to different RFI threats scenarios.
- To define an **operational concept** for RFIs management by the different stakeholders, which includes the identification of mitigation operational safeguards to complement the technical ones
- To **update the security risk assessment** in order to estimate the remaining level of operational risk should those recommended technologies be implemented as technical safeguards, as well as the impact of operational mitigations on meeting the target level
- To propose a **timeline for** the **implementation** at different stages (short-, mid-, and long-term) of the recommended set of technologies, and a **roadmap** with the activities to promote and facilitate the implementation of the proposed technical and operational safeguards

Next sections describe these main tasks of the project:

- Section 4.1 describes the initial security risk assessment
- Section 4.2 identifies the different types of safeguards to be implemented
- Section 4.3 describes the recommended technologies
- Section 4.4 describes the proposed operational concept to manage RFIs
- Section 4.5 presents the results of the updated security risk assessment

- Section 4.6 explains the timeline for the implementation of the recommended technologies
- Section 4.7 details the short-, mid- and long-term roadmap

Besides these main sections, the reader can find in this document additional information on the laboratory assessment on the on-board and ground technologies (5. Annex A and 6. Annex B), on other assessment activities such as the open field tests, live demonstrations and operational tests (7. Annex C), and some recommendations to support the implementation of the roadmap (8. Annex D)

4.1. INITIAL SECURITY RISK ASSESSMENT

The **main steps of this security risk assessment** are:

- The identification of the RFI threats environment
- The definition of the RFI security events,
- The estimation of the likelihood of each of those RFI security events,
- The definition of the KPAs to assess the operational impact of any of those RFI security events in a given operational scenario,
- The definition of a number of representative operational scenarios and the assessment of the impact of those RFI security events on each of those scenarios, and
- The combination of the likelihood of each RFI security event and its operational impact on each operational scenario in order to estimate the risk level in each of those adverse scenarios.

An analysis has been performed to assess the effects that different **RFI types** may have on GNSS receivers, operational concerns, perpetrators and the RFI sources. The analysis is based on the widely used classification of jamming and spoofing threats presented in the table below [ION].

Table 4-1 Classification of RFI threats

RFI Types		
Jamming		**Spoofing**
J1 – Collateral jammers		**S1** – Repeaters
J2 – High Power jammers		**S2** – Errant signals
J3 – Targeted jammers		**S3** – Collateral spoofers - simulators
J4 – Targeted sophisticated jammers		**S4** – Collateral Re-radiating spoofers
		S5 – Targeted spoofers
		S6 – Targeted re-radiating spoofers
		S7 – Targeted sophisticated spoofers

Different types of emissions (RFI types) can result in similar consequences on the GNSS receiver. These consequences could be:

- [1] Decrease of the measured C/N0.
- [2] Temporal loss of one or several observed satellite / loss of satellite track.
- [3] Loss of all satellite tracks in a frequency band.
- [4] Jump in the estimated pseudorange/time of a satellite due to cycle slips in phase measurements.
- [5] Track of spoofed satellite signal causing large jumps in estimated pseudorange/time.
- [6] Track of spoofed satellite signal in phase with true satellite signals causing minor errors in estimated pseudorange/time.

The consequences of the different RFI types have been grouped into three RFI security events:

- GNSS degraded.
- GNSS unusable.
- GNSS misleading.

GNSS degraded: this event covers all situations in which the position error increases due to the RFI. In such cases, it is expected that error estimates will increase and as such, an aircraft navigation solution will be able to inform the pilot on the GNSS conditions. The timing error inflicted by this event remains below one millisecond. When GNSS is degraded the position error increases but the signal is not completely lost. This can happen when low power or intermittent inference is encountered. Typically, this can be by collateral jammers **(J1)** or when aircraft fly at the fringes of a targeted jammer event **(J3 or J4)** or when attacks are planned, using intermittent jamming techniques. These events will lead to increased noise levels.

GNSS unusable: This RFI security event covers all situations in with the GNSS position estimates becomes unavailable. Meaning that the GNSS receiver is not able to make a valid position report. The most likely threat scenarios for this event are (High Power) Targeted Jammers (**J2, J3**) or Targeted Sophisticated Jammers (**J4**). The effect will be the loss of all satellite tracks in the frequency band(s) used by the receiver. It also includes all situations in which position estimates are on-and-off available such that continuity is lost.

GNSS misleading: In this RFI security event the GNSS position and time calculation is not correct but still used by the systems on board the aircraft. The integrity of a position estimate will be lost without warning to the flight crew. This includes erroneous position and time estimates due to falsified GNSS signals causing minor to large errors in the pseudorange estimates (**E4, E5, and E6**). This covers a large group of errors resulting from different type of spoofers, including collateral spoofers, errant signals and repeaters creating jumps in pseudorange and time measurements (**S2 to S7**).

To characterize the likelihood of each of the RFI security events a weighted likelihood that combines the likelihood of each of the RFI threat types with the likelihood that each of those RFI threat types causes one of the RFI security events has been computed.

The resultant **likelihood** of a "GNSS Unusable" event affecting an aircraft caused by a jamming threat has been assessed as **occasional** (between 10^{-3} and 10^{-5} per flight hour), whereas the likelihood of a "GNSS Misleading" event caused by a spoofing threat has been assessed as **remote** (between 10^{-5} and 10^{-7} per flight hour). The numerical values for the likelihood categories are taken from [SKYBRA] (which refers to the ICAO Safety Management Manual, [Doc9859])

To assess the impact of RFI security events on aircraft operation three Key Performance Areas (KPA) are applied: **Flight Safety, Flight Efficiency, and Flight Capacity**.

In aviation, safety is the most critical performance indicator. The selection of capacity and efficiency results from the review of the PBN Handbook No 6 [PBNHND], which applies these areas when assessing the operational impact of GNSS unusable. This seems an obvious choice as aviation is a highly competitive industry and a global enabler of connectivity.

The impact on operations is assessed through **six nominal operational use scenarios**:

- **Scenario 1**: High density TMA/CTR of an airport with mostly IFR commercial traffic and RNP 1 SID and STAR procedures.
- **Scenario 2**: Low density TMA/CTR serving one or multiple smaller regional airports, including IFR and VFR traffic and RNAV 1 SID and STAR procedures. This scenario is divided into two:
    - **Scenario 2A**: currently operating low density regional airport, with back-up navigation infrastructure, such as VOR, DME, ILS Cat I
    - **Scenario 2B**: future regional airport (on the 2030 horizon), without back-up navigation infrastructure (i.e. a GNSS-only scenario)
- **Scenario 3**: Medium to high density en-route continental airspace with good DME-DME / VOR-DME coverage.
- **Scenario 4**: Medium to high density en-route oceanic, remote continental and continental airspace with no DME-DME / VOR-DME coverage.

- **Scenario 5**: Drone traffic over urban and rural areas, including Beyond Visual Line of Sight (BVLOS) operations and U-space Traffic Management (UTM).
- **Scenario 6**: High density TMA/CTR of an airport with IFR commercial traffic and high-density drone traffic in and over the nearby urban area.

Risk Assessment is an analysis that combines the probability of the hazard (the likelihood of that harm being realized during a specified amount of time of exposure to the risk) with the severity of these effects (the potential to cause harm) on the aircraft operation.

The result of a Risk Assessment is a score (a risk severity level) in a risk matrix. This is done by **combining the likelihood score with the impact score**. The risk score (severity level) has been assessed in each of the flight phases of each of the adverse scenarios, and for each of the identified RFI security events. To do so, the highest of the Flight Safety, Flight Efficiency and Flight Capacity severity levels has been taken as the impact score, and the estimated likelihood category for each of the RFI security events has been taken as the likelihood score.

Next, the following risk matrix taken from SecRAM 2.0 [SECRAM] (the Security Risk Assessment methodology by the SJU for the SESAR 2020 program) has been applied to **determine the risk score** (risk level). However, the names of each likelihood category and impact severity scores are taken from ICAO Safety Management Manual [Doc9859]:

Table 4-2: Risk matrix from [SECRAM]

		Impact				
Likelihood category [Doc9859]	**Likelihood score**	**1**	**2**	**3**	**4**	**5**
Frequent	**5**	Low	High	High	High	High
Occasional	**4**	Low	Medium	High	High	High
Remote	**3**	Low	Low	Medium	High	High
Improbable	**2**	Low	Low	Low	Medium	High
Extremely improbable	**1**	Low	Low	Low	Medium	Medium

The risk levels obtained after assessing the different flight phases of the adverse scenarios for each RFI security event are summarized in the following table:

		GNSS Degraded							GNSS Unusable							GNSS Misleading						
Scenario	**Flight phase**	**1**	**2A**	**2B**	**3**	**4**	**6**	**5**	**1**	**2A**	**2B**	**3**	**4**	**6**	**5**	**1**	**2A**	**2B**	**3**	**4**	**6**	**5**
Manned	**Departure**	L	M	M			M		M	M	H			H		H	H	H			H	
	En-route				L	L						M	H						H	H		
	Arrival	L	M	M			M		M	M	H			H		M	H	H			H	
	Approach	L	M	M			M		M	M	H			H		H	H	H			H	
Unmanned	**BVLOS**							M							H							H

In the light of the results of the previous risk assessment, which found that there is a **high security risk in many flight phases of the adverse operational scenarios** studied, it is imperative that new safeguards are implemented to reduce that risk.

The **overall goal** of the new safeguards is to reduce to **medium** the maximum level of operational risk in any phase of the selected operational scenarios when subject to the different RFI security events.

4.2. IDENTIFICATION OF NEW SAFEGUARDS

Safeguards can be classified into two groups, those aimed at **reducing the likelihood of an RFI security event**, and those aimed at **minimizing the impact of an RFI security event** after it has occurred.

Safeguards aimed at reducing the likelihood of an RFI security event occurrence are:

- **Deterrence**: a safeguard deters attackers when they do not dare to attack (e.g. legislation or enforcement). If the safeguard is not effective enough, the attack will take place. A deterrent safeguard could be prohibiting the free marketing of jamming devices.

- **Elimination**: a safeguard eliminates an incident when it prevents it from occurring. These safeguards work before the incident occurs. They do not limit harm if the safeguard is not perfect, and the incident occurs.

  In this context, an elimination safeguard would be the act of making adequate resources available to States and for States to use them to eliminate a detected and located RFI emitter.

- **Prevention**: a safeguard is preventive when it reduces the likelihood of the incident occurring. If the safeguard fails and the incident occurs, the impact does not change.

  In this context, **mitigation techniques** that could be **implemented in the on-board GNSS receiver** are considered preventive safeguards, as they are intended to prevent the occurrence of a given RFI security event that would occur in the absence of such mitigations.

Safeguards aimed at **minimizing the impact of an RFI security event** after it has occurred are:

- **Detection**: safeguards that detect incidents and enable or trigger immediate reaction

  In this context, **detection techniques that could be implemented in the on-board GNSS receiver**, **detection and localization techniques that could be implemented in ground systems**, and **airspace impact assessment**, as well as **information sharing** between the different actors (e.g., aircrew, ATCOs, ANSPs, AOCs, NM) are considered detection safeguards.

  Note that if an RFI security event is detected and the affected airspace is identified, aircraft flying into that airspace can change their planned route, and thus avoid that security risk; in other words, detecting an RFI security event at one location may also reduce the likelihood of an RFI security event to affect other aircraft at other locations.

- **Awareness**: awareness safeguards are those focused on improving the capabilities of people who may interact with the system (e.g., pilots, ATCOs, AOCs staff). Awareness reduces unintentional errors. Operators training improves incident response time, and the performance of recovery safeguards.

- **Consequences minimization**: a safeguard minimizes the impact when it does not prevent the incident from occurring but limits the consequences.

  In this context, the availability of **redundant** (non-GNSS) **on-board equipment, ground services** (e.g. conventional navaids), and **operational procedures** (e.g., non-GNSS navigation applications) are regarded consequences minimization safeguards.

  The availability of **alternative GNSS navigation modes in the on-board GNSS receiver** (e.g., GPS or Galileo only) is also considered a consequences minimization safeguard

- **Recovery**: safeguards that, after an incident has occurred, are capable of restoring the previous situation after a period of time. The incident is not less likely, but the consequences are limited.

  In this context, the measures that pilots (supported by their AOCs) and ATCOs could take to deal with a detected RFI security event are considered recovery safeguards.

4.3. SELECTION OF TECHNOLOGIES

The project research has focused on **new prevention** (e.g. mitigation measures implemented in the on-board GNSS receivers) **detection** (e.g. detection capabilities implemented in the on-board GNSS receivers, and detection and localization capabilities implemented on ground-based systems), and **consequences minimization** (e.g. operational procedures) **safeguards**.

Next sections describe the main findings of that research:

- Section 4.3.1 presents a system concept to manage RFIs in Aviation, in order to provide a framework to understand how the proposed technological and operational safeguards fit
- Section 4.3.2 describes the proposed on-board detection and mitigation technologies
- Section 4.3.3 describes the recommended ground detection and localization technologies
- Section 4.3.4 briefly outlines some potential space-based detection and localization technologies

- Section 4.3.5 presents some potential alternative PNT services that can act as back-up to GNSS
- Section 4.3.6 describes other supporting technologies (e.g. an API to foster information sharing)

Note that for the update of the security risk assessment only the recommended on-board and ground technical safeguards have been considered (but not the space-based nor the A-PNT services)

4.3.1. SYSTEM VIEW FOR RFI MANAGEMENT IN AVIATION

Figure 4-2 below depicts a system view of the Aviation system for RFI detection, mitigation and localization. In particular, that figure shows the key system elements and the interfaces among them.

First of all, the key elements identified in a generic aircraft are the crew (supported by a set of operational mitigation procedures and contingency plans), a cockpit (where the information on RFIs are presented to the crew), GNSS antennae and GNSS receivers (a fully redundant GNSS processing chain in many cases), other sensors (e.g. IMU) and equipment (e.g. to navigate with conventional navaids), an ADS-B transponder, and, possibly, a specific equipment that could be installed on-board to provide additional GNSS RFI detection capabilities (e.g. processing the signals from two GNSS antennae with spatial processing techniques could support spoofing detection and spoofing signal DOA estimation).

Note that the conventional GNSS antenna shown in the picture could be replaced by a Dual Polarization Antenna (DPA), a Controlled Radiation Pattern Antenna (CRPA), or a Synthetic Antenna Array.

Being the GNSS receiver a key on-board element, it is worthy to show here a more detailed view of its lower-level constituents (corresponding to different stages of the GNSS signal processing chain) because the proposed on-board RFI detection and mitigation techniques (see section 4.3.1) are classified accordingly.

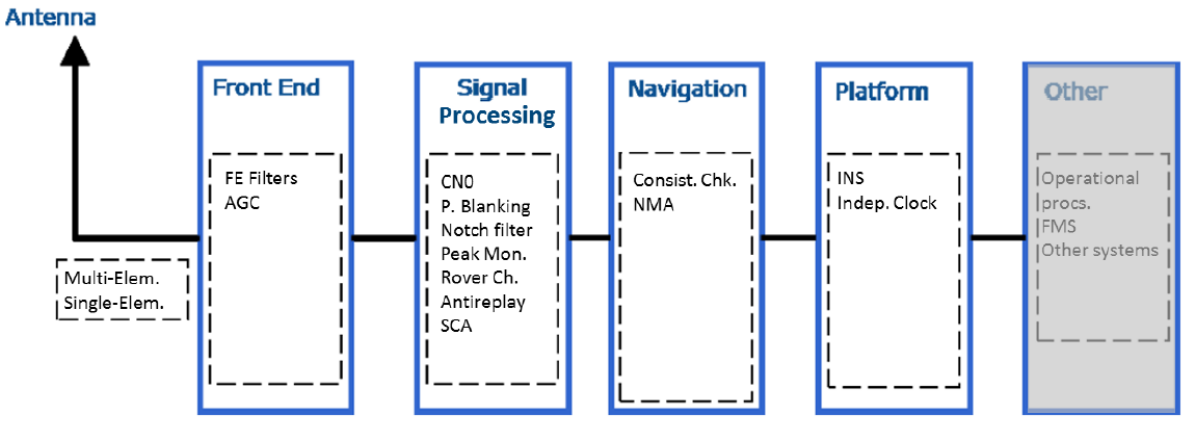


Figure 4-1: Generic GNSS receiver architecture [ION]

Secondly, it is also worth highlighting the key aircraft-ground interfaces.

On the one hand, the interfaces between the crew/cockpit and the ATCO/ATC, e.g. a voice communication interface for crew to convey information to ATC about any GNSS problem detected on-board (as the GPS outages reported today, which are reported on a voluntarily basis and that are periodically reported by Eurocontrol in the EVAIR bulletins [EVAIR]) or for crew to receive instructions from ATC to mitigate operationally the reported GNSS problem (e.g. radar vectors in the approach phase of the flight in the event of a total loss of the GNSS service due to a wide area jamming event), and a data link interface (e.g. D-ATIS) to exchange any new piece of RFI information available automatically, or upon a crew or ATCO specific action.

On the other hand, the aircraft-ground interface that consists in the automatic transmission of information from some on-board equipment to the corresponding CNS infrastructure on-ground.

In this diagram we assume that such interface will be implemented through an ADS-B transponder (by including the relevant RFI information in the ADS-B messages which are periodically transmitted to ground) rather than through other specific communication equipment.

It is worth clarifying that three different sets of information could be transmitted automatically to ground through this interface: (a) the current content of the ADS-B messages, (b) basic information on the GNSS RFI events detected on-board (e.g. RFI flags), or (c) more elaborated information on the GNSS RFI events detected by the on-board equipment (e.g. power, DOA or AOA of the detected RFI signal) which could be further processed on ground to, by combining the information from other aircrafts affected by the same RFI source, enable hybrid (i.e. on-board + ground) RFI source localization.

On the ground side, one must emphasize that the elements shown correspond to two different stakeholders: a generic ANSP (because the airspace is managed at State level, and so each ANSP needs to have its own ATM/CNS systems and operational staff) and the Network Manager (NM), a role currently performed by Eurocontrol for the ECAC and other associated countries (a wider context than the EU).

At the ANSP level, the diagram (Figure 4-2) shows different mechanisms for the identification of GNSS events:

- The collection (e.g. through the crew/ATCO voice, aircraft/ATC data link, and ADS-B messages interfaces) of GNSS reports generated on-board the aircraft.
- Two mechanisms that provide ground with the capability to further process the RFI information collected from one or multiple aircraft: (i) to detect GNSS jamming events affecting those aircraft (and localize the source of the GNSS jamming source) by processing ADS-B messages; and (ii) to detect GNSS spoofing events affecting those aircraft by processing the surveillance information available on ground from several independent sources (e.g. ADS-B, MLAT/WAM)
- RFI monitoring networks that provide ground with the capability to detect GNSS jamming and spoofing events occurring on ground, and, possibly, to localize the source of the corresponding GNSS jamming and spoofing signals.

  We must stress that this diagram only shows the ground elements that are expected to be continuously operated by a generic ANSP, i.e. those elements subject to integration into a wider system (with their output data automatically processed). For this reason, other resources that some ANSP could have available but that would require their activation upon the detection of a RFI event (e.g. a flight inspection aircraft, a portable RF direction equipment, an UAS able to detect and localize the source of a RFI) are not shown.
- RFI detection equipment associated with GBAS stations.

The diagram (Figure 4-2) also identifies, at ANSP level, an element which will perform several centralized tasks:

- The collection of GNSS RFI on-board and on-ground data and reports accessible to the ANSP
- The collection of GNSS RFI data and reports generated by other sources external to the ANSP

  To achieve this goal, we have represented a standardized interface for the exchange of data.
- The reception of information from the GNSS service providers (e.g. EGNOS and Galileo service providers) on the current (and possibly on the short and mid-term forecast) availability of different levels of E-GNSS services
- The reception of information on GNSS forecast outages from other sources (e.g. from Eurocontrol's AUGUR API REST services, from NOTAM proposals published in EAD by Eurocontrol, or from NOTAM proposals submitted by ESSP).

  Note that these forecast GNSS outage notifications refer to either a particular aerodrome or to a particular approach procedure. In other words, they are not forecast wide area outage notifications and, as such, could be used to infer the potential presence of a GNSS RFI as the cause of the notified outage but, per se, they are not GNSS RFI notifications.
- The joint processing of all the collected and received information in order to:
  - Confirm that the detected GNSS RFI events are caused by jamming and/or spoofing signals

- Further process the collected data to cluster (i.e. group together) the RFI events caused by the same jamming and/or spoofing signal, improve the accuracy of the RFI source localization, and estimate the airspace volumes that could be impacted by a localized RFI source as well as the level of impact that different aircraft categories flying within each of those airspace volumes could suffer (e.g. performances degradation, total loss of GNSS navigation, high risk of successful GNSS spoofed navigation, etc.)
- Extract information from the GNSS RFI data and reports about the key features of the RFI signal, and store that information in a RFI Threats database, with the applicable security-driven access rights
- Generate consolidated GNSS RFI reports (on top of the individual collected reports) and store them in a database that could be shared, with the access rights defined by the security policy in force, through an API mechanism (see below)
- Generate, in accordance with the applicable security policy and operational procedures, GNSS RFI NOTAM proposals, and send them to the ANSP NOF for their approval and distribution (e.g. to airspace users, such as the aircraft operators). Note that the current RFI NOTAM standard only allows the definition of a time period, a location or area, and a generic message

Another important element that will be required at ANSP level to allow the sharing of RFI information will be an API that would provide automated data services (e.g. by means of RESTful services) to distribute information about the collected GNSS RFI data reports to other stakeholders' systems.

As far as the interfaces of an ANSP API with other stakeholders are concerned, we foresee, at least, the following: an interface with its own ATC units, an interface with the Network Manager (NM), an interface with other stakeholders (e.g. the National Spectrum Regulator, Airport Operators, Airspace Users, CNS service providers, the Military -for the sake of civil-military coordination-, and other ANSPs -to address, for instance, cross-border events-), and an interface with other external sources of RFI information (e.g. national monitoring networks, Space-based RFI detection systems).

Please notice that in the concept we are proposing, one API instance (server) would need to be deployed by each ANSP at their own facilities, and enabled to exchange data among them in accordance with the security policy defined at State level (if relevant)

The diagram also shows, at ANSP level, the mitigation operational procedures and contingency plans that would be available to the ATCOs to react in difference GNSS RFI scenarios.

Moreover, as mentioned above, the diagram also shows some key elements that should be managed by the Network Manager, which are:

- The generation of periodic GNSS RFI reports (e.g. to replace the GPS outages section of the current EVAIR bulletins, or to be inserted into upgraded EVAIR bulletins in the future) that could be shared, with the access rights defined by the security policy in force, through an API mechanism.
- The deployment of an additional API (server), which would collect data from the APIs deployed at ANSP level and, possibly, share some of its own data with the ANSPs, for instance, in the case that certain stakeholders (Aircraft Operators, IATA, etc.) report directly to the NM (as today with EVAIR)

  This API specific to the NM would also establish an interface with its own ATFCM system, to enable NM operational staff to be aware of any GNSS RFI data relevant for its Demand and Capacity function

Finally, please notice that the diagram does not show some elements that could play an operational role in a system-wide management of GNSS RFI threats, such as Space-based GNSS RFI detection and localization capabilities, or other navigation (A-PNT) infrastructure, etc.

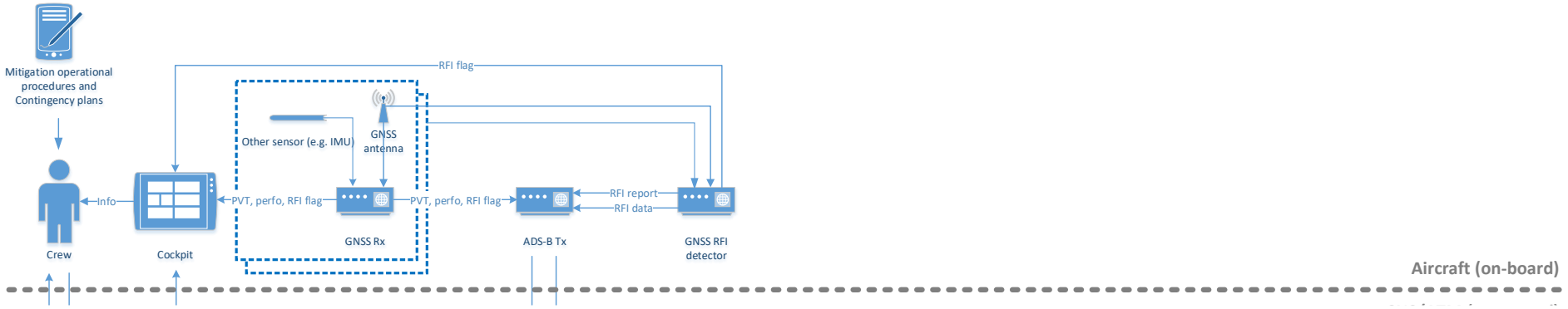


Figure 4-2: Aviation system view for RFI detection, mitigation and localization (on-board segment)

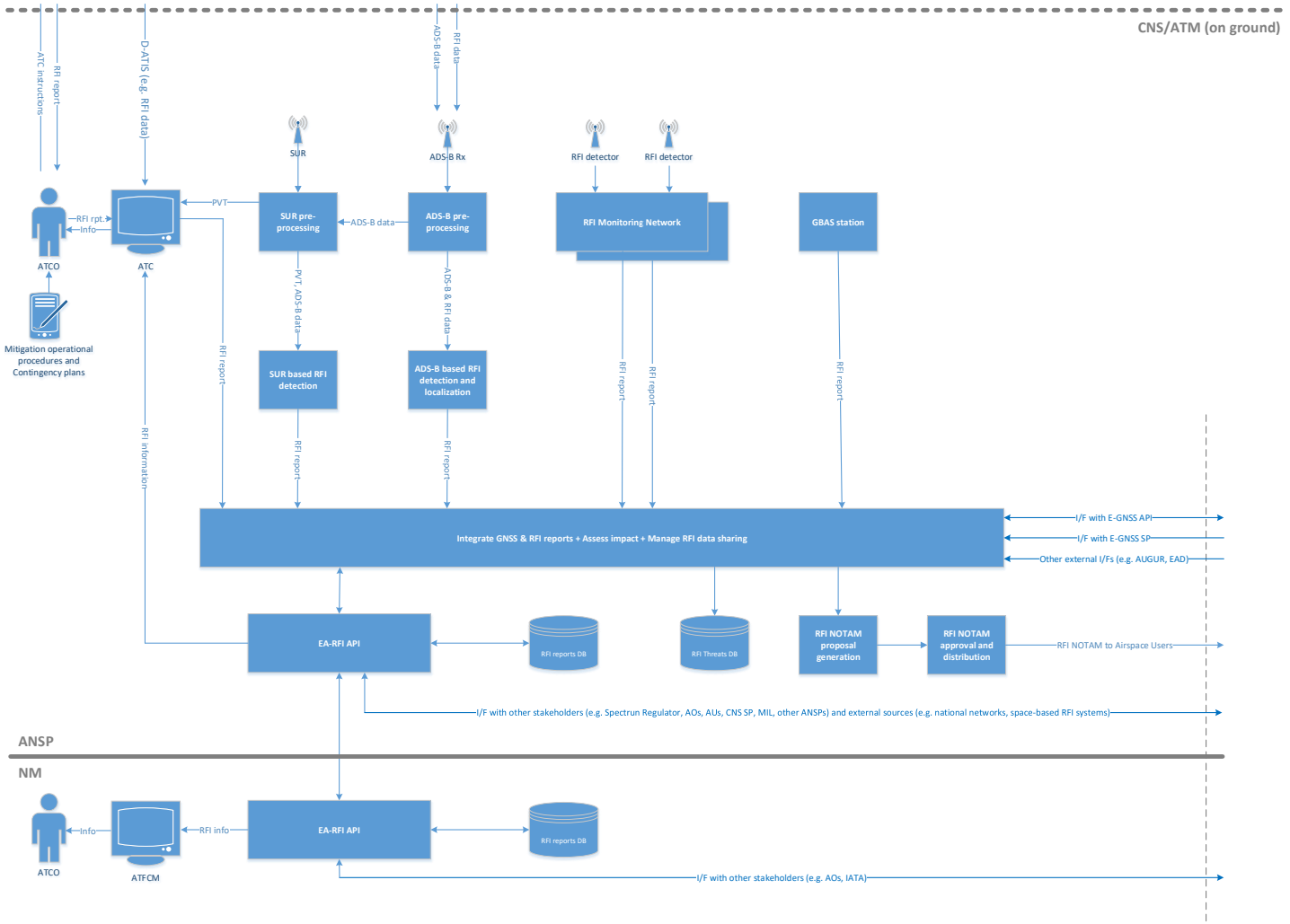


Figure 4-3: Aviation system view for RFI detection, mitigation and localization (ground segment)

4.3.2. ON-BOARD DETECTION AND MITIGATION TECHNOLOGIES

The analysis performed on the on-board technologies to detect and mitigate GNSS RFIs in the frame of the AIRING project (see [REP05]) can be summarized in the next set of tables. The technologies tested in the AIRING project are highlighted in red.

Jamming and spoofing detection

Effectiveness of each technique against different threats (threat definition below) on a scale between 1 (ineffective) and 5 (very effective).

The threats are defined as:

Threat 1: CW interference

Threat 2: swept-CW interference

Threat 3: broad-band interference

Threat 4: pulsed interference

Threat 5: non-consistent spoofing (inconsistent in position, time and/or power)

Threat 6: consistent spoofing (consistent in position, time and power)

Threat 7: very-advanced spoofing (multiple coherent transmitters)

Table 4-3: jamming and spoofing detection techniques effectiveness matrix

	Threat 1	Threat 2	Threat 3	Threat 4	Threat 5	Threat 6	Threat 7
CRPA	5	5	5	4	5	1-4	1
-DS DoA	5	5	5	4	5	1-3	1
-MVDR DoA	5	5	5	4	5	1-3	1
-MUSIC DoA	5	5	5	4	5	1-4	1
-ESPRIT DoA	5	5	5	4	5	1-4	1
D3	N/A	N/A	N/A	N/A	5	5	2-4
P&F DoA	N/A	N/A	N/A	N/A	5	5	2-5
AGC	5	5	5	5	1-3	1-3	1-3
APM	4	4	4	1-3	1-3	1-3	1-3
C/N0	3	3	3	1	1	1	1
Filter-based detection	5	5	4	5	3	1	1
Correlation peak monitoring	SF+DF	N/A	No	No	4-5	3-4	3-4
Rover channels	N/A	N/A	N/A	N/A	4-5	3-4	3-4
Consistency checks	N/A	N/A	N/A	N/A	3-5	4-5	2-3

Table 4-4: jamming and spoofing detection techniques properties matrix

	SF/DF	Single / multiple antenna	Jamming detection	Jamming characterisation	Jamming localization	Spoofing detection	Spoofing localization
CRPA	SF+DF	Single, 4+ elements	Yes (N-1)	No	Yes (AoA)	Yes	Yes (AoA)
- DS DoA	SF+DF	Single, 4+ elements	Yes (N-1)	No	Partial	Yes	Partial
- MVDR DoA	SF+DF	Single, 4+ elements	Yes (N-1)	No	Partial	Yes	Partial
- MUSIC DoA	SF+DF	Single, 4+ elements	Yes (N-1)	No	Yes	Yes	Yes
- ESPRIT DoA	SF+DF	Single, 4+ elements	Yes (N-1)	No	Yes	Yes	Yes
D3	SF+DF	2+	No	No	No	Yes	No
P&F DoA	SF+DF	2+	No	No	No	Yes	Yes
AGC	SF+DF	N/A	Yes	No	No	Partial	No
APM	SF+DF	N/A	Yes	No	No	Partial	No

	SF/DF	Single / multiple antenna	Jamming detection	Jamming characterisation	Jamming localization	Spoofing detection	Spoofing localization
C/N0	SF+DF	N/A	Partial	No	No	Partial	No
Filter-based detection	SF+DF	N/A	Yes	Partial	No	Partial	No
Correlation peak monitoring	SF+DF	N/A	No	No	No	Yes	No
Rover channels	SF+DF	N/A	No	No	No	Yes	No
Consistency checks	SF+DF	N/A	No	No	No	Yes	no

Impact aspects versus technology. Consider Complexity (1 low – 5 high), Technology maturity (1 low – 5 high), impact on aircraft (1 low – 5 high), cost of implementation on a 1 (cheap) – 5 (very expensive) scale.

Table 4-5: jamming and spoofing detection techniques implementation matrix

	Complexity	Technology maturity	Impact on aircraft	Cost of implementation
CRPA	3-5	2-3	3-5	3-4
-DS DoA	3	4	2	2
-MVDR DoA	3	4	2	2
-MUSIC DoA	4	4	2	2
-ESPRIT DoA	4	4	2	2
D3	2	4	2	2
P&F DoA	4	3	2	3
AGC	1	4-5	1	1
APM	3	3	3	2
C/N0	1	5	1	1
Filter-based detection	1-2	4-5	1	1-2
Correlation peak monitoring	4-5	4-5	3-5	3-5
Rover channel	4-5	1-3	3-5	3-5
Consistency checks	1-2	3-5	1	1

Jamming and spoofing mitigation

Effectiveness of each technique against different threats (threat definition below) on a scale between 1 (ineffective) and 5 (very effective).

The threats are defined as:

Threat 1: CW interference

Threat 2: swept-CW interference

Threat 3: broad-band interference

Threat 4: pulsed interference

Threat 5: non-consistent spoofing (inconsistent in position, time and/or power)

Threat 6: consistent spoofing (consistent in position, time and power)

Threat 7: very-advanced spoofing (multiple coherent transmitters)

Table 4-6: jamming and spoofing mitigation techniques effectiveness matrix

	Threat 1	Threat 2	Threat 3	Threat 4	Threat 5	Threat 6	Threat 7
Choke ring	1-3	1-3	1-3	1-3	1-3	1-3	1-3
CRPA	4-5	4-5	4-5	3	4-5	1-3	1
ANF	5	5	1	3	1	1	1

	Threat 1	Threat 2	Threat 3	Threat 4	Threat 5	Threat 6	Threat 7
PB	1	1	1	5	1	1	1
MFT	4	4	4	4	1	1	1
Filter-based	5	4	1	5	1	1	1
Control Loop Parametrization (effective when already tracking actual GNSS signals)	N/A	N/A	N/A	N/A	4	2-3	2
Consistency checks, Multi-frequency multi-constellation diversity	3-4	3-4	3-4	3-4	3-4	3-4	3-4
NMA	N/A	N/A	N/A	N/A	4	4	4
Independent clock reference	4	4	4	4	4	2	1
Aircraft level checks	4	4	4	4	4	2	1
Ranging code encryption*	1	1	1	1	5	5	5

Table 4-7: jamming and spoofing mitigation techniques properties matrix

	SF/DF	Single / multiple antenna	Jamming mitigation effectiveness	Spoofing mitigation effectiveness	Encryption-based
Choke ring	SF+DF	Single	Low elevations only	Low elevations only	No
CRPA	SF+DF	Single, 4+ elements	Yes	Yes, higher power only.	No
ANF	SF+DF	Single	Yes High for CW jamming	No	No
PB	SF+DF	Single	Yes High for Pulsed jamming	No	No
MFT	SF+DF	Single	Yes High for Wideband jamming	No	No
Filter-based	SF+DF	Single	Partial	No	No
Control Loop Parametrization	SF+DF	Single	No	Partial	No
Consistency checks Multi-frequency multi-constellation diversity	SF+DF		Yes Medium	Yes Medium	
NMA	SF	Single	No	Partial	Yes
Independent clock reference	SF+DF	Single	Yes, timing only	Yes, timing only	No
Aircraft level checks	SF+DF	Single	Yes	Yes	No
Ranging code encryption*	DF	Single	No	Yes	Yes

Table 4-8: jamming and spoofing mitigation techniques implementation matrix

	Complexity	Maturity	Impact on aircraft	Cost of implementation
Choke ring	1	5	2	1
CRPA	3-5	2-3	3-5	3-4
ANF	1	4	1	1

	Complexity	Maturity	Impact on aircraft	Cost of implementation
PB	1	4	1	1
MFT	5	1	3	4
Filter-based	1-2	4-5	1	1-2
Control Loop Parametrization	4	2	3-4	3-4
Consistency checks Multi-frequency multi-constellation diversity	1-3	3-4	2-4	2-4
NMA	1-2	2-3	2-3	2-3
Independent clock reference	2-4	4	3	2
Aircraft level checks	3	3-5	2	3
Ranging code encryption*	5	4	4-5	4

4.3.3. GROUND DETECTION AND LOCATION TECHNOLOGIES

The analysis performed on the ground technologies to detect and locate GNSS RFIs in the frame of the AIRING project (see [REP05]) can be summarized in the next two tables.

The first table (Table 4-9) shows the functional capabilities of the analyzed technologies to detect and locate jamming and/or spoofing threats in different GNSS bands and signals.

Table 4-9 Functional capability of ground technologies for RFI detection and location

	GNSS constellations and bands	Jamming detection	Spoofing detection	Jamming location	Spoofing location
RFI monitoring networks					
1st capability level	GPS L1/L5 GAL E1/E5a	Yes			
2nd capability level		Yes	Yes		
3rd capability level (state-of-the-art)		Yes	Yes	Yes	*
4th capability level		Yes	Yes	Yes	Yes
Surveillance data processing systems					
Current ADS-B messages (QIs)	L1/E1	Yes		Yes	
Future ADS-B messages (RFI power) EUROCONTROL RFI mitigation concept	L1/E1 L5/E5a	Yes**		Yes	
Future ADS-B messages (RFI AoA/DoA)	GPS L1/L5 GAL E1/E5a	Yes**	Yes**	Yes	Yes
Comparison between surveillance sources (ADS-B vs MLAT/WAM)	GPS L1		Yes		
Multilateration based on extensive surveillance networks (ADS-B /FLARM)	GPS L1/L5 GAL E1/E5a		Yes		Yes

* Spoofing RFI detected as a jamming RFI (if above detection threshold)
** Requires new on-board GNSS antenna, Rx, ADS-B Tx or specific equipment

One observation worth mentioning about this table is that the RFI monitoring networks are classified in four capability levels (the 3rd representing the state-of-the-art of solutions available in the market)

The table highlights in red the technologies that have been further assessed in AIRING with laboratory tests and/or live demonstrations.

The second table (Table 4-10) presents the results of the analysis of the implementation of each of those technologies expressed in terms of maturity, impact, complexity and cost factors.

Table 4-10 Analysis of ground technologies for RFI detection and location

	Complexity	Maturity	Impact on aircraft	Impact on CNS	Cost
RFI monitoring networks 3rd capability level (state-of-the-art)	5	4	1	1	4
Surveillance data processing systems					
Current ADS-B messages (QIs)	3	3	1	1	2
Future ADS-B messages (RFI power) EUROCONTROL RFI mitigation concept	3	3	3	2	3
Future ADS-B messages (RFI AoA/DoA)	4	2	5	2	5
Comparison between surveillance sources (ADS-B vs MLAT/WAM)	2	2	1	1	2
Multilateration based on extensive surveillance networks (ADS-B /FLARM)	4	2	1	5	5

4.3.4. SPACE DETECTION AND LOCALIZATION TECHNOLOGIES

Space-based RFI detection systems consist of a number of satellites that provide continuous global monitoring of GNSS frequency bands through a payload of sensors, to detect and potentially characterise and localise GNSS RFI sources.

There are three options in terms of number of satellites: single satellite, dual satellite and multi satellite. Single satellite implies detection is only possible via Doppler or repeated measurements over several orbits, dual satellite implies two satellites in formation using TDOA/FDOA combined localisation and multi satellite implies constellation with three or more satellites with overlapping coverage.

In terms of data processing, there are also three options, ground based where events are detected with raw data sent to ground stations by downlink for post-processing, ISL where inter-satellite link is used to transmit data to satellite in view of ground station time of event, and OBP where full on-board processing of RFI event with characterisation and localisation. The combination of these options provides different level of complexity in implementing the in-space detection systems.

These combined options are assessed in terms of their capability for jamming and spoofing detection, localization and characterization, in the summary tables below.

Table 4-11: Space detection techniques properties matrix

	Jamming detection	Jamming characterisation	Spoofing detection	Jamming localisation	Spoofing localisation
Global coverage single sat LEO – Ground processing	Yes	No/ground-only	Yes – dependent on hardware	No/possible with repeated measurements	No/possible with repeated measurements
Global coverage – single sat LEO, with ISL	Yes	No/ground-only	Yes – dependent on hardware	No/possible with repeated measurements	No/possible with repeated measurements
Global coverage – single sat LEO, OBP	Yes	Yes	Yes – dependent on hardware	No/possible with repeated measurements	No/possible with repeated measurements
Global coverage – dual sat LEO	Yes	Ground-only	Possible	Yes – TDOA/FDOA combined	Possible – TDOA/FDOA combined
Global coverage – multi sat LEO – ground processing	Yes	Yes – ground only	Yes	Yes	Yes
Global coverage – multi sat LEO, with ISL	Yes	Yes – ground only	Yes	Yes	Yes
Global coverage – multi sat LEO, OBP	Yes	Yes	Yes	Yes	Yes

Effectiveness of each technique against different threats on a scale between 1 (ineffective) and 5 (very effective) is assessed in the next table. The threats are defined as:

Threat 1: CW interference

Threat 2: swept-CW interference

Threat 3: broad-band interference

Threat 4: pulsed interference

Threat 5: non-consistent spoofing (inconsistent in position, time and/or power)

Threat 6: consistent spoofing (consistent in position, time and power)

Threat 7: very-advanced spoofing (multiple coherent transmitters)

Table 4-12: Space detection techniques effectiveness matrix

	Threat 1	Threat 2	Threat 3	Threat 4	Threat 5	Threat 6	Threat 7
Single satellite	5	5	5	5	2	5	1
Dual satellite	5	5	5	5	3	5	1
Multi satellite	5	5	5	5	4	5	3

Finally, next table assesses some implementation factors: complexity, maturity (1 – low, 5 – high), reporting latency (1 – low, 5 – high), cost of implementation (1 - cheap, 5 - very expensive)

Table 4-13: Space detection techniques implementation matrix

	Complexity	Maturity	Reporting Latency	Cost of implementation
Global coverage single sat LEO – Ground processing	1	3	5	2
Global coverage – single sat LEO, with ISL	5	2	3	4
Global coverage – single sat LEO, OBP	5	1	2	5
Global coverage – dual sat LEO	2	1	2	3
Global coverage – multi sat LEO – ground processing	3	3	4	4
Global coverage – multi sat LEO, with ISL	5	2	2	5
Global coverage – multi sat LEO, OBP	4	2	1	5

Given that space-based monitoring of GNSS frequency bands is still at a very low level of maturity, more investigation work is needed to verify various detection techniques and gather data on the level of power of the signals that can be detected. Due to the development and maintenance costs, it is not feasible to build a large LEO based constellation to provide real-time global coverage for RFI detection. As technology becomes mature for small satellites in terms of the data processing, inter-satellite links would be recommended to ease the burden of ground processing and to decrease latency. Payloads hosting on-board other commercial or governmental programs is also a potential solution for space-based monitoring network without the need to develop a whole spacecraft. In terms of an 'early-service' it is recommended that a space-based RFI monitoring system makes use of single or dual-satellite localisation techniques which can be upgraded and scaled up with the development of data processing technology and an increase of monitoring satellites.

Space-based RFI detection system can be used for wide scale monitoring (and potentially localization) of strong RFI signals. The study of the three options regarding the number of satellites used for interference monitoring have shown that detection and Localisation is possible for each methodology, where the differing options also have a varying complexity of implementation in regard to the ground control segment required to support the spacecraft. These options combined with three implementation options for the data processing offer various complexity levels to the system.

To reduce the burden on the spacecraft systems in terms of processing power, characterization algorithm processing is better to be conducted mainly via ground systems. Spoofing detection may depend on the detection hardware on-board the satellite. The detection sensitivity by signal acquisition could be up to 1000 times more sensitive than C/N0 or received power monitoring for jamming

detection. This may be improved with multiple satellites in a constellation. With single-satellite localization, repeated measurements will be required in order to converge the position solution of an interferer. This may restrict the capability of a monitoring system to only static interference sources.

4.3.5. GROUND REVERSION TECHNOLOGIES

Several alternative PNT (A-PNT) solutions, such as passive ranging, hybrid A-PNT, eDME, eLoran, LEO PNT, LDACS and Mode N have been assessed.

Regarding **passive ranging**, two types are proposed: UAT based and DME based.

UAT already operates a signal designed for pseudo-ranging so that the existing signal can be used with no modifications. A benefit of UAT ground message is that it experiences little interference from intra-system sources. The primary technical challenge anticipated for UAT concerns coverage and multipath. Also UAT operates on a single frequency which allows for lower cost avionics. The drawbacks are that UAT is not used internationally and may not be desirable for commercial aircraft as they will be equipping with Mode S (1090 MHz) rather than UAT for ADS-B.

The benefits of DME passive ranging is that it uses compatible/complementary to DME/DME, and it does not modify the existing DME ground transmitters or signal. The most significant drawback is that currently using multiple DMEs requires expensive scanning DME. A purely passive DMPR receiver may be lower cost

Both UAT and DME normally only have the coverage in terminal areas. So it is difficult for them to be used for enroute navigation. However, the **hybrid APNT** by combining the two will extend the coverage and have the potential to cover the enroute navigation with more stations, as horizontal position only needs two stations in hybrid APNT. This reduces the DME loading by half and the needed stations by half. The drawback of hybrid APNT include the need for a high-quality clock and confidence on clock estimates and error growth.

These solutions all have the potential to meet the accuracy required for RNP 0.3, but a common issue for passive ranging and hybrid PNT is that the coverage is very challenging as the low altitude supported results in very few stations visible.

Enhanced DME (eDME) includes two proposed methods, one of which is to use more stable oscillators to provide carrier phase capabilities. It requires a clock stability in the order of 10^{-11} s^{-1}, such as the stability provided by RbXO clocks. Current ground station clock accuracy is in the order of 10^{-6} s^{-1}.

The implementation of DME carrier phase tracking improves accuracy significantly and boosts integrity performance, without DME spectrum modification.

Another method of enhanced DME is modification of pulse shape. Using Smoothed Concave Hexagonal Pulse (SCP) will help with multi-path mitigation and accuracy improvement about 37-38%.

eLORAN uses the existing infrastructure and low frequency band wholly independent of GNSS and can be used as backup of GNSS. It includes one or more Loran data channels that provide correction and integrity information. The key to meet the high availability requirement is the eLoran receiver's use of all-in-view technology. The performance of the system must also be maintained throughout each approach, with its duration of some 150 seconds.

eLORAN is considered suitable for remote and oceanic areas where the long-range characteristic plays the most important role, however the worldwide coverage would require construction of new stations.

The United States planned to build a new eLoran system as a complement to and backup for the GPS system by 2018. And the South Korean government had already pushed plans to have three eLoran beacons active by 2019. UK strived to push forward the eLoran application in Europe, however, in light of the decision by France and Norway to cease Loran transmissions on 31 December 2015, the UK announced at the start of that month that its eLoran service would be discontinued on the same day.

LEO constellations operate at low earth orbit below 2000 km. Compared to GNSS constellations operating at MEO, LEO based satellites signal has power level 30 dB stronger than GNSS signal, thus more resilient to interferences such as jamming and spoofing. The higher power level also makes it more ideal than GNSS signal in scenarios where GNSS signal is weak or unavailable, such as indoors. **LEO PNT** can be a wholly independent backup to replace GNSS when GNSS service is unavailable.

Currently the only operating LEO PNT is the STL service based on Iridium system which has 66 satellites in operation at altitude of 780km. The STL satellite time and location broadcast service is encrypted thus making it especially difficult to spoof. STL has the ability to provide timing within 1 microsecond and positioning with accuracy of 20 meters, all while deep indoors where GNSS is unavailable.

Satelles Inc., the provider of STL service, has raised $26 million in Series C funding. This new investment brings Satelles's total funding since the launch of its platform to $39 million and will help the company expand its sales and marketing efforts, broaden its partner network, and accelerate product development. This has made STL look more promising in the future. Other companies may follow the steps of Satelles. OneWeb promises to launch 648+ satellites, slated for the 2020s.

It is worth noting that LEO PNT requires large number of satellites to be launched and maintained, therefore it is very expensive to implement.

LDACS is developed by DLR. It has built-in ranging functionality which is developed and implemented to support APNT. It operates between two adjacent channels of DME in order to achieve spectral efficiency and minimize interference at the same time. When used as the APNT, the advantage of LDACS is that there is no major modification to the current network infrastructure, thus no extra cost incurred while achieving the spectral efficiency. DLR carried out verification and assessment flight trials in 2012 and 2018 with four ground stations. The results of both tests showed that LDACS has the potential to meet the accuracy requirement of RNP 0.3.

It is worth noting that LDACS is still at the verification stage. There are many aspects that are open to be answered, such as the coverage.

Mode N is a ground-based navigation service to provide a backup navigation solution by substituting DME with a system based on SSR/Mode S signals. All ground sites are synchronized in time via GNSS, RF time beacons and local high precision time network. Preliminary tests have shown an accuracy of 30 –50 m. Mode N is believed to have performance of 40 m (2σ). Mode N is still a concept that has not been widely used. So the maturity of this technology is relatively low.

It is recommended to consider where the systems should be implemented as the various features of individual systems can be advantageous under different operating conditions. When global coverage is considered, then LEO PNT has the advantage over other APNT solutions due to its global coverage. When application is mainly in remote and oceanic areas where the long-range characteristic plays the most important role, eLORAN has its relative advantage. When considering the feasibility, DME upgrade is recommended over LDACS and Mode N. As LDACS technology is being standardized and gradually introduced as an international standard to provide the digital communication service, its navigation function can be used as APNT worldwide. To operate all CNS systems in the L band, Mode N will be the most comprehensive solution when considering the APNT technologies. It is also recommended that in deciding which technology is the most suitable, factors like location of the APNT system, coverage requirements, unique advantages, drawbacks, performances, complexity and costs, etc., all should all be taken into consideration.

The analysis of alterative PNT solutions leads to the following conclusions: eLoran has better resilient to GNSS jamming and spoofing attacks as it is operating at low frequencies. LEO PNT is also good at spoofing mitigation as its timing and data is encrypted making it difficult to spoof. LEO PNT, eLoran and LDACS all have the highest accuracy of around 20 meters while Mode N and DME based systems have accuracy of 40 meters or lower. No candidate has the accuracy to the level of GNSS. DME based systems and eLoran have relatively better integrity. LEO PNT is expected to have good integrity as well for its encrypted timing and data as mentioned above. LEO PNT is satellite based and it has global coverage. Hybrid PNT expands the coverage of DME based APNT systems for its advantage of positioning based on two ground stations. LEO PNT requires launching and maintaining tens of or hundreds of satellites, therefore it is the most complex and expensive APNT system, followed by hybrid PNT which requires multiple DMEs and expensive scanning DME. eLoran and LEO PNT have already been used, therefore both technologies are more mature than other technologies which are still in either concept or verification stage, although some of them have high feasibility, for example, DME update.

Next tables summarize the A-PNT techniques properties (or performances), effectiveness and impact on aviation. The assessment scale is from 1 to 5 which means low to high.

Table 4-14 A-PNT solutions properties (or performance) and effectiveness matrix

	Accuracy	Integrity	Coverage	Jamming mitigation effectiveness	Spoofing mitigation effectiveness
Passive Ranging	3	4	2	4	4
Hybrid PNT	3	4	3	4	4
eDME	3	4	2	4	4
eLoran	4	3	3	5	5
LEO	4	3	4	3	5
LDACS	4	2	2	4	4
Mode N	3	2	2	4	4

Table 4-15 A-PNT techniques impact on aviation

	Complexity	Maturity	Impact on aircraft	Cost of implementation
Passive Ranging	2	2	2	2
Hybrid PNT	3	2	2	3
eDME	2	1	2	2
eLoran	2	3	4	3
LEO	5	3	3	5
LDACS	3	2	3	3
Mode N	2	2	2	2

4.3.6. OTHER SUPPORTING TECHNOLOGIES

To support the timely and effective sharing of information between stakeholders to support the detection and reporting of GNSS RFI events to ATC, and the assessment by ATC of the operational impact of those events, a brand-new API mechanism is proposed, which will allow the automatic exchange and storage of information between the difference operational devices and systems of those stakeholders.

Though API stands for Application Programming Interface, the API concept we propose consists of:

- An API web server hosted in a certain infrastructure that offers data services to two broad types of external roles, those that send data to the web server, and those that get data from the web server. To support these roles the web server needs to have an internal database in which the data received is stored and made it available for retrieval.
- The API itself, which consists in the definition of the data services offered by the web server, and that allows any external application hosted in a stakeholder device or system to make use of those data services to exchange data with the web server (and hence, to share information with other stakeholders that exchange data with the same web server)

Next figure shows the envisaged high-level architecture of how to implement the proposed API concept to support the operational concept and multiple stakeholders identified before.

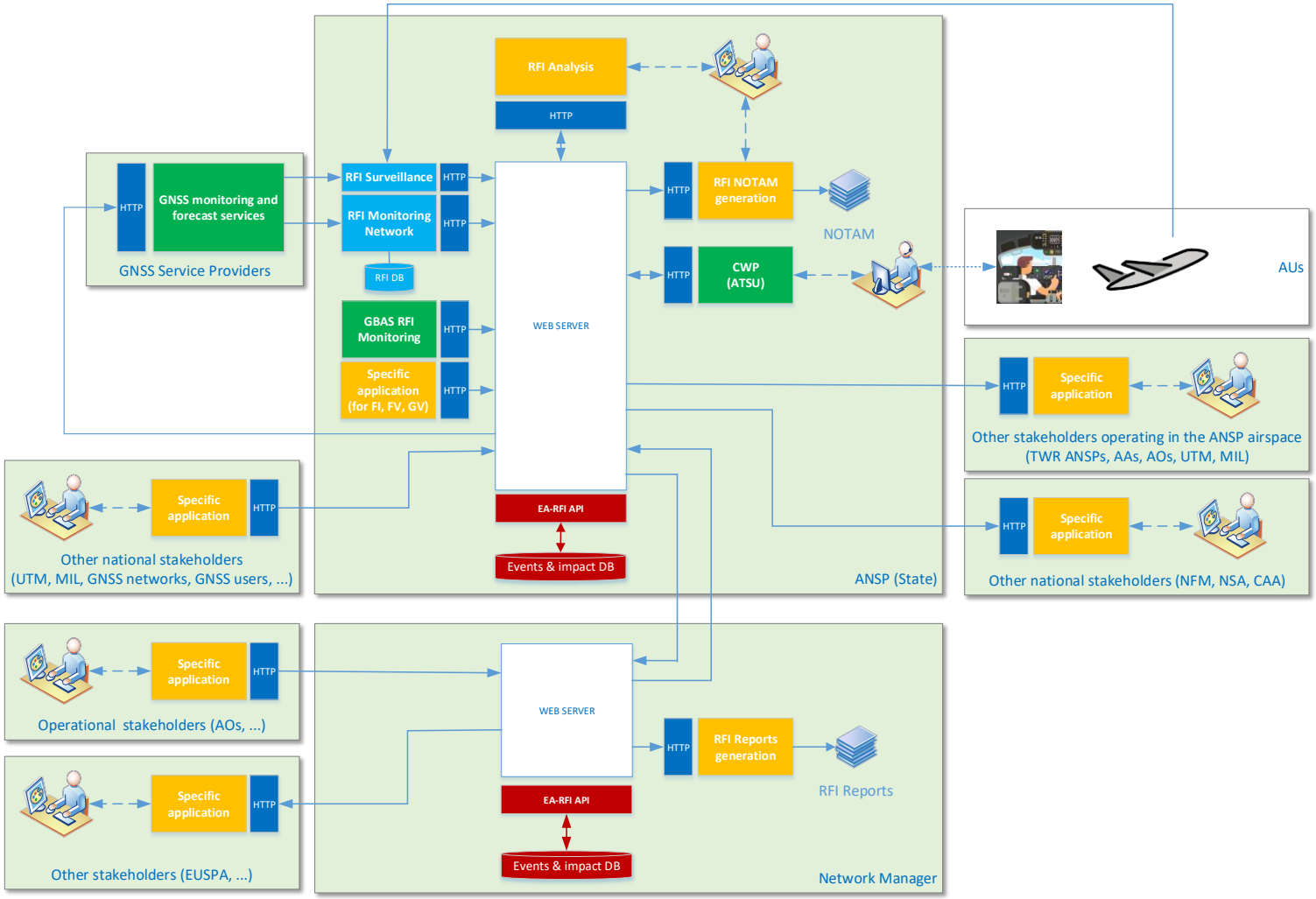


Figure 4-4 GNSS RFI notification and storage overview

Some remarks that are worth highlighting are:

- We propose to deploy one API web server at each ANSP, and another one at the NM.

  Notice that any API web server could connect (and exchange information) with any other.

- The arrows shown in the diagram represent whether the different stakeholders are assumed to be able to provide data to and/or retrieve data from a specific ANSP API web server.

- Except for the "RFI analyst" role (see below) and for the Military (for planned RFI exercises), data provision consists of RFI *events*, whereas data retrieval consists of the *airspace impact* due to the RFI that caused those events

  - An *event* would consist in the detection of a problem at three different levels: a) at the signal level (i.e. a jamming and/or a spoofing signal has been detected); b) at the level of the GNSS performances of a specific GNSS receiver working in a certain navigation mode (i.e. either the degradation of the GNSS performances, wrt the expected nominal performances, or the total loss of the GNSS navigation has been detected); and c) at the level of the types of operations that a specific GNSS receiver (which can work in different navigation modes) is able to support.

    Notice that, depending on the source of the event detection, the nature of that event could be different: for instance, an event detected by the aircraft crew (and reported to ATC) may be at the level of GNSS performances (e.g. GPS UNAVAILABLE) or at the level of supported operations (e.g. LPV UNAVAILABLE). On the other hand, an event detected by a ground monitoring station would be, at least, at the signal level (e.g. L1 jamming)

    Furthermore, the events correspond always to problems detected in the past, either at the fixed position of a ground monitoring station (over a certain time period) or along the flight path flown by an aircraft (i.e. at different aircraft positions along a time period).

  - The *airspace impact* would consist in the definition of an airspace volume that has been, or is expected to be, affected by a detected (or planned) RFI over a given time period.

    Note that there are three ways to define the airspace impact: a) to gather together multiple events (detected on-board and on ground); b) to localize the position of the RFI source and estimate some of its key features (e.g. its *effective* power, which could be function of its EIRP and, at least for jamming signals, of its waveform); and c) to know in advance the position of the RFI source and its features (e.g. for a military exercise).

    It is noteworthy that in cases b) and c) the location (and key features) of the RFI source would be known (together with the airspace impact), but not in case a).

    Furthermore, as in the case of the events, the airspace impact could be assessed at three levels: a) at the level of the signals (e.g. by determining the JSR or SSR of the different GNSS signals at different positions, and time, within the airspace); b) at the level of the GNSS performances of a specific GNSS receiver working in a certain navigation mode (e.g. by defining JSR and/or SSR thresholds that, if exceeded, are expected to either degrade the GNSS performances or cause the total loss of GNSS navigation); and c) at the level of the supported operations by a specific GNSS receiver

  Next figure illustrates the relationship between the described concepts

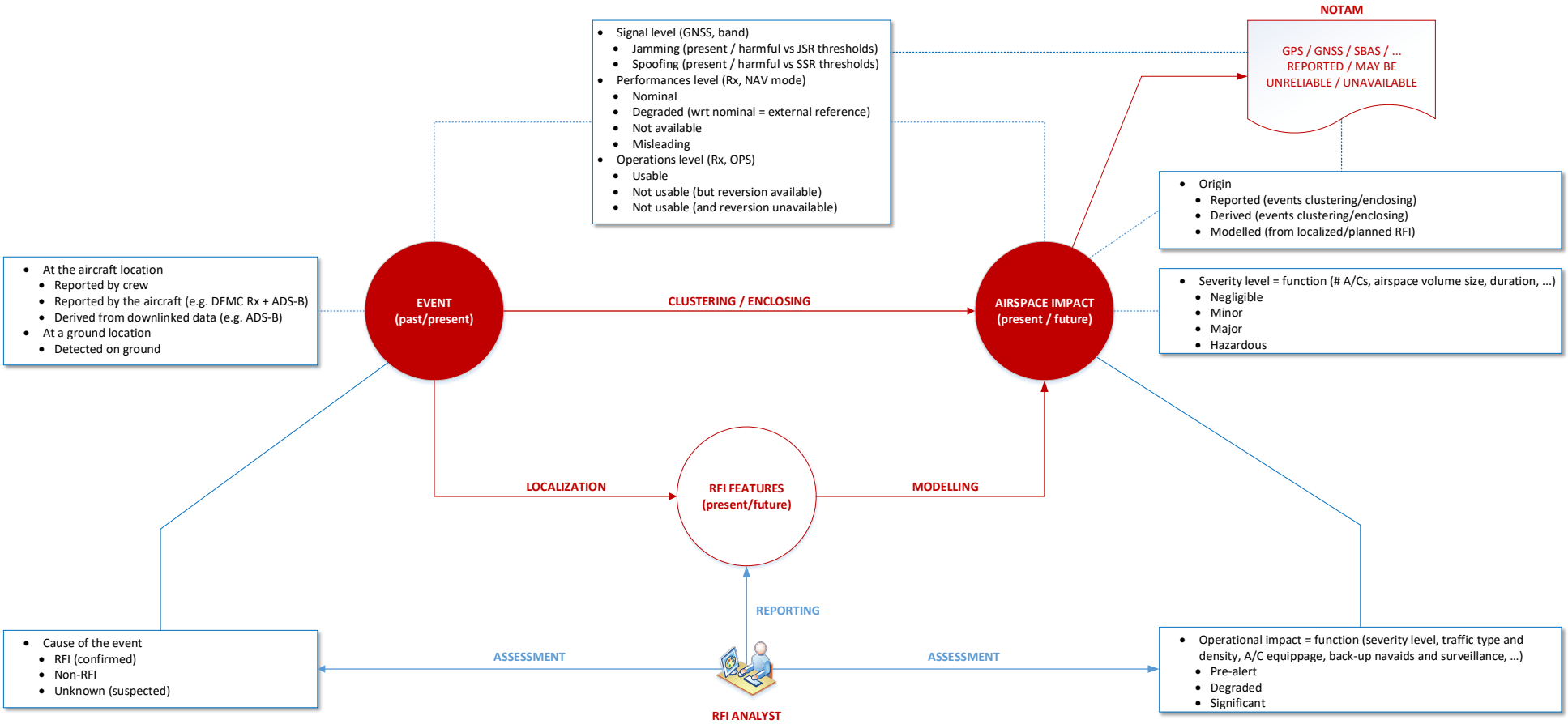


Figure 4-5 Relationships between RFI events and Airspace impact

- The stakeholders that are expected to exchange data with an ANSP's API web server are:
  - To report RFI events
    - ATCOs: when an aircraft crew reports (e.g. through RTF or CPDLC) a GNSS navigation issue (e.g. GPS PRIMARY LOST, UNABLE RNP) the ATCO should be able to report it to the ANSP API web server through its CWP (which should be adapted to make use of the API to send that report).
    - RFI surveillance system: when an aircraft is able to detect a RFI and/or a GNSS navigation issue and download the associated data to ground (e.g. through ADS-B), the surveillance system that collects the downlinked data could send the corresponding RFI events to the ANSP API web server.

      Alternatively, if the aircraft is not able to detect autonomously a RFI and/or a GNSS navigation issue, the surveillance system could still be able to process the downlinked GNSS-related data (e.g. quality indicators) to infer RFI events, which could be sent to the ANSP API web server.
    - RFI monitoring networks: the detected RFI and/or GNSS navigation issues should be sent automatically to the ANSP API web server.
    - GBAS RFI monitoring: the RFI monitoring subsystem of a GBAS station should send the detected RFI or GNSS navigation issues to the ANSP API web server.
    - Other technical staff: the ANSP staff involved in flight inspection, flight validation and ground validation may report any detected RFIs and/or GNSS navigation issues through a dedicated mobile or website application (both to be developed), which would send them to the ANSP API web server
    - Other national stakeholders, such as the Military, UTM service providers (e.g. CIS, USPs), other GNSS monitoring networks, or even any GNSS user (e.g. through a web page), may report RFIs and/or GNSS navigation issues, as long as they use the API to send their data to the ANSP API web server.

    It is noteworthy that the definition of the different types of events (and the criteria to trigger them) should be standardized to allow their assessment and comparison (as well as to prevent false RFI events detection)
  - To report the airspace impact
    - RFI surveillance system: if this system is able not only to detect RFI events but also localize the position of the RFI source and other features (e.g. emission power), then it should be able to compute and share the airspace impact
    - RFI monitoring networks: if a network of monitoring stations is able not only to detect RFI events but also localize the position of the RFI source and other features (e.g. emission power), then it should be able to compute and share the airspace impact
    - Military: if they plan an exercise that involves the emission of jamming and/or spoofing signals, they should be able to assess the operational impact of those emissions, and send that information to the ANSP API web server well in advance, to let the ANSP warn the airspace users (e.g. through a NOTAM)
    - Other ANSPs: an ANSP that identifies that an airspace impact affects the airspace of other State, should share it with the affected ANSPs.
    - Network Manager: it should send to ANSPs the airspace impact determined with its own technical means and sources of information.
  - To retrieve the airspace impact
    - ATCOs: they should be able to retrieve from their CWP, and as soon as available, the airspace impact caused by an RFI. Combining the information on the airspace impact with the coverage of the conventional navaids and surveillance

services within the affected airspace volume, as well as with the equipage of each aircraft within that airspace, would allow the identification of the aircraft that may need operational assistance (e.g. radar vectoring).

        - RFI NOTAM generator: the tool in charge of generating the RFI NOTAMs could get the required information (e.g. date/time, position, affected service, type of impact) from the ANSP API web server
        - Other operational stakeholders in the same State of the ANSP, such as other local (tower) ANSPs, AAs, AOs, the Military and UTM service providers, could get access also to the airspace impact caused by the detected RFIs
        - Other national stakeholders, such as the NFM, NSA, CAA could get access to the airspace impact caused by the detected RFIs
        - The Network manager, should know the airspace impact caused by the detected RFIs whenever the affected airspace covers more than one State and/or could have a network effect (e.g. international routes, high density TMA and airports)

- The stakeholders that are expected to exchange data with the NM API web server are:
    - To report events
        - ANSPs: they may send detected events of importance to the NM, to allow the NM to generate statistical reports at ECAC level
        - Aircraft Operators: the information on RFI and/or GNSS navigation issues (e.g. outages) that today the NM receives through the EVAIR system could be channeled through the NM API web server. However, this information could be redundant with the information collected by the different ANSPs
    - To retrieve events
        - RFI Reports generation: the tool in charge of generating reports with events statistics should read the required data from the NM API web server
    - To report the operational impact
        - ANSPs: they should send to the NM API web server the airspace impact caused by a RFI when relevant for the NM
    - To retrieve the operational impact
        - Other stakeholders (e.g. EUSPA) may be interested in retrieving the airspace impact caused by a RFI (e.g. to inform E-GNSS service providers)
- A specific role "RFI analyst" is proposed (at each ANSP) with the aim of collecting all the detected RFI events as well as any planned or expected airspace impact, and the known or localized position (and key features) of the RFI sources affecting, or that may affect, the airspace of an State. Moreover, this "RFI analyst" should be in charge of cross-checking the collected information in order to keep a consolidated view of the overall situation, which may imply:
    - The classification of events as RFI or non-RFI (if previously unknown)
    - The closure of open events (i.e. if their status remain active)
    - The definition of the baseline airspace impact, either by generating an airspace impact only on the basis of the collected events, the confirmation (or update) of the airspace impact reported by an external source (e.g. a surveillance-based system, a RFI monitoring network, or the military for a planned exercise), or a combination of the two.

      This baseline airspace impact should also define whether the information is relevant to the ANSPs of other States (e.g. to address cross-border scenarios), or to the Network Manager (e.g. when international routes or high-density airports or TMAs are affected).
- The GNSS Service Providers (or other stakeholders' services, such as Eurocontrol AUGUR API) may provide information about the current (or forecast) status (e.g. outages) and performances

of their services (or the services they monitor/forecast) to those stakeholders that need to know the expected nominal GNSS performances (to allow them to identify their degradation).

In turn, these stakeholders (in particular the E-GNSS Service Providers) may get from the ANSP API web servers the location and features of the detected RFI sources, which would allow them to determine the expected (current and forecast) GNSS performances subject to those RFIs.

4.4. DEFINITION OF THE OPERATIONAL CONCEPT

The main use case of the Operational Concept (see [REP11]) described hereunder is focused on the ANSP perspective providing ATS, because it plays an integrator role in the aviation scene. The use case considers that the detection of the GNSS RFI is already done by an on-board receiver, ground based RFI detector, human action, or any other available method. The high-level use case is shown below:

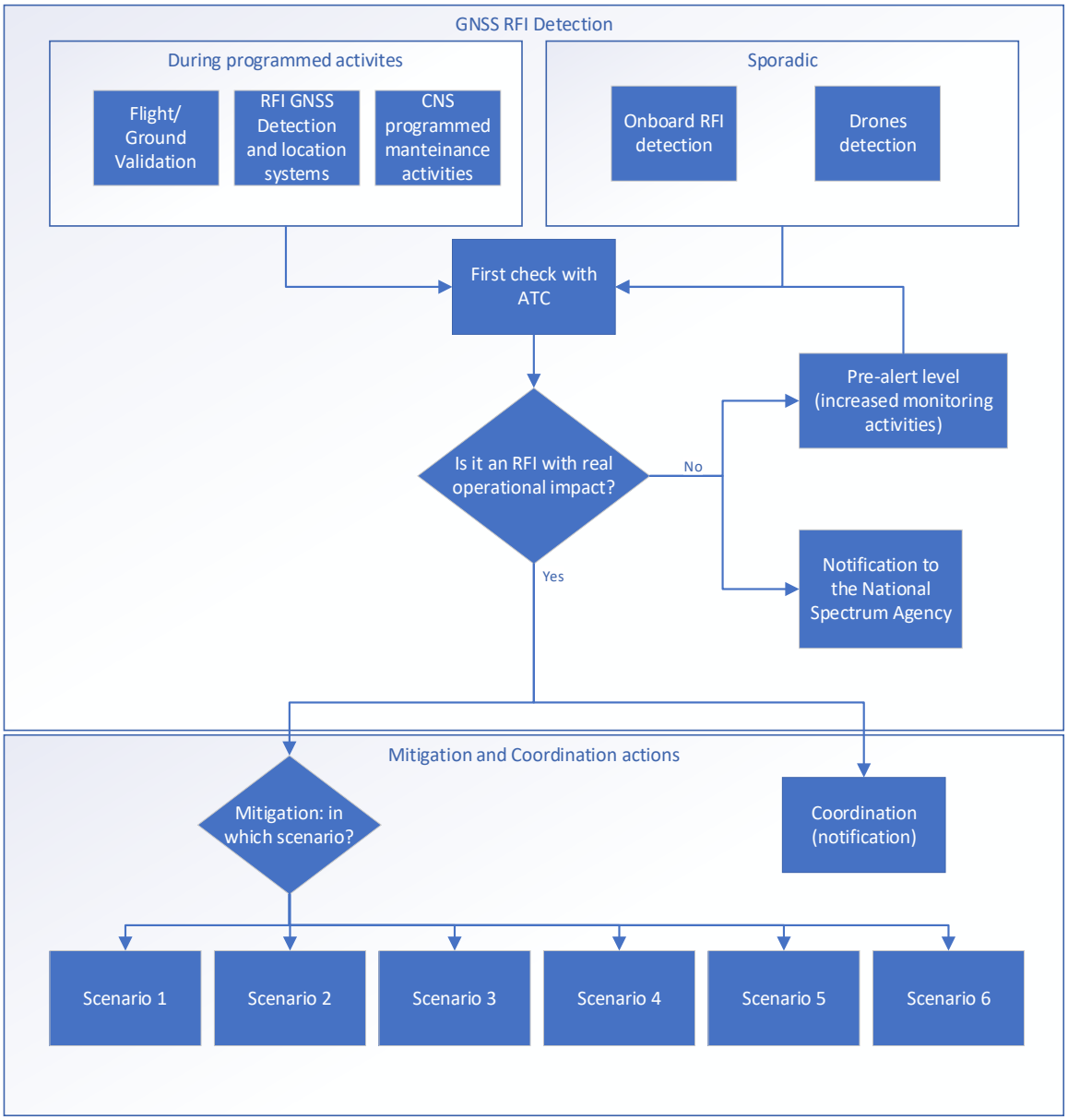


Figure 4-6 High level GNSS RFI use case

GNSS RFI detection activities

The detection of the GNSS interference is considered as the kick-off of the use case. Two means of RFI detections have been identified. The first one is when the RFI is detected by systems or activities particularly designed to detect interference in the GNSS signal.

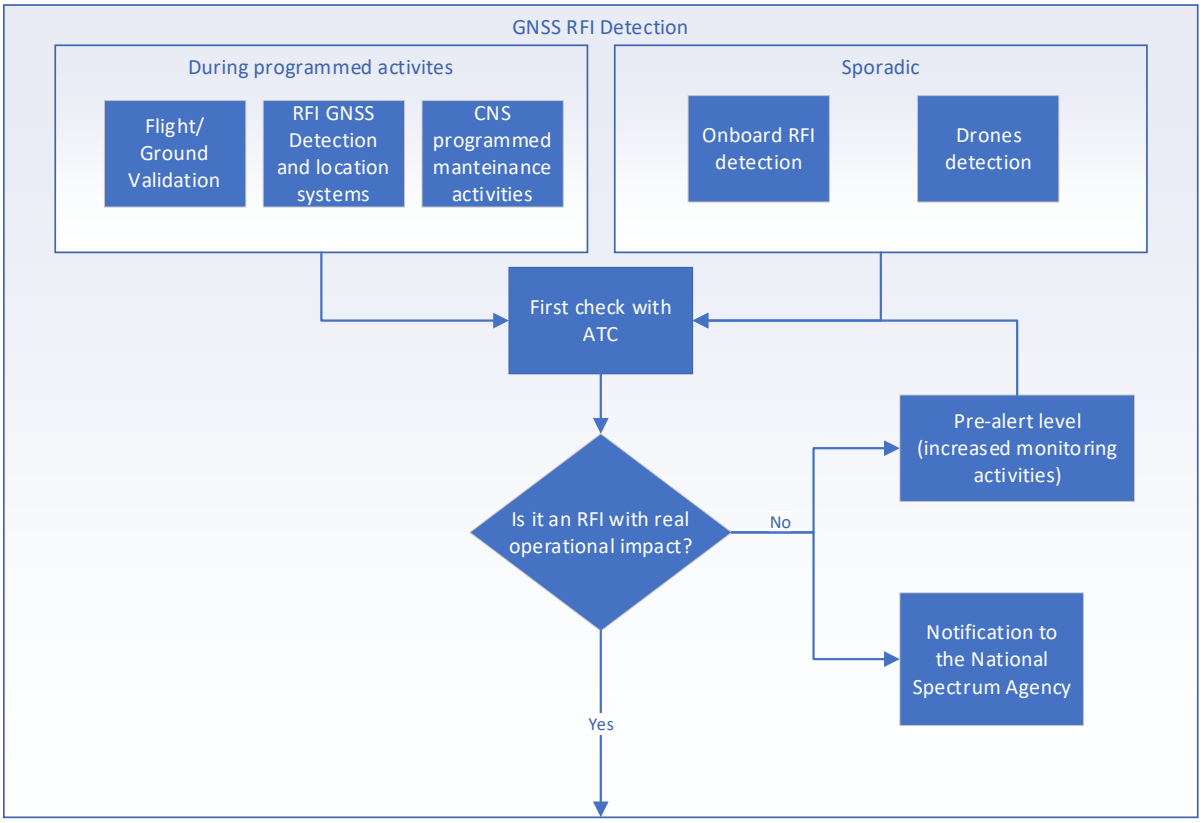


Figure 4-7 GNSS RFI detection activities

Inside this RFI detection category the detection could come from the validation and verification activities. These activities include the validation flights to implement TMA manoeuvres, the verification flights made to check the quality of the CNS system signals and the validation activities made on ground before the implementation of any procedure.

In this same category are the RFI monitoring systems deployed mainly but not only around the airports to detect and localize the GNSS interferences, as well as the surveillance-based detection and localization systems (e.g. by processing the ADS-B data downlinked by aircraft).

The last method identified to detect the interferences within this category is during the programmed maintenance activities of the CNS equipment, mainly those that use the GNSS signal (e.g. GBAS systems).

The second RFI detection means is when the RFI is detected during the normal operation of the aviation system. In this category two different sources are found.

- The most common way is through the air crew. When the onboard GNSS equipment fails or generate an alert the aircrew notify this outage to the ATC, warning the rest of the airspace users nearby.
- The second source is related to the operation of unmanned aircraft systems (UAS) through the UAS traffic management system within the U-space. Within the U-space the UTM service provider could notify the RFI event to the National Spectrum Agency and to the impacted ANSP. Out of the U-space, the UAS operator would notify the RFI event to the National Spectrum Agency; it is

recommended that, if required, a communication procedure be developed between the UAS operator and the National Spectrum Agency to this end.

Once the GNSS interference has been detected, a cross check between the different actors is needed to make sure that this interference has a real impact on air navigation operations. If the detection has been made during programmed activities the next step should be the coordination with the ATC operators to verify if the aircraft have experienced the same interference onboard. If the answer is affirmative there is, with high probability, an interference event with impact in aviation. If not, a thorough monitorization of the RF environment should be made.

On the other hand, if the RFI has been detected onboard one aircraft, the pilot should notify to ATC to start the contingency procedures. ATC should check if other airspace users are experiencing the same GNSS outage. Also, if there is any GNSS interference monitoring ground station near the aircraft notification spot, ATC should check with its operators to verify it.

It should be pointed out that if the detection is made by different airspace users but not by the detection systems deployed on ground the event should be considered as a real interference and all the mitigation procedures should start. The other way around doesn't imply the same. If the GNSS RFI detection system is detecting an interference event but there is no impact on the airspace users[1], the mitigation procedures shouldn't be activated. However, a thorough monitorization of the RF environment should be made in this case too (pre-alert level).

The ANSP and the Airspace users should start the mitigation actions and the contingency plans to keep up the safety, efficiency, and capacity levels of the aviation ATM system. To do so, it is necessary to evaluate the effect of the RFI on the aircraft as a system and in particular on those elements that use the GNSS signal: Navigation, Communication and Surveillance as well as other onboard systems. Once the effect is evaluated, the impact shall be assessed to put the mitigation actions in place. However, these two evaluations, the effects, and the impacts, are linked to the scenario on which the RFI is taking place. It is not the same having a GNSS RFI in a crowded TMA over a huge airport than having the same interference in a low-density area.

[1] Reasons might be e.g. low power interference broadcast near the detection and far away from the airspace users, directional antenna when using counter UAS systems or interference sources close to high buildings or high mountains affecting the GNSS RFI detectors but the aircraft flying nearby.

Coordination (notification) activities

Independently of the scenario, notification activities should start once the GNSS RFI event has been confirmed. The notification should be made to all the aviation stakeholders in order to minimize its impact. The time period between the interference is detected and its notification will be different depending on the criticality of the impact on the stakeholder concerned.

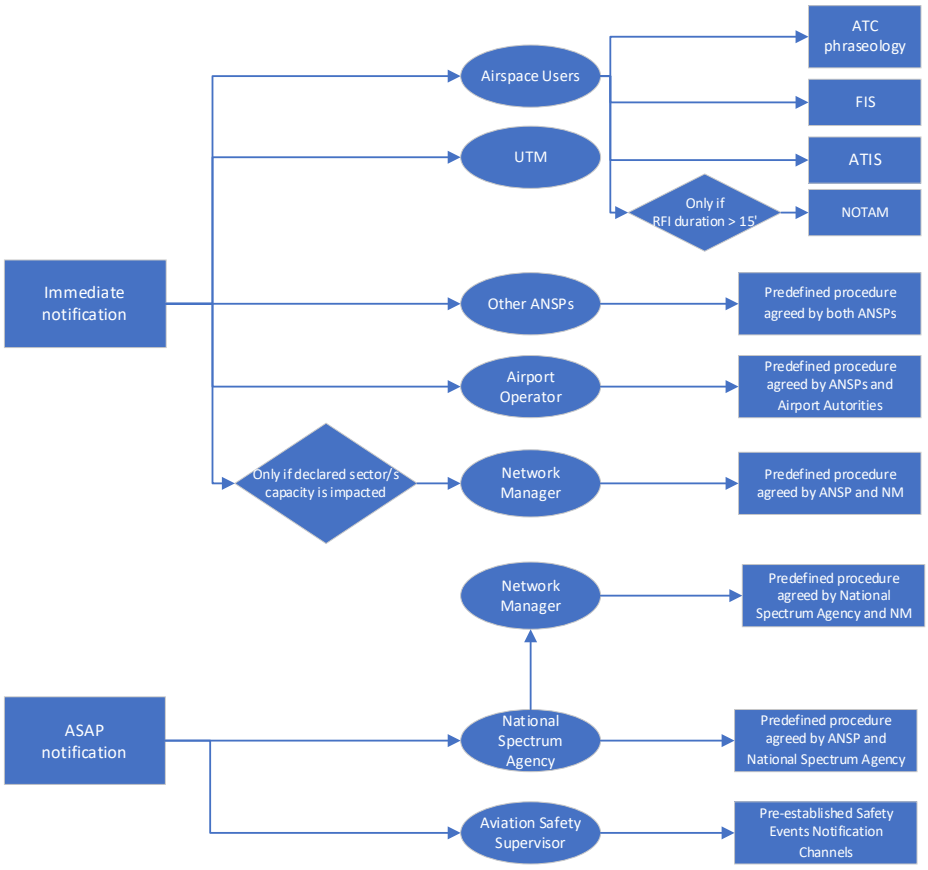


Figure 4-8 Coordination (notification) activities

In this sense, the notification process has been split up in two categories: immediate and as soon as possible notifications.

In case of an interference affecting the GNSS signal the most critical stakeholder in aviation is the airspace users, so the communication to them should be immediate. The methods used to inform the aircraft flying in any phase of a flight are through air/ground communications service using a previously defined and harmonized phraseology (where ATC service is provided), through flight information service (where AFIS is provided) and through ATIS service (where available). If the RFI event is active for fifteen minutes or more its mandatory the emission of a NOTAM within another 15 minutes to warn the airspace users in flight and when defining their flight plans.

Also, it is needed to inform the UTM service providers to notify the GNSS outage to the drones flying in a specific airspace, especially for those flying BVLOS. When the UTM system is configured one of the important aspects should be the coordination protocols with the ANSPs that share the airspace. One of these protocols should be specific for the notification process when a GNSS outage occurs.

Other important actor in the aviation system is the airport operator because under a GNSS outage near the airport the mitigation procedures could affect the capacity of the airport and the contingency

procedures on ground could be necessary. This situation could derive on flight delays and all the associated effects on the aircraft operators. A predefined procedures agreed between the ANSP and the airport operators to notify the degradation of the GNSS signal is necessary to guaranty the correct transmission of the information.

When the GNSS RFI could have impact on the ATS and/or CNS services provided by close ANSPs, they should be notified immediately. This applies either if the ANSP is from a neighbour country affected by a cross border interference or if it is a service provider from the same country (e.g. if the tower ANSP is different from the TMA ANSP). In that case the coordination between close ANSPs is necessary in order to mitigate the RFI impacts tactically (for example between ATCOs). Different types of notification should be used depending on the complexity of the operations (e.g. directly through ATCOs or through the notification office). The involved stakeholder should agree beforehand the suitable options.

Another stakeholder identified to be kept informed under a GNSS outage is the Network Manager (NM). It needs the information immediately if the RFI event causes a capacity reduction in any sector, since it will then need to introduce ATFM measures. For instance, if the RFI affects a high density TMA or airport, the delays could impact the international traffic and in consequence demanding a reactive reschedule of the flight slots. .

Otherwise, immediate notification to the NM wouldn't be necessary, but in any case, it should be done as soon as possible to keep track of the GNSS RFI events in Europe and be prepared in case the range of the impact suddenly increases, delaying or affecting international traffic.

The National Spectrum Agency should be notified of the RFI event as soon as possible if the interference has been detected by any mean. A predefined agreement that includes the information needed by the National Spectrum Agency to look for the interference should be done.

Finally, if the GNSS events have an impact on the safety of the air operations the ANSP should notify the NSA or the authorized safety supervisor through the pre-established safety events notification channels that are used to report every safety issue. Also, a category dedicated to report the GNSS RFI events should be created to collect this type of safety events unequivocally.

4.5. SECURITY RISK ASSESSMENT UPDATE

The **initial risk assessment is updated** based on the results of the assessment (in particular out of the laboratory tests) carried out in the project of the on-board and ground technologies recommended for implementation.

One of the results obtained from laboratory tests of the recommended techniques that could be implemented in the on-board GNSS receiver to mitigate jamming threats [REP14] is that the resilience of the receiver could be increased significantly (the minimum jamming to signal ratio – JSR - to cause an unusable event can be increased by as much as 20 dB). This increase in resilience would result in a significant reduction in the amount of airspace affected by a given RFI, which has been assessed as equivalent to a reduction in the likelihood of a "GNSS Unusable" event occurring by a factor of 10^3.

This reduction factor has been computed assuming that the airspace affected by RFI can be modeled by a ground-centered semi-sphere, that the radius of such semi-sphere is proportional to the inverse of the square root of the minimum JSR causing a "GNSS Unusable" event (applying a free space RFI path loss model), and that the likelihood of such an event (expressed as number of aircraft affected) is proportional to the volume of such a semi-sphere (which is proportional to the third power of its radius).

The results obtained from laboratory tests of different techniques that could be implemented in the on-board GNSS receiver to detect jamming threats and, specially, of different techniques that could be implemented on ground-based systems to detect and locate the position of the jamming source (e.g., ADS-B based RFI detection and location systems) proved to be effective. Then, assuming that the location of a jamming source could be obtained, and the affected airspace identified, the risk exposure of aircraft flying into that airspace could be avoided, which has been assessed as equivalent to a further reduction in the likelihood of an unusable event occurring by a factor of 1.5.

This factor has been calculated assuming an average flight duration of 90 min and a reference RFI duration of 45 min (an upper limit of the GPS outages reported in Eurocontrol's EVAIR bulletins [EVAIR]),

implying that half of the aircraft flying into the affected airspace while the RFI is active would be affected, unless the RFI is detected, those aircraft are warned, and then their exposure to the risk is avoided.

Combining the two types of safeguards (prevention and detection) the likelihood of a "GNSS Unusable" event caused by a jamming threat has been assessed to change from occasional to remote (from 4 to 3 in the likelihood score within the risk matrix above).

With regards to the laboratory tests that dealt with different types of spoofing attacks (S1, S3, S5 and S6), some conclusions have been drawn:

- In many cases (specially with untargeted spoofing attacks), the effect of the spoofing RFI on the on-board GNSS receiver resembles the effect of a jamming RFI, so when the receiver is subjected to a spoofing RFI it is more likely than expected to cause a "GNSS Unusable" event than a "GNSS Misleading" event. This is evaluated as equivalent to a reduction of the initially estimated likelihood of a "GNSS Misleading" event caused by spoofing by a factor of 2.
- In many cases, the Spoofing to Signal Ratio (SSR) of the spoofing RFI required to deceive the on-board GNSS receiver (i.e. to make the receiver track a spoofed SV signal) is high (about 15 dB, according to the laboratory tests performed), while the tested detection techniques that could be implemented in the on-board GNSS receiver were found to be effective when the SSR is much lower (above 5 dB, according to the laboratory tests performed). This difference between the measured minimum SSR for threat detection and for receiver deception seems to be a strong barrier against the occurrence of a "GNSS Misleading" event as long as those detection techniques are implemented.
- Furthermore, combining some of the proven detection techniques could make that barrier much stronger as it would virtually remove the existence of a minimum SSR to cause a "GNSS Misleading" event in an on-board GNSS receiver. This could be reached by combining OSNMA to detect the presence of a spoofing RFI affecting Galileo signals, followed by a consistency check at navigation level to detect the presence of a spoofing RFI affecting GPS signals (e.g. by comparing the PVT obtained by processing only Galileo or GPS signals).

The combined effect of these results is that the implementation of the proven detection techniques to address spoofing threats would equate to a reduction in the likelihood of a "GNSS Misleading" event caused by a spoofing threat from remote to improbable (from 3 to 2 in the likelihood score within the risk matrix above)

Once the effectiveness of the new safeguards (in terms of reducing the likelihood of an RFI security event) have been determined, those effectiveness values can be taken into account in reassessing the adverse scenarios to determine the residual risks levels that would result from the implementation of those safeguards, as shown in the table below:

		GNSS Unusable							GNSS Misleading						
Scenario	**Flight phase**	**1**	**2A**	**2B**	**3**	**4**	**6**	**5**	**1**	**2A**	**2B**	**3**	**4**	**6**	**5**
Manned	**Departure**	L	L	H			M		M	M	H			L	
	En-route				L	L						M	H		
	Arrival	L	L	H			M		L	L	H			L	
	Approach	L	L	H			M		M	M	H			L	
Unmanned	**BVLOS**							M							M

Looking at this table, it can be seen that the implementation of the proposed on-board and ground RFI detection, location and mitigation techniques would reduce the residual risk to low/medium except in two scenarios:

- Scenario 2B: Low density TMA/CTR serving one or multiple smaller regional airports, including both IFR and VFR traffic and RNAV 1 SID and STAR procedures (2030 timeframe).
- Scenario 4: Medium to high density en-route oceanic, remote continental and continental airspace with no DME-DME / VOR-DME coverage.

These two scenarios share the key feature (by design) that there are no ground navaids (e.g. DME, VOR) nor surveillance systems (e.g. PSR, SSR) to support aircraft operations if GNSS is lost.

In addition, an examination of the reasons for high operational risk despite having significantly reduced the likelihood of RFI security events shows that the impact on the efficiency and capacity KPAs was assessed as either hazardous (4) or catastrophic (5) considering the impact in the risk matrix above.

Therefore, in order to further reduce the operational risk in such scenarios, it seems unavoidable to implement new safeguards other than the technical safeguards described in the previous section. Indeed, one of the main conclusions of the Concept of Operations [REP11] for managing RFIs in Aviation proposed in the project was precisely the implementation of a number of consequences minimization safeguards (operational mitigations), namely:

- Nominal operations should not be based solely on GNSS (i.e. RNAV rather than RNP flight instrument procedures should be published).
- Surveillance and Communications should not only use GNSS as time reference,
- A-PNT should be in place to support operations in case of GNSS outage.

The objective of these operational safeguards should be to reduce the severity of the impact on safety, efficiency and capacity KPAs to major (3) or lower impact within the risk matrix above, so that the resulting residual risk turns out medium or low.

4.6. TECHNOLOGIES IMPLEMENTATION TIMELINE

4.6.1.ON-BOARD DETECTION AND MITIGATION TECHNOLOGIES

This section proposes a timeline for the implementation of RFI detection and mitigation technologies in the on-board GNSS receiver. The timeline not only considers the on-board techniques tested in AIRING (highlighted in red in Table 4-3) but also the on-board techniques analyzed in [REP03] and [REP05].

To define the implementation timeline for the recommended technologies we need to apply the general constraints related to GNSS aviation receivers (see Table 4-16 below) to each individual recommended on-board technologies in order to assess the impact that the implementation of that technology would have on all the affected stakeholders.

Table 4-16 Aviation Constraints

Aviation Constraints	Description
Operational environment	Although the operational environment is less complex than, for example, urban environments with dynamic multipath conditions and severe signal masking, there are still several challenges which can affect selection and performance of the RFI detection and mitigation techniques: ▪ Carrier to noise (C/N0) values ranging from 30 to 50 dB-Hz. The lower bound might decrease with the finalization of DFMC MOPS, as it is desired to remain operational at a presence of stronger interference. ▪ Unintentional interference from other systems in the same or surrounding RF bands (e.g. DME, TACAN, JTIDS/MIDS and others). ▪ Aircraft maneuvers (e.g. banking) can lead to a rapid change of C/N0 as well as signal masking ▪ Multipath caused by reflections from the aircraft itself and from surrounding objects. Multipath creates a second version of the GNSS signal. ▪ Ionospheric scintillations result in rapid change of C/N0. Moreover, in the upcoming DFMC MOPS it is intended to stringent the recovery requirements, what might make the spoofing attack difficult to detect. ▪ RTCA's DO-160 defines the temperature operation range to be -55° to 70° Celsius, with relatively rapid variations. This might impact some of the spoofing detection methods based on AGC and receiver clock monitoring which both show significant temperature dependency.

Aviation Constraints	Description
Aviation standards	The safety, interoperability and minimum performance of the systems and services onboard aircrafts is guaranteed by variety of standards published by organizations like ICAO, RTCA or EUROCAE. These standards often mandate certain performance requirements or even use of certain algorithms which may limit adoption of some of the techniques for spoofing detection/mitigation otherwise generally recognized as feasible. Examples of such requirements: the early-late DLL discriminators, specific correlator spacing and RF bandwidth ranges, maximum time to first fix. Furthermore, requirements on availability, continuity and integrity of the service directly impact the false alarm and missed detection probability requirements which need to be met by any potential anti spoofing algorithm.
IPR	Severe restrictions are imposed on inclusion of techniques covered by IPRs in avionics standards and these techniques are unlikely to be broadly adopted by more manufacturers.
Certification	The GNSS receiver SW is usually certified as DO-178C/ED-12C Design Assurance Level B or A and therefore any added complexity in the SW induces significant cost increase for development, testing and certification of such a software. The usage of complex algorithms must be therefore properly justified with their performance. The same applies to HW including algorithms implemented in FPGA which is certified according to RTCA DO-254 / EUROCAE ED-80.
Limited retrofitting	Airplanes are a very complex ecosystems with many interoperating devices so it may be problematic to introduce new systems which would significantly affect other systems already in place. Moreover, the aircrafts are usually in service for decades so introducing new systems usually leads to retrofitting and grounding the airplane for longer period which induce significant costs. The best way forward, at least in short-term horizon, would be to limit retrofitting and reuse already existing aircraft systems, antennas, RF cables and data buses as much as possible.
Export restrictions	Limitation connected with export control of certain technologies and devices, which would limit their adoption in civil aviation. This may include for instance usage of CRPA antennas, ADCs with too good resolution and sampling frequency or FPGAs with too many IO pins
Limited HW resources and cost	There are certain HW limitations which may affect feasibility of selected algorithms. Airborne GNSS receivers are embedded devices running with real-time constraints, limited computational power, memory, weight, size and power consumption. This may rule out algorithms which are computationally demanding, have big memory requirements or depend on addition of bulky HW components.

Note that the *impact* term is understood as the extent of the changes required for the implementation of a particular technology by the different stakeholders (e.g. changes to the aircraft, avionics retrofit, upgrade of the type certificate, etc.). On the other hand, it is worth clarifying that the impact categories (minor, medium, high) are relative to each other, i.e. "minor" only means that the impact is lower than "medium" or "high" (not that the impact is "minor" in absolute terms).

The resultant implementation impact for each of the recommended technologies is shown in next table

Table 4-17 Implementation impact of On-Board Technologies in Aviation

Layer	On-Board Family of Techniques / Technique	Feasibility in Aviation	Impl. Impact
Antenna	**Multi-element antenna technologies (CRPA)**	Airplane manufacturers are generally sensitive to requirements demanding changes of the antenna setup especially addition of antennas, change of the antenna form factor or less convenient aerodynamic profiles. Any change of setup, especially adding more antennas might be difficult to justify. Moreover, export control restrictions should be definitely avoided in the proposed solution, which, together with significantly increased cost and processing complexity, will make it very difficult to implement algorithms based on CRPA in the short and medium term. This means that from an aviation point of view, CRPA-based algorithms are a solution with a potentially high impact. Aircraft manufacturers and supplemental type certification holders are usually cautious about making changes to a certified antenna setup, in particular adding new antennas or changing their shape, because this could affect the aircraft aerodynamic profile and being expensive to implement. additionally they want to avoid export control restrictions, which could make it difficult to use certain algorithms based on the CRPA signal processing technique in the short and medium term. Re-certification costs will also be a major concern	High Impact
	Multi-element technologies – Using currently deployed dual antenna architecture (e.g. D3)	Currently deployed dual antenna architectures aim mainly on redundancy (two independent chains of antenna-RF cable-receiver), but it should be possible to reuse it for some of the presented DOA algorithms which could be useful for both detection and mitigation of the spoofing threats, or for simple spoofing detection techniques like dispersion of double differences (D3). To achieve this, it may possibly require including extension of current onboard data-communication standards (ARINC 429) or to aid the mitigation in the currently present receivers with the data from an independent RFI detection unit physically connected to both antennas. For DOA algorithms certain challenge may lie in the fact that the receiver's clocks are not synchronized and the antenna baseline vector changes with aircraft attitude, but that should be possible to solve using clock steering algorithms and aiding from inertial sensors. To not overcomplicate the GNSS receiver itself and the interface between them it might be beneficial to keep the receivers as simple sensors providing phase measurements and process the DOA based spoofing detection and identification algorithm in some higher-level system like GNSS-AHRS or FMS.	Medium Impact
	Single-element antenna technologies (Dual Polarization Antenna)	Dual polarization antennas might be difficult to adopt because of their non-standard interface, but it might be the only available choice in the antenna layer for single antenna aircrafts, since FRPA antennas masking the elevation with a physical element like choke-rings are too heavy and bulky for use in aviation. Additionally, the effectivity of the single antenna methods based on identification or blockage of signal coming from bellow the aircraft may be diminished by the fact that the spoofing signals may in some spoofing scenarios come also from above the aircraft (for instance airplane landing in a valley, airborne spoofer etc.)	Medium Impact
	Single-element antenna technologies (Synthetic Antenna Array)	Single antenna Synthetic Array could be employed for spoofing Detection if it can cope with the fact that the antenna movement trajectory is fixed to the aircraft motion and can be measured with inertial sensors. Synthetic antenna array for moving vehicles technology is complex and has not been deployed yet in commercial systems.	Medium Impact (Low maturity)

Layer	On-Board Family of Techniques / Technique	Feasibility in Aviation	Impl. Impact
Front-End (Pre-Correlation)	**AGC with Running Digital Sum (RDS)**	Relatively simple method deemed feasible for aiding detection of any form of non-nominal RFI is observation of the AGC state in time and detection of unexpected jumps which may sign presence of jammer or spoofer. Although this method can't work as sole mean of the detection, it requires relatively small complexity and broad availability of the AGC blocks in the present GNSS receivers.	Low Impact
	Spectral and statistical detection – Simple Methods (Statistical Detection)	Interference detection can also be performed by monitoring statistics of the ADC output (see [REP03] and [REP05], e.g. Kurtosis, Histogram analysis), which show good results for all interference types except for wideband (noise-like) interference. These techniques were employed in ANF&PB tests to trigger the mitigation (see section 5.3.1.2.1 in [REP14]).	Low Impact
	Digital filtering – Simple Methods (ANF&PB)	Simple digital filtering algorithms, like adaptive notch filtering (ANF) or pulse blanking (PB), can be both effective and feasible for implementation in the aviation GNSS receivers. As an example, pulse blanking is proven to be efficient against DME pulsed interference, which is nominally present in the L5 band and can cause problems to the aviation receivers in the so-called DME hotspots. The adaptive notch filtering may introduce additional group delay to the system. Care should be taken that the overall differential group delay for the receiver, antenna and installation doesn't exceed 150 ns as required in [MOPS] ED-259 ([DMS:052]). Care should be taken concerning potential interaction with AGC mechanism and detection/mitigation techniques based on the AGC, C/N0 and correlation function monitoring.	Low Impact
	Spectral and statistical detection + Digital filtering – Complex Methods	More complex digital filtering methods like RIM filtering or spectral and statistical detection might be too computationally demanding and have large negative impact on FPGA/ASIC footprint, power consumption, heat dissipation and costs. Proper justification would be needed to employ these algorithms in aviation receivers.	Medium Impact
Signal Processing (Correlation and Post-Correlation)	**SCA (Spreading Code Authentication)**	The spreading code authentication is considered as a very strong anti-spoofing technique, but it is not yet supported for civilian use by the GNSS constellations. Therefore, it cannot be evaluated for the usage in civil aviation for both short and mid-term. It can be a potential solution in the future, but several operational aspects of secure distribution of the cryptographic keys will need to be resolved before it can be accepted by the aviation industry.	Not yet supported for civilian use
	RSS (C/N0 Monitoring)	Some RSS monitoring techniques like C/N0 fluctuation monitoring are deemed feasible for implementation in aviation GNSS receivers mainly because their low complexity and cost. C/N0 can significantly fluctuate when the airplane is performing flight maneuvers like banking. Therefore, the C/N0 monitoring should be always used in combination with other detection techniques and possibly also aided by attitude obtained from INS. It is also deemed as beneficial and feasible to perform received power crosschecks on dual-frequency signals, since the number of dual-frequency receivers allocated in aircrafts is assumed to grow in short and mid-term horizon as soon as the dual-frequency receiver MOPS are published. Other listed techniques like Power Distortion Monitoring, Absolute Power Monitoring or Support Vector Machines may be too heavy for the aviation usage from both HW and operational perspective.	Low Impact

Layer	On-Board Family of Techniques / Technique	Feasibility in Aviation	Impl. Impact
	Correlation peak monitoring (CPM)	Generally, monitoring of the correlation peak shape and presence of more correlation peaks is considered as very powerful method for spoofing detection. Some compromises between performance on the one side and complexity and computational demands on the other side will need to be taken, since these techniques usually require more correlators in a channel, complex tracking loops, more channels tracking the same signal or a significant time to skim through the whole frequency/phase search space. It should be also noted that certain algorithms like the listed Rover Channel might be patented which will prevent its broad adoption among other manufacturers and in standards. The presence of multipath may falsely trigger the spoofing detection alert and thus affect availability and continuity of the navigation solution. The algorithm must be tuned in a way that the availability and continuity requirements are fulfilled. Some of currently deployed receivers may already use similar techniques (e.g. monitoring of tracked signals using additional tracking channels with dissimilar configuration), but they usually aim to increase integrity and robustness in general and are not primarily designed and tested against specific jamming and spoofing threats.	Medium Impact
Navigation	**Consistency check of measurements and PVT (e.g. CCH)**	The consistency checking of the pseudorange measurements, phase measurements and PVT results is considered as a good way to detect and mitigate certain types of the spoofing attacks with low complexity and additional costs. It should be also possible to reuse some algorithms already present in the receiver as RAIM checking consistency of the navigation solution or the step detector which checks unexpected jumps of the pseudorange measurements, or the satellite position based on navigation data. There are some extensions to RAIM techniques which can handle also more than one faulty/spoofed signal (e.g. algorithms applying solution separation method like ARAIM), but the care must be taken here to keep the computational load in the limits, because it rises quickly with additional number of used satellites.	Low-Medium Impact
	Multi-frequency multi-constellation (MFMC) diversity	Crosschecking the signals, measurements, navigation messages, receiver clock, and PVT results using more frequencies and constellations could be a feasible complementary means of spoofing/jamming detection and mitigation for the next generation dual-frequency multi-constellation aviation GNSS receivers. The complexity is relatively low, and it could be very efficient against simpler single-frequency jammers and spoofers. No major aviation specific constraints were identified, except the fact that the final version of the [MOPS] ED-259 is not yet released. Concerning the RFI mitigation using unaffected signals, attention should be paid also to the [MOPS] ED-259 requirements concerning the constellations, signals and NAV data content allowed to be used by a civil aviation receiver in different operation modes.	Low Impact
	Consistency checking with other navigation and positioning technologies	Big passenger airplanes are equipped with variety of dissimilar navigation sensors and systems. Although the final set of used systems differ based on the category of the aircraft and some of them are not available for all phases of flight or in all geographical locations, it is definitely recommended to do a crosschecking of the navigation results. Some hybrid architectures like GNSS, INS, magnetometer, altimeter are already deployed nowadays and can improve resilience against both jamming and spoofing.	Low Impact

Layer	On-Board Family of Techniques / Technique	Feasibility in Aviation	Impl. Impact
	NMA (e.g. Galileo OSNMA)	Cryptographic navigation message authentication (e.g. Galileo OSNMA) is an important technique to increase resilience against spoofing attacks targeted on forcing receiver to use counterfeit data. NMA techniques will be very likely required by the aviation receiver standards in the future, but so far, no standard is readily available. Besides the Galileo OSNMA there is also a NMA service using SBAS L5 signals in study. One of the implementation constraints overlapping also to the other aircraft systems is the cryptographic keys management where certain data may need to be obtained using other channels than GNSS signal in space, and securely stored.	Low Impact (when available)

At the end, to define the implementation timeline of these on-board technologies (i.e. to define the implementation strategy in the short-, medium- and long-term) we have taken into account the following aspects and made a trade-off between them:

- Maturity of the technology (see section §4.3.2)
- Implementation impact on Aviation (see Table 4-17 above)
- Complexity and cost of the on-board techniques (see section §4.3.2)
- Effectiveness of the on-board techniques (see §4.3.2)

It is important to note that, while impact of implementation could be also a proxy for the time required for the deployment of a particular technology (the larger the extent of the changes, the longer the deployment period) and for the deployment cost, the combination of the *maturity* and *complexity* terms could be an indication of the time and cost required for a particular technology to be ready for industrialization (TRL6) and/or deployment (TRL9). The *cost* term combines the cost of technology development and deployment

The **main trade-off criterion consists in trying to maximize as much as possible the effectiveness against RFI while introducing techniques with the lowest possible implementation impact, complexity and cost**.

When assessing the techniques by their effectiveness, it is important to take into account the differences between RFI detection and mitigation:

- When a jamming and/or spoofing RFI is not detected then there can be an impact on safety, especially with spoofing. Hence, RFI detection capabilities are especially important for safety.
- RFI can only be mitigated if it has been detected beforehand. Some mitigation techniques require to be triggered by other detection technique, while others carry out detection at the same time as mitigation (they are detection & mitigation techniques) or can use other detection techniques providing better detection performances.
- When a jamming and/or spoofing RFI is mitigated this improves the availability performance because otherwise the positioning solution would not be available. However, if the RFI is not properly or completely mitigated then, although the availability is improved, there could be an impact on safety, especially with spoofing. Therefore, an important trade-off between safety and availability arises from the application or not of mitigation techniques. This can be assessed depending on the type of RFI attack:
    - Jamming:
        - In most cases the purpose/consequence of jamming RFI is just to reduce positioning availability: jamming increases the measurement noise and position errors and can even make the receiver to lose track of the signals preventing it from providing any position estimation. Hence, it will be positive if a jamming mitigation technique can be applied to reduce the impact of jamming on availability. However, the jamming signal may not be completely mitigated, and the remaining part will affect the measurements.

Besides, the mitigation itself could imply the removal of part of the GNSS actual signal, which also affects the measurements. Any of both effects can increase the measurement errors beyond the specifications. Nevertheless, the impact on safety due to the application of RFI jamming mitigation techniques will be under control as long as the level of positioning error can be properly estimated (as it is done for example with the estimation of the position protection levels when redundant SVs are available).

- In other cases, jamming could be employed before a spoofing attack starts to increase its chance of success, so again a jamming mitigation technique could help to reduce the effect of jamming and reduce the spoofing success chances. However, this second case shows that the detection of jamming could be an indicator of a possible spoofing attack.

- Spoofing:
  - The objective/consequence of a spoofing attack is to deceive a receiver (our receiver could be the target or just be affected by the attack to another receiver) and, if successful, it can have a direct impact on safety.

    A spoofing mitigation technique could prevent the attack from succeeding or not, so the question is if, after the mitigation technique is applied, we are able to detect/confirm if the spoofing mitigation has avoided the attack and the estimated position has not been deceived.

    That is, once knowing that we are the potential target of a spoofing attack because we have detected it, the question is whether we can trust the position estimated after applying the spoofing mitigation technique or not, because if we cannot completely trust it, then it would be better from the safety point of view to declare the positioning estimation unavailable.
- False Alarm:
  - In both cases, jamming and spoofing, the false alarm rate of the detection technique needs to be considered in the trade-off. In general terms, when a false detection happens:
    - If there is no mitigation, then the availability can be degraded (the impact will depend on the consequences of raising the detection flag).
    - If a mitigation technique is activated, the mitigation may degrade the accuracy of the signal, which will also affect the availability.

As a consequence of the different effects of RFI detection and mitigation on safety and availability, **the proposed timeline gives priority to effective detection techniques with respect to effective mitigation techniques**.

The **proposed timeline** considers the deployment of the aviation on-board techniques in three different steps/phases:

- **Short Term**: The objective is to give priority to detection techniques with low implementation impact, low complexity, and low cost.
  - **Jamming Detection** capabilities: High against all jamming types, chirp (CH), constant wave (CW), pulsed (PL) and noise like / wideband (NL). This is achieved through the combination of:
    - AGC with Running Digital Sum (RDS)
    - Spectral and Statistical Detection – Simple Methods
    - RSS (C/N0 Monitoring)
    - Multi-frequency multi-constellation (MFMC) diversity (when affecting one band/constellation)

- **Spoofing Detection** capabilities: High against S1, S3 and S5 attacks and medium against S6 (high when only affecting one band/constellation) with the combination of:
  - AGC with Running Digital Sum (RDS)
  - Consistency check of measurements and PVT (e.g. CCH)
  - Multi-frequency multi-constellation (MFMC) diversity (when affecting one band/constellation)
- **Jamming Mitigation** capabilities: High against chirp (CH), constant wave (CW) and pulsed (PL) jamming types through the use of ANF&PB (noise like / wideband jamming type cannot be mitigated). ANF&PB mitigation techniques are already applied in commercial GNSS receivers and can be employed to improve the availability while maintaining safety as long as the impact on the positioning error can be estimated (e.g. through the computation of protection levels thanks to redundant available measurements).
  - Digital filtering – Simple Methods (ANF&PB)
- **Spoofing Mitigation** capabilities: High against S1, S3, S5 and S6 but when the attack only affects one band / constellation and assuming that the spoofed band/constellation can be identified based on solutions in previous epochs.
  - Multi-frequency multi-constellation (MFMC) diversity (when affecting one band/constellation)

- **Medium Term**: The objective is to considerably improve spoofing detection capabilities by including NMA (e.g. Galileo OSNMA and by employing data from the dual-antenna architecture already deployed in civil aircrafts. The combination of both techniques will allow to detect targeted and sophisticated spoofing attacks.

  Besides, the application of those two techniques also in combination with the Multi-frequency multi-constellation (MFMC) diversity technique will improve the spoofing mitigation capabilities as it will be possible to identify the spoofed band or constellation without making previous assumptions.

  In addition, the spoofing detection capabilities can be enhanced by including a medium cost and complexity Correlation Peak Monitoring (CPM) along with the consistency check with the aircraft INS.

  - **Spoofing Detection** capabilities
    - Multi-Antenna – Using currently deployed dual antenna architecture (e.g. D3)
    - NMA (e.g. Galileo OSNMA) (when available for Aviation)
    - Correlation Peak Monitoring (CPM) – Medium
    - Consistency check with INS

- **Long Term**: Although the combination of the techniques included in previous phases provide high jamming and spoofing detection and mitigation capabilities, they still lack certain capabilities like the mitigation of noise-like / wideband (NL) jamming and the mitigation of spoofing attacks when several bands and constellations are affected.

  Besides, jamming and spoofing attacks could get more sophisticated in the long term or could become much more frequent thus considerably impacting on availability, so the detection and mitigation capabilities may need to be enhanced.

  Techniques like multi-antenna (CRPA) and SCA (Spreading Code Authentication) could be a good complement to the techniques included in previous phases and including both would be a good complement. Hence, the timeline proposes to include in the long term a subset of the following techniques as long as the subset fulfils the objectives:

  - **Jamming Detection** capabilities
    - Multi-element antenna (CRPA)

        - Single-element antenna (Synthetic Antenna Array)
    - **Jamming Mitigation** capabilities
        - Multi-element antenna (CRPA)
        - Single-element antenna (Synthetic Antenna Array)
        - Spectral and statistical detection + Digital filtering – Complex Methods
    - **Spoofing Detection** capabilities
        - Multi-element antenna (CRPA)
        - Single-element antenna (Dual Polarization Antenna)
        - Single-element antenna (Synthetic Antenna Array)
        - SCA (Spreading Code Authentication)
        - Correlation Peak Monitoring (CPM) – High
        - Consistency check with other navigation and positioning technologies
    - **Spoofing Mitigation** capabilities
        - Multi-element antenna (CRPA)
        - Single-element antenna (Synthetic Antenna Array)

Table 4-5 provides an overview of the aviation on-board techniques to be included in each phase.

Table 4-18 Proposed Deployment Timeline of On-Board Technologies in Aviation

Layer	Technique	Maturity	Impact	Complexity	Cost	Effectiveness			
						Jamming Detection	Jamming Mitigation	Spoofing Detection	Spoofing Mitigation
Front-end	**AGC with Running Digital Sum (RDS)**	High	Low	Low	Low	High: CH,CW,NL		High:S1,S3, S5 Medium: S6	
Front-end	**Spectral and statistical detection – Simple Methods (Statistical Detection)**	High	Low	Low	Low	High: CH,CW,PL			
Front-end	**Digital filtering – Simple Methods (ANF&PB)**	High	Low	Low	Low		High: CH,CW,PL		
Signal processing	**RSS (C/N0 Monitoring)**	High	Low	Low	Low	High: CH,CW,NL			
Navigation	**Consistency check of measurements and PVT (e.g. CCH)**	High	Low-Medium	Low	Low			High S1, S5	
Navigation	**Multi-frequency multi-constellation (MFMC) diversity**	High	Low	Low	Low	High: CH,CW,NL		High: S1,S3,S5,S6	High: S1,S3,S5,S6
Short Term – Aggregated Effect			Low	Low	Low	CH: High CW: High PL: High NL: High	CH: High CW: High PL: High NL: Low	S1: High S3: High S5: High S6 Medium (High when only one band / const)	S1,S3,S5,S6 : High when only one band / const
Antenna	**Multi-antenna technologies – using currently deployed dual antenna architecture (e.g. D3)**	Medium-High	Medium	Low	Medium			High: S1,S3,S5,S6	
Signal processing	**Correlation Peak Monitoring (CPM) – Medium**	High	Medium	Medium	Medium			Medium: S3 Medium: S1,S5,S6	
Navigation	**NMA (e.g. Galileo OSNMA)**	Medium	Low	Low	Low			High: S1,S3,S5,S6	
Navigation	**Consistency check with other navigation and positioning technologies (INS)**	Medium-High	Low	Low	Low			High: TBD (since not assessed in AIRING)	
Medium Term – Aggregated Effect			Medium	Low	Medium	CH: High CW: High PL: High NL: High	CH: High CW: High PL: High NL: Low	S1: High S3: High S5: High S6 High	S1,S3,S5,S6 : High when only one band / const
Antenna	**Multi-element antenna technologies (CRPA)**	Medium	High	High	High	High CH,CW,NL	High CH,CW,NL	High S1,S3	High S1,S5
Antenna	**Single-element antenna technologies (Dual Polarization Antenna)**	Low	Medium	High	High			High: TBD	
Antenna	**Single-element antenna technologies (Synthetic Antenna Array)**	Low	Medium	High	High	High	High CH, CW, NL (+complex)	High: TBD	High S1,S5 (+complex)

Layer	Technique	Maturity	Impact	Complexity	Cost	Effectiveness			
						Jamming Detection	Jamming Mitigation	Spoofing Detection	Spoofing Mitigation
Front-end	**Spectral and statistical detection + Digital filtering – Complex Methods**	Medium	Medium	High	Medium		High		
Signal processing	**SCA (Spreading Code Authentication)**	Not yet supported						High: TBD	
Signal processing	**Correlation Peak Monitoring (CPM) – High**	High	Medium	High	High			High: S3 Medium: S1,S5,S6	
Navigation	**Consistency check with other navigation and positioning technologies (except INS)**	Low-Medium	Low	Low	Low			High: TBD	
Long Term – Aggregated Effect			High	High	High	High	High	High	High

4.6.2. GROUND DETECTION AND LOCATION TECHNOLOGIES

Based on the functional capabilities and implementation analysis of each ground technology presented in section §4.3.3, **the proposed timeline** for implementation is the following:

- **Short term**: the objective is to provide ANSPs (or the organization responsible for the monitoring of RFI, e.g. at State level) with RFI monitoring capabilities in all the airspace in which GNSS is used for navigation (e.g. aerodromes, TMAs, En-route) on the basis of COTS solutions already available or that could be available in the short term (< 2 years), considering the assessed maturity level of their underlying technologies. The proposed capabilities are:
    - **Jamming and Spoofing Detection and Location** capabilities:
        - Deployment of a basic (capability level 1) RFI monitoring network (able to detect jamming signals in L1/E1 and L5/E5) is recommended at all the aerodromes where RNP approach procedures are published. Optionally, this RFI monitoring network could include (capability level 2) some spoofing detection capabilities (e.g. affecting GPS L1 navigation)
        - Deployment of a high-end (capability level 3) RFI monitoring network (able to detect and locate the source of jamming signals on L1/E1 and L5/E5, and to detect spoofing signals affecting GPS L1/L5 and Galileo E1/E5) is recommended to protect busy TMAs (in which the disruption of operations due to the loss of the GNSS service could have a significant safety, capacity and efficiency impact)
        - Deployment of a surveillance-based system that processes ADS-B messages to detect aircraft affected by a jamming signal in L1 (in particular in the En-route airspace). Upgrade the system as soon as the capability to locate the source of the jamming signal is operationally validated
        - Other ground technologies (comparison between different surveillance sources such as ADS-B vs WAM/MLAT, see [REP05]) could be implemented to provide ANSPs with additional capabilities to detect the presence of spoofing signals.
        - Utilization of other means available to ANSPs (or to the appropriate organization at State level), such as flight inspection aircraft that could be adapted for RFI detection and location, or portable RF direction finder units that could be used for the same purpose (see [REP11]).
- **Mid-term**: the objective is to enhance the monitoring capabilities of ANSPs in the En-route airspace for RFIs in the L5/E5 band (to support DFMC GNSS operations)

- **Jamming and Spoofing Detection and Location** capabilities:
  - Upgrade the surveillance-based system that processes ADS-B messages to be able to detect aircraft affected by jamming in L1/E1 or L5/E5 bands, by processing the new envisaged ADS-B messages protocol that will include RFI information (e.g. RFI power) reported by aircraft with RFI detection capabilities

- **Long-term**: the objective is to enhance the monitoring capabilities of ANSPs of jamming and spoofing RFIs, particularly to improve the capability to locate the source of a spoofing signal
  - **Jamming and Spoofing Detection and Location** capabilities:
    - If one of the on-board technologies (D3, DPA, CRPA, Synthetic antennae array) that provides information on the angle or direction of arrival of a RFI signal (in particular, of a spoofing signal) were implemented in the mid- or long-term, that additional RFI information could be included in the new envisaged ADS-B messages protocol, and so the surveillance-based system could be upgraded to locate not only the source of jamming but also of spoofing signals.
    - Other ground technologies (e.g. multilateration based on extensive surveillance ADS-B/FLARM networks, see [REP05]) could be implemented to provide ANSPs with additional capabilities to locate the source of spoofing signals.

Next table summarizes the proposed implementation timeline of the ground technologies.

Table 4-19 Proposed Deployment Timeline of Ground Technologies in Aviation

	GNSS constellations and bands	Jamming detection	Spoofing detection	Jamming location	Spoofing location	Maturity	Impact CNS	Impact aircraft	Implementation timeline
RFI monitoring networks									
1st capability level	GPS L1/L5 GAL E1/E5a	Yes				5	1	0	Short-term*
2nd capability level		Yes	Yes			5	1	0	
3rd capability level (state-of-the-art)		Yes	Yes	Yes		5	1	0	
4th capability level		Yes	Yes	Yes	Yes	3	1	0	Medium-term
UAS for RFI detection and location		Yes	Yes	Yes	Yes	2	0	0	Medium-term**
Surveillance data processing systems									
Current ADS-B messages (QIs)	L1/E1	Yes		Yes***		3-5	1	0	Short-term
Future ADS-B messages (RFI power) EUROCONTROL RFI mitigation concept	L1/E1 L5/E5a	Yes		Yes		3-4	2	3	Medium-term
Future ADS-B messages (RFI AoA/DoA)	GPS L1/L5 GAL E1/E5a	Yes	Yes	Yes	Yes	2	2	5	Long-term
Comparison between surveillance sources (ADS-B vs MLAT/WAM)	GPS L1		Yes			2	1	0	Short-term
Multilateration based on extensive surveillance networks (ADS-B /FLARM)	GPS L1/L5 GAL E1/E5a		Yes		Yes	2	5	0	Long-term

* ANSPs should perform a security risk assessment to decide which RFI monitoring network to deploy to protect each aerodrome / TMA

** The main research challenge is to embark available RFI detection and location technology on an UAS

*** It still requires some research to mature the technology / consolidate performances but can be integrated seamlessly in operational systems

4.6.3. SUMMARY OF TECHNOLOGIES IMPLEMENTATION TIMELINE

Next table summarizes the proposed implementation timeline for the recommended technologies

Table 4-20: Technologies implementation timeline.

LOCATION	LAYER / EQUIPMENT	TECHNOLOGY	MAIN FUNCTION						ASSESED IN AIRING	TIMELINE
			JAMMING			SPOOFING				
			Detection	Localization	Mitigation	Detection	Localization	Mitigation		
On-board	2. Front End	Spectral and statistical detection – Simple Methods (Statistical Detection)	Y	N	N	N	N	N	Y	Short term
On-board	2. Front End	Digital filtering – Simple Methods (ANF&PB)	N	N	Y	N	N	N	Y	Short term
On-board	2. Front End	AGC with Running Digital Sum (RDS)	Y	N	N	Y	N	N	Y	Short term
On-board	3. Signal processing	RSS (C/N0 Monitoring)	Y	N	N	N	N	N	Y	Short term
On-board	4. Navigation	Consistency check of measurements and PVT (e.g. CCH)	N	N	N	Y	N	N	Y	Short term
On-board	4. Navigation	Multi-frequency multi-constellation (MFMC) diversity	Y	N	Y	Y	N	Y	Y	Short term
Ground	5. RFI monitoring network	RFI monitoring networks (capability level 1 to 3)	Y	Y (POS)	N	Y	N	N	Y	Short term
Ground	6. SUR data processing	Surveillance data processing system (current ADS-B message: QIs)	Y (L1)	Y (POS)	N	N	N	N	Y	Short term
Ground	6. SUR data processing	Comparison between surveillance sources (ADS-B vs WLAM/MLAT)	N	N	N	Y	Y (POS)	N	N	Short term
On-board	1. Antenna	Multi-antenna technologies – using currently deployed dual antenna architecture (e.g. D3)	N	N	N	Y	N	N	N	Medium term
On-board	3. Signal processing	Correlation Peak Monitoring (CPM) - Medium	N	N	N	Y	N	N	Y	Medium term
On-board	4. Navigation	NMA (e.g. Galileo OSNMA)	N	N	N	Y	N	N	Y	Medium term
On-board	4. Navigation	Consistency check with other navigation and positioning technologies (INS)	N	N	N	Y	N	N	N	Medium term
Ground	5. RFI monitoring network	RFI monitoring networks (capability level 4)	Y	Y (POS)	N	Y	Y (POS)	N	N	Medium term
Ground	5. RFI monitoring network	UAS for RFI detection and location	Y	Y (DOA)	N	Y	Y (DOA)	N	N	Medium term
Ground	6. SUR data processing	Surveillance data processing system (future ADS-B message: RFI power)	Y (L1/L5)	Y (POS)	N	N	N	N	Y	Medium term
On-board	1. Antenna	Single-element antenna technologies (Dual Polarization Antenna)	N	N	N	Y	Y (DOA)	N	Y	Long term
On-board	1. Antenna	Multi-element antenna technologies (CRPA)	Y	Y (DOA)	Y	Y	Y (DOA)	Y	Y	Long term
On-board	1. Antenna	Single-element antenna technologies (Synthetic Antenna Array)	Y	Y (DOA)	Y	Y	Y (DOA)	Y	N	Long term
On-board	2. Front End	Spectral and statistical detection + Digital filtering – Complex Methods	N	N	Y	N	N	N	N	Long term
On-board	3. Signal processing	Correlation Peak Monitoring (CPM) - High	N	N	N	Y	N	N	Y	Long term
On-board	3. Signal processing	Spreading Code Authentication (SCA)	N	N	N	Y	N	N	N	Long term
On-board	4. Navigation	Consistency checks with other navigation and positioning technologies (except INS)	N	N	N	Y	N	N	N	Long term
Ground	6. SUR data processing	Surveillance data processing system (future ADS-B message: AoA/DoA)	Y (L1/L5)	Y (POS)	N	Y	Y (POS)	N	N	Long term
Ground	6. SUR data processing	Multilateration based on extensive surveillance networsks (ADS-B/FLARM)	N	N	N	Y	Y (POS)	N	N	Long term

4.7. ROADMAP FOR IMPLEMENTATION

In the AIRING project several on-board and ground technologies with different Technology Readiness Levels (TRLs) as well as an operational concept to detect, mitigate and locate RFIs (jamming, spoofing) affecting GNSS in Aviation have been assessed with different methods (including laboratory tests, live demonstrations, and operational simulations with humans in the loop) in order to identify and recommend the implementation of a set of technological and operational safeguards that will contribute to increase GNSS resilience and thus achieve a medium or low level of operational risk by 2030.

To define the way forward towards the implementation of the recommended set of technologies (and the supporting operational concept) we have taken as reference the European Operational Concept Validation Methodology [EOCVM], which is a framework to provide structure and transparency in the validation of air traffic management (ATM) operational concepts as they progress from early phases of development towards implementation.

The E-OCVM methodology defines a lifecycle of eight phases (see next figure), being E-OCVM and validation mainly concerned with lifecycle phases V1, V2 and V3.

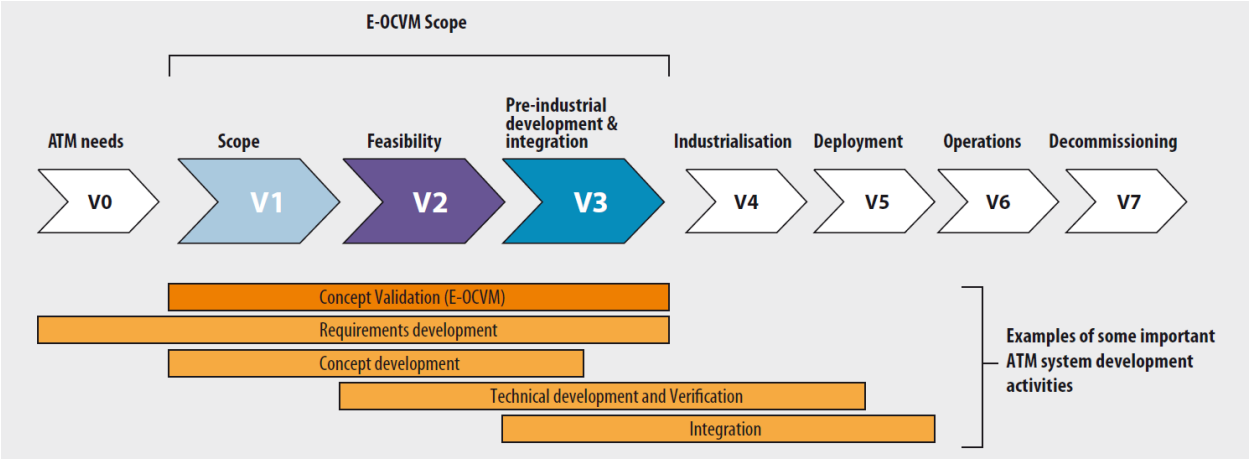


Figure 4-9. E-OCVM validation and other ATM system development activities

The goal of the E-OCVM validation activities is to complete V3 phase (pre-industrial development & integration), point at which industrial and operational stakeholders can take over the industrialization, deployment and operation of the new ATM system (which obviously includes the airborne segment of the ATM system, i.e. the aircraft and its avionics, and the cockpit crew).

In the AIRING project the main target stakeholders are avionics manufacturers (specifically the GNSS receiver manufacturers), Supplemental Type Certificate holders, Aircraft manufacturer, CNS manufacturers (RFI monitoring networks and surveillance systems manufacturers), ANSPs (which are responsible for the deployment of new ATM/CNS systems), and Regulators (such as EASA, because if at some point in time the risk of using GNSS as unique means for PNT, including approaches and landing, needs to be mitigated, only the regulator can mandate the installation of resilient systems).

If we look at the E-OCVM methodology, we can conclude that, overall, the goal (and results) of the AIRING project corresponds to phase **V2 (feasibility)**, because the main objective of this phase is to develop and explore the **individual** concept elements and support enablers, on the basis of analysis, modelling and **simulations** (fast and real-time), including **functional prototyping**, exposed to a range of **representative operational contexts**, and evaluated with a **common performance framework**.

The main goal of phase V2, according to the E-OCVM methodology, is to establish the feasibility from an operational and transitional viewpoint and provide initial elements for technical feasibility. One of the outcomes of this phase may be that **one or more prototyping and validation iterations may be needed** before the transition criteria to phase V3 are reached.

In turn, the objective of phase **V3 (pre-industrial development & integration)** is threefold:

- Firstly, to further develop and refine operational concepts and supporting enablers to prepare their transition from research to an operational environment
- Secondly, to validate that all concurrently developed concepts and supporting enablers (procedures, technology and human performance aspects) can work coherently together and are capable of delivering the required benefits
- Thirdly, to establish that the concurrent packages can be integrated into the target ATM system

The main type of validation exercise conducted in this V3 phase is thus concerned with **integration** and establishing that the performance **benefits** predicted for individual concept elements in V2 **can be realized collectively**. It requires **integration of pre-industrial prototypes** in representative system platforms. This could include the use of **real-time simulations** and **shadow mode/live trials**, allowing exposure to different representative operational context environments.

One point worth recalling is that in AIRING the prototyped and validated technologies do not have the same TRL but, on the contrary, they cover a wide TRL range (from TRL3 to TRL9, see [EOCVMA]), and so they have reached different levels of maturity (see section 6.1 of [REP15])

On the other hand, considering the level of maturity of each technology and other key criteria (impact, complexity, cost, and effectiveness), the **timeline of implementation of the recommended set of technologies** has been split into three periods: short-term, mid-term and long-term (see §4.6).

However, when we talk about the **roadmap for implementation**, we refer to the activities that we should carry out in the short-, mid- and long-term to support the implementation of the different technologies within their corresponding implementation timeline.

Then, what is important to note is that the short-term roadmap should include activities not only to facilitate the implementation of those technologies that are recommended for implementation in the short-term, but also activities to increase the maturity (or reduce the complexity, impact or cost) of the technologies that are recommended for implementation in the mid- and long-term timeline.

As a matter of fact, the **short-term roadmap** we propose should include, depending mainly on the maturity of the recommended technology, activities to:

1. Promote the deployment by stakeholders of systems / COTS available in the market
2. Promote the industrialization by stakeholders of the recommended technologies
3. Increase the maturity of the technologies recommended for implementation in the short-term in order to reach the criteria of the EOCVM V3 phase, mainly through the validation of the benefits that those technologies, when integrated, could bring collectively (while at the same time increasing the maturity of each individual technology from TRL4 to TRL6 or beyond).
4. Increase the maturity of the technologies recommended for implementation in the mid- and long-term. The goal is to either:
    a. Carry out a second validation iteration (e.g. from TRL2 to TRL4) of technologies that we have assessed as still being in the EOCVM V2 phase, or
    b. Start the validation of new technologies to advance (e.g. to reach TRL2 or higher) throughout the EOCVM V2 phase

The activities proposed to address (3) and (4), the core of the short-term roadmap, are described in §4.7.1.1 and §4.7.1.2, respectively. The activities proposed to attain goals (1) and (2) are described in sections §8.1 and §8.2, as **recommendations to support the** short-term **roadmap**.

Section §4.7.2 covers the **mid- and long-term roadmap** and describes other activities to further increase the maturity of the technologies proposed for implementation in the mid- and long-term.

Next figures illustrates how to tailor the EOCVM methodology to support the definition of the short-term and mid- and long-term roadmaps, as well as the relationship between the activities proposed in those roadmaps and the proposed timeline for implementation of the recommended set of technologies.

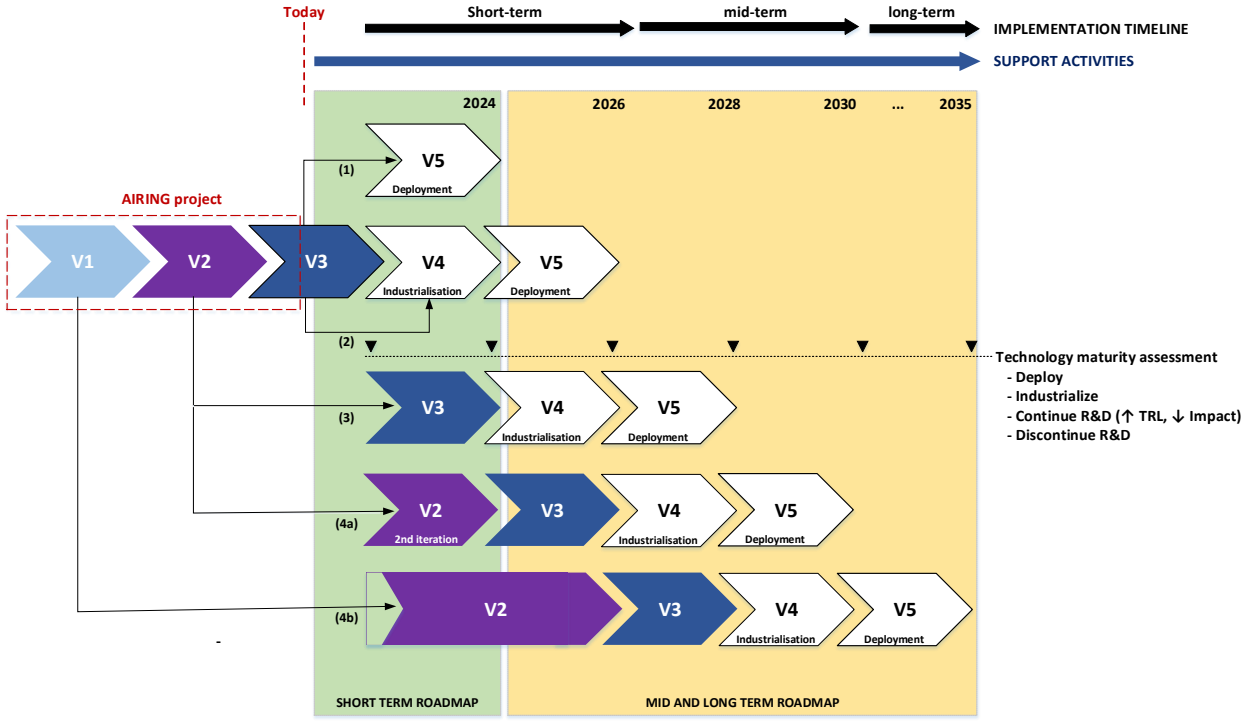


Figure 4-10. E-OCVM validation framework applied to the AIRING project

It is important to note that the E-OCVM validation methodology shown in the figure is applied in iterative steps, and that at the end of each of those steps there should be a maturity assessment of each researched technology (as the one described in section 6.1 of [REP15]) in order to decide whether it is ready for deployment or industrialization, it requires additional research effort to increase its maturity or reduce its impact, complexity or cost, or it is better to discard it.

4.7.1.SHORT-TERM ROADMAP

This short-term roadmap includes two types of activities:

- Those aimed at facilitating the implementation of recommended technologies in the short-term
- Those aimed at increasing the maturity and/or reducing the impact or cost of the recommended technologies for implementation in the mid- and long-term

Note that these two types of activities refer to (3) and (4), respectively, in Figure 4-10 above.

4.7.1.1. TO IMPLEMENT RECOMMENDED TECHNOLOGIES IN THE SHORT-TERM

To support the buy-in, and eventual adoption, by industry of the recommended short-term technical safeguards (e.g. techniques), the main objective of the short-term roadmap is to **reach an E-OCVM V3 maturity level of the Operational Concept and technological enablers** selected in AIRING (e.g. the on-board and ground technologies proposed in §4.6.3 for implementation in the short term).

To attain this objective, it is crucial, according to [EOCVM], that validation is "*concerned with integration, and establishing that the performance benefits predicted for individual concept elements in V2 can be realized collectively. It requires integration of pre-industrial prototypes in representative system platforms. This could include the use of real-time simulations and shadow mode/live trials, allowing exposure to different representative operational context environments.*".

Given the complex nature of the technical elements (on-board, ground), operational actors (cockpit crew, ATCOs), and systems, we suggest splitting their integration and operational validation into two phases, the first phase to be performed within the short term roadmap, and the second phase, if necessary, to be performed within the mid- and long-term roadmap (see §4.7.2)

In the first phase, we propose to carry out a **partial integration and operational validation of** some of those **elements** (**on-board** and **ground technologies**), **actors** (**cockpit crew, ATCOs**), and **systems** (**RFI monitoring networks**, **surveillance systems**) taken together.

Besides, **improvements to** the technical and operational **maturity of each** of those **stand-alone elements** are also targeted in this first integration phase.

The groups of elements, actors and systems proposed for this first integration phase are:

- The integration and combined validation of the following detection and mitigations techniques proposed for the on-board GNSS receiver into an **on-board GNSS receiver demonstrator**:
    - AGC with Running Digital Sum (RDS)
    - Chi-square test on digital samples
    - Spectral and statistical detection – Simple Methods (Statistical Detection)
    - Digital filtering – Simple Methods (ANF&PB)
    - RSS (C/N0 monitoring)
    - Consistency checks (CCH) of measurements and PVT, and
    - Multi-frequency Multi-constellation (MFMC) diversity

  The main objective of this task is to study the interaction between the mitigation techniques applied in the Front-End (and Pre-correlation) stage, with the detection techniques applied in the next stages of the processing chain, i.e. signal processing (correlation and post-correlation) and navigation.

  A preliminary list of the **improvements** that could be pursued for each individual stand-alone **on-board technique** are described in section 4.2.1 of [REP15]

  Furthermore, the navigation stage of the GNSS receiver should implement **on-board integrity monitoring** capabilities (e.g. FDE and computation of HPLs with H-ARAIM), in order to be able to verify the integrity of the PVT computed solution (as required in [MOPS]).

- The integration and validation of a RFI monitoring network and a surveillance based RFI detection and localization system into a **ground RFI detection demonstrator**

  The goal of this integration is twofold:

    - To define how to reconcile (e.g. crosscheck) the RFI information coming from different sources and how to present this information to the involved actors. To achieve this goal we propose to prototype an RFI events simulator, an API and an HMI to present the information to the operational staff. This demonstrator could be used to customize and validate the human performance (human factors) of the HMIs for the ATC, ATSEP and engineering personnel, leveraging their situational awareness of GNSS RFI events
    - To define and assess a reliable model to estimate the impact of a located RFI source on the surrounding airspace with enough assurance, so that consistent actions would be made by the ATCO in such area. The constrains regarding the trustworthy of the information given by the system should also be assessed to avoid any misleading information that could lead to a safety issue or a misuse of the GNSS systems.

  In this phase, **improvements** to **ground techniques** should be also addressed, including those described in section 4.2.1 of [REP15]

- The preparation and integration of a **real-time simulation environment** to enable the **operational validation of the interactions between cockpit crew and ATC controllers** (with humans in the loop) in order to further develop the operational procedures and technical enablers required to manage different RFI scenarios.

  To take this validation to the proper level, it is required to follow scientific point of view, achieving measurable results and allowing true recommendations and conclusions. Aiming at TRL3 (analytical and experimental proof of concept), section 4.2.1 of [REP15] describes the proposed steps.

Besides these three main integration and operational activities, two other tasks are recommended:

- To **improve the laboratory environment** to support the assessment of the on-board and ground integrated demonstrators.

  The main required improvement consists in adding the capability of generating more sophisticated spoofing attacks (e.g. S5, S6 attacks, to be included in next [MOPS] version), in which the simulated spoofer is time-synched with GPS time system within few nanoseconds to some tens of nanoseconds, so that a running receiver which is continuously tracking the satellite will experience more than one correlation peaks in its correlation domain at the tracking stage.

  Other features that could be added to the laboratory environment to increase the fidelity of the results (and that could be also used to assess the technologies proposed in the mid- and long-term roadmap) is the modelling and simulation of the aircraft fuselage multipath effects on the true GNSS signals, and the aircraft fuselage shielding effects on the RFI signal. Furthermore, the need of modelling and simulating the effects of certain Space Weather events (e.g. scintillation), could be assessed and, eventually, added to the laboratory environment.

  The improvement of the laboratory environment should support, through automation, the definition and **execution of a much higher number of RFI scenarios** (e.g. to assess different types of Chirp and Pulsed jamming signals, the combination of multiple jamming signals, signals with different power variations, spoofing attacks where changes -drop or rise- of CN0 are minimal), as well as the **computation of additional KPIs** to assess the performances of the detection, location and mitigation techniques (e.g. false alert and missed detection rates)

  Besides, the laboratory environment should **include** some **certified GNSS aeronautical receivers** (or red-label receivers) to use them as benchmarks to compare the measured KPIs, and to be able to generate new data sets to test the ground surveillance-based RFI detection and localizations techniques (e.g. to generate new ADS-B data, beyond the GRIT data set)

  Last but not least, an **optional activity** that could be included is the **improvement of the live demonstration environment** to support the execution of new exercises with the on-board and ground demonstrators. As for the laboratory environment, the main objective of this improvement would be to add the capability of generation of intelligent (tightly time synchronized) spoofing attacks.

- To prepare and run **fast-time ATM simulations to characterize quantitatively** (e.g. safety, capacity, and flight efficiency indicators) the **impact of different RFI events** (GNSS degraded, GNSS unavailable, GNSS misleading) on different operational scenarios

  The overall goal of this task is to update the security risk assessment, replacing the expert judgement of the impact of RFI events on adverse scenarios, with quantitative assessments.

Besides the recommended activities to promote the implementation of short-term technical measures described above, this short-term roadmap should include the further **development of the operational concept to manage RFIs** to take advantage of the on-board and ground technical and operational detection, location and mitigation capabilities available today.

This operational concept development should address several issues described in section 6.1 of [REP15]

The aim of the activities described is to **prepare specific material to support the industrialization and deployment of the technologies proposed for short-term implementation**.

That material would be the **main output of the short-term roadmap**, and would include:

- A **refinement of the methodology proposed in the security risk assessment** described in [REP02] in order to classify and count consistently across Europe the detected RFI events (either reported by aircraft or detected on ground, e.g. by ANSPs or other public ground monitoring networks), **with the aim of computing periodically the security risk** and so to monitor the trends of the different type of events as well as to identify, and manage, RFI hot spots
- A **refinement of the labelling scheme** described in [REP09] for the on-board GNSS receiver and for the ground RFI detection and localization equipment, that could be later incorporated into regulation, standardization or technical material applicable to those systems.

- A set of **proposals of specific additions or amendments** (i.e. describing the text to be added or amended) **of regulations and standards** (section 8.2 identifies the regulations and standards that should be created or modified, but not any proposed specific change)
- A set of **interoperability technical specifications for the ground RFI detection and localization systems** and other enablers (e.g. an API to share information), addressing the operational and performance requirements of the proposed solutions, for instance, to address the high-level standards applicable to the systems that work into the ATM network (e.g. SWAL), and the integrity and reliability of the data to be provided by the systems

  These specifications would be a valuable information for industrial stakeholders to define the evolution roadmaps of their commercial products, for operational stakeholders to define the scope of their procurement and tendering processes, and for all stakeholders to ensure the interoperability of their systems.
- A **detailed Operational Concept and** recommended **operational procedures**, that could be tailored by the different ANSPs to their operational needs
- A **Cost Benefit Analysis (CBA)** for the proposed short-term solutions, to help stakeholders to select and justify the technical solutions that best fit their needs
- **Training and awareness material** that could be provided to stakeholders to help them understand the characteristics, likelihood and impact of RFIs affecting GNSS, as well as the technical and operational solutions available and how to make the best use of them.
- To make some **Customer Furnished Items (CFIs)** available to stakeholders, such as:
  - A prototype of the API (including the source or object code, and use documentation)
  - A data set with reference GNSS and RFI adverse scenarios (which, for instance, could be used to apply the labelling scheme and methodology described above)
  - The use of the laboratory set-up as a service for other projects.

4.7.1.2. TO INCREASE MATURITY / REDUCE IMPACT OF OTHER TECHNOLOGIES

This section identifies the activities that are recommended within the short-term roadmap to increase the maturity and/or reduce the impact or cost of a sub-set of the technologies that are recommended for implementation in the mid- and long- term.

Two criteria have been followed to select this sub-set of technologies:

- Technologies assessed in the AIRING project (because they were found to be part of the most promising, see §4.6.3) but that are not proposed to be integrated into the on-board GNSS receiver and ground RFI detection and location demonstrators described in §4.7.1.1. These are:
  - CRPA antenna
  - Dual Polarization (DPA) antenna
  - Correlation Peak Monitoring (CPM)
  - OSNMA
- Other technologies recommended for implementation but that were not assessed in the AIRING project (due to budget and schedule constraints), and that do not have a high impact nor a high cost and have at least a medium maturity (see §4.6.1). These are:
  - Multi-Antenna – Using currently deployed dual antenna architecture (e.g. D3)
  - Spectral and statistical detection + Digital filtering – Complex Methods

It is note worthing that all these technologies would be implemented on the on-board GNSS receiver

The research approach to be followed with these technologies would be similar to the approach followed in AIRING, i.e. to test them stand-alone in a laboratory setting.

Section 4.2.1 of [REP15] describes some specific research goals for those technologies.

4.7.2. MID- AND LONG-TERM ROADMAP

In the mid- and long-term roadmap we have included activities to:

- Widen the scope of the program to improve GNSS resilience in Aviation
- Increase the maturity and/or reduce the impact or cost of other recommended technologies for implementation in the mid- and long-term
- Increase the level of integration and fidelity of the researched on-board and ground technologies

Regarding the **scope of the program to improve GNSS resilience in Aviation**, it may address some GNSS services and applications not considered in AIRING, such as the following:

- Impact on current (e.g. EGNOS V2, Galileo HAS), short-term (Galileo OSNMA) or mid- and long-term E-GNSS services (e.g. EGNOS V3, ARAIM, SBAS L5 NMA, EGNOS evolution, G2G)

  One technical challenge to address these or other GNSS services not assessed in AIRING is that both the laboratory environment (e.g. GNSS simulator) and the DUTs (e.g. GNSS receivers) must be able to generate and process, respectively, the corresponding GNSS signals.
- Other applications of the GNSS receiver beyond positioning (e.g. generate a time signal to feed other on-board equipment or CNS systems on ground; be part of a GBAS station, RIMS or GSS)
- Use of GNSS in aviation beyond ATM, in particular the specific conditions (e.g. on-board equipment, operational context, missions, stakeholders) of U-Space

Regarding the proposed research to **increase the maturity or reduce the impact or cost of new technologies**, it encompasses on-board detection, location and mitigation technologies, on-ground detection and location technologies, but also other space-based (or HAPS) detection and localization techniques as well as A-PNT technologies:

- On-board technologies
  - Synthetic Antenna Array
  - Spread Code Authentication (SCA)
  - Other NMA services (e.g. on SBAS L5)
  - Consistency checks with INS
  - Consistency check with other navigation and positioning technologies

  A new recent concept that could be also assessed is the Retrofit Signal Conditioning. This is a concept to detect, characterize and mitigate threats to GNSS in a unit that sits between the antenna and the receiver, ingesting RF and returning "cleaned" RF, receiver agnostic. It targets jamming, spoofing and system degradations, such as evil waveforms.
- On-ground technologies
  - Spoofing detection by comparison with non-GNSS surveillance means (e.g. WAM/MLAT)
  - Spoofing detection and localization by comparison with non-GNSS multilateration based on the processing of the RF surveillance signals (e.g. ADS-B) received from aircraft
  - Use of UAS equipped with RFI detection and localization technologies (e.g. those able to measure the AoA of the RFI signals) to enhance ANSPs capabilities.

    With the use of UAS, operating in open category, an altitude of 120 m can be reached, enabling a large coverage (up to 45 Km of radio horizon), better than those available with typical ground stations. The first expected operations of RFI-detection UAS would be in line of sight from the pilot location, dealing with possible GNSS denied scenarios, and not requiring special A-PNT navigation techniques. These A-PNT techniques could be added in the future, enabling BVLOS UAS based interference hunting operations
- Other technologies
  - Space-based detection and localization techniques (see [REP05])

- HAPS (High Altitude Platform Station, a.k.a. High Altitude Pseudo Satellite) based RFI detection and localization system.

  The use of HAPS, flying in the stratosphere at altitudes of 20-24 Km, would enable a very large coverage for RFI detection (up to 600 Km of radio horizon), with much better sensitivity than using LEO satellites (with altitudes of 200-2000 Km)

- A-PNT systems, both GNSS-based (e.g. LEO PNT) and non-GNSS (see [REP05])

Finally, the mid- and long-term roadmap may also include activities to support the integration and operational validation of the on-board and ground demonstrators proposed in section 4.7.1.1, to **make the operational validation closer to resemble the final operational conditions** (e.g. on-board and ground demonstrators running in real-time on representative HW platforms)

5. ANNEX A: LABORATORY ASSESSMENT OF ON-BOARD TECHNOLOGIES

5.1. JAMMING DETECTION AND MITIGATION

To effectively test the ability of a **Controlled Radiation Pattern Antenna (CRPA)** to **detect and mitigate** RFIs (**both jamming and spoofing**), all components of the test have been virtualized:

- Signal generation (clean, disturbed with interference, disturbed with spoofing)
- CRPA antenna with MUSIC algorithm (implemented in software)
- Interference detection (as part of MUSIC algorithm)
- Interference mitigation (as part of MUSIC algorithm)
- GNSS receiver (open-source software receiver)

The CRPA tests have been performed for a number of test scenarios as previously described. In general, the results are very positive and the CRPA antenna is shown to be very effective in both detection and mitigation of jamming and spoofing. However, as the tests are idealized laboratory tests the true effectiveness is to be proven in further studies with real hardware and more realistic environmental conditions. Notably the relative strength of the interference signals and the exact way they are introduced may impact the quality of detection.

Next figures show some results of the tests performed.

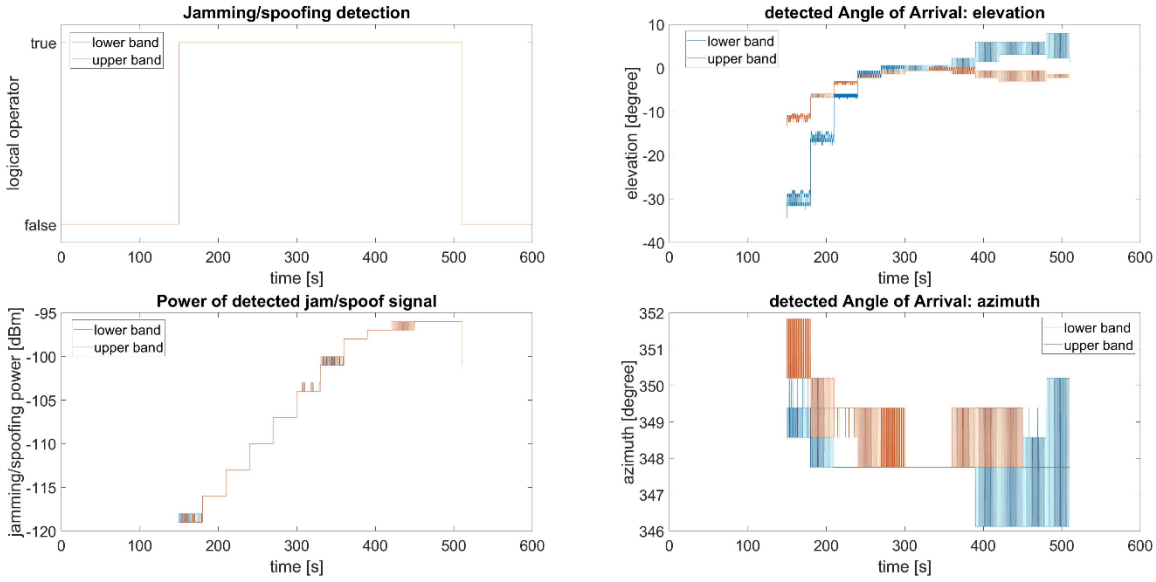


Figure 11: RFI detection parameters obtained by CRPA algorithm in a jamming scenario

As far as jamming pre-correlation mitigation techniques are concerned, two techniques have been researched, namely, **Pulse Blanking (PB)** in time and frequency domains and **Adaptive Notch Filter (ANF)**. These are well known jamming mitigation techniques that are effective against pulsed, CW and chirp interferences, but not against noise-like wideband interferences. In order to activate these mitigation techniques, a detection technique that allows the characterisation of these three types of jamming interferences with 100% accuracy was used to automatically trigger the most appropriate mitigation mechanism for each type of interference (pulsed, chirp, and continuous wave).

The tests that were carried out can be split into two categories: laboratory tests and live tests. During the laboratory tests, synthetic data produced with the help of a Skydel simulator and a combiner tool to introduce jamming was used to emulate real life scenarios by covering different jamming cases, each being tailored to a specific type of interference and dynamic modes of the receiver.

Table 5-1 Jamming Pre-correlation Mitigation Tests Summary

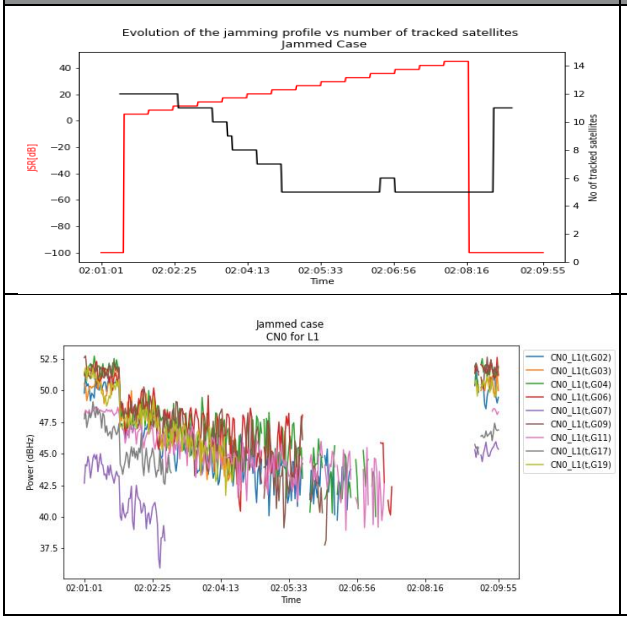
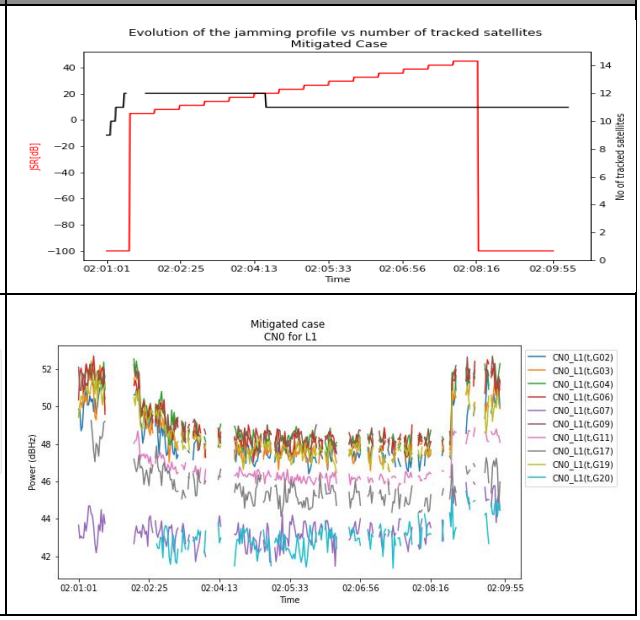
Interference Type	Type of test	Pre-Correlation Mitigation Technique	Effective	JSR Level effectively Mitigated
Pulsed	Laboratory Static MFMC	**PB in Time Domain**	**YES**	All the tested Pulsed RFI, up to 45dB JSR, were mitigated
CW	Laboratory Static SF and MFMC	**PB in Frequency Domain**	**YES**	All the tested CW RFI, up to 45dB JSR, were mitigated
Chirp	Laboratory Static SF and MFMC	**ANF**	**YES**	Chirp RF: • SF: Up to 17dB JSR, were mitigated • MFMC: Up to 25dB JSR, were mitigated
Noise-Like (wideband)	Laboratory Static MFMC	N/A *The tested techniques cannot cope with this type of interference.*	NO	As expected, the tested mitigation techniques were not effective against Noise-like interferences.

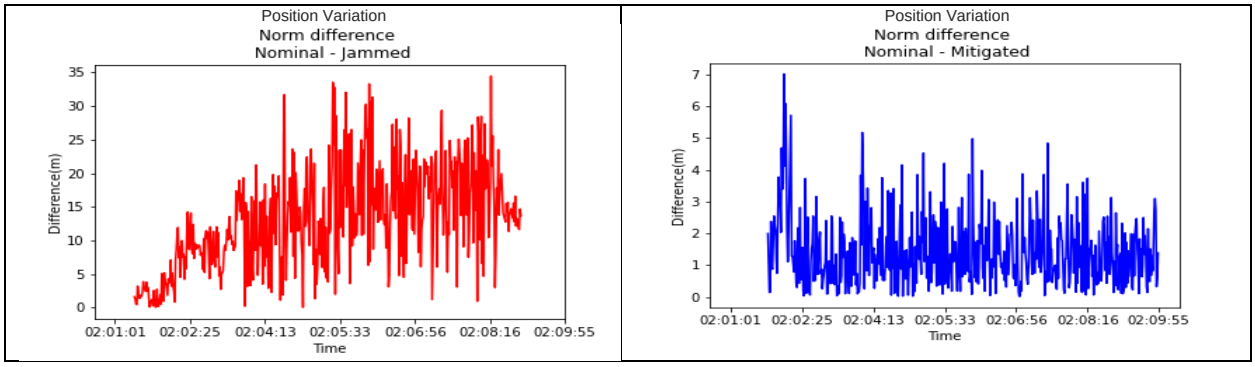
An RFI is considered to be mitigated as long as the PVT solution is not degraded more than some meters or a few tens of meters.

The results obtained when applying the mitigation mechanisms provide considerable improvements in terms of tracking and PVT solution.

Table 6-2 presents some of the results obtained after pulse blanking (PB) in time domain was applied to the case when pulsed interference was present. The improvement due to the mitigation technique can be clearly noticed in the increased number of tracked satellites and better C/N0 for the mitigated case, which translates into an improved PVT solution with a much lower variation with respect to the position obtained without jamming (nominal).

Table 5-2 Results of the laboratory tests for pulsed interference PB mitigation techniques

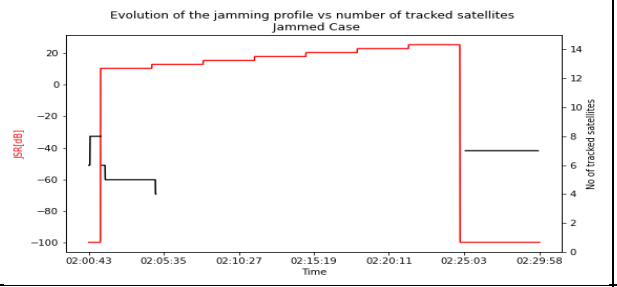
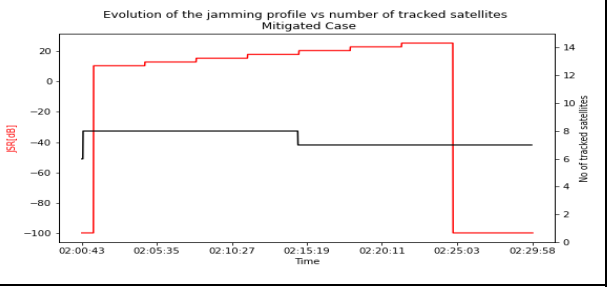
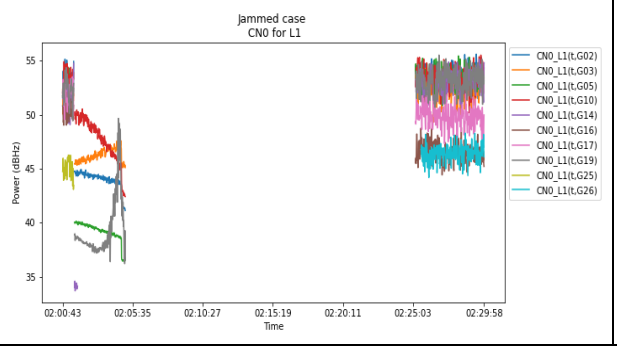
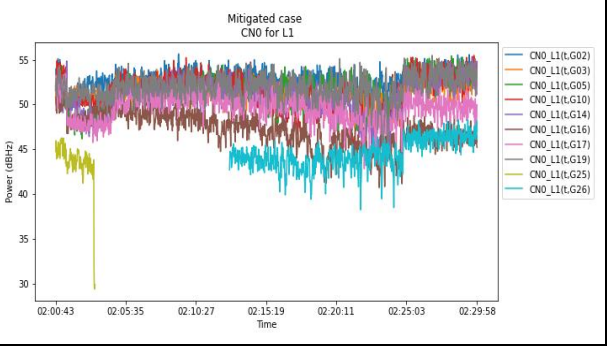
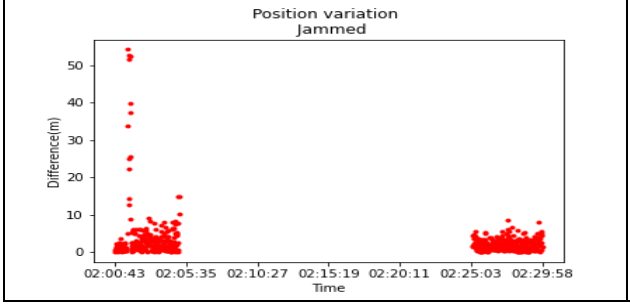
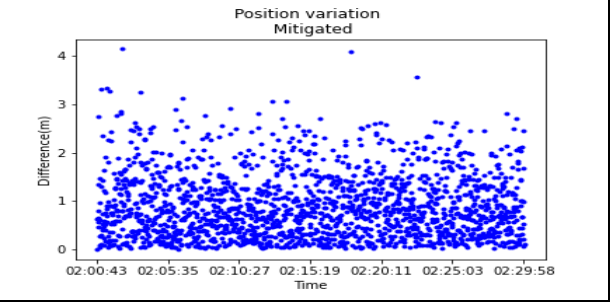
Jammed (no mitigation)	Jammed with Mitigation
	



Hence, the results show that PB in time domain is effective against pulsed interference.

Table 6-3 provides an overview of the effect that the pulse blanking (PB) in frequency domain technique has over continuous wave (CW) interferences. A considerable improvement can be observed in the number of satellites that are tracked and C/N0 across the period during which the scenario was simulated and in the PVT solution that has a lower position variation with respect to the position obtained without jamming (nominal).

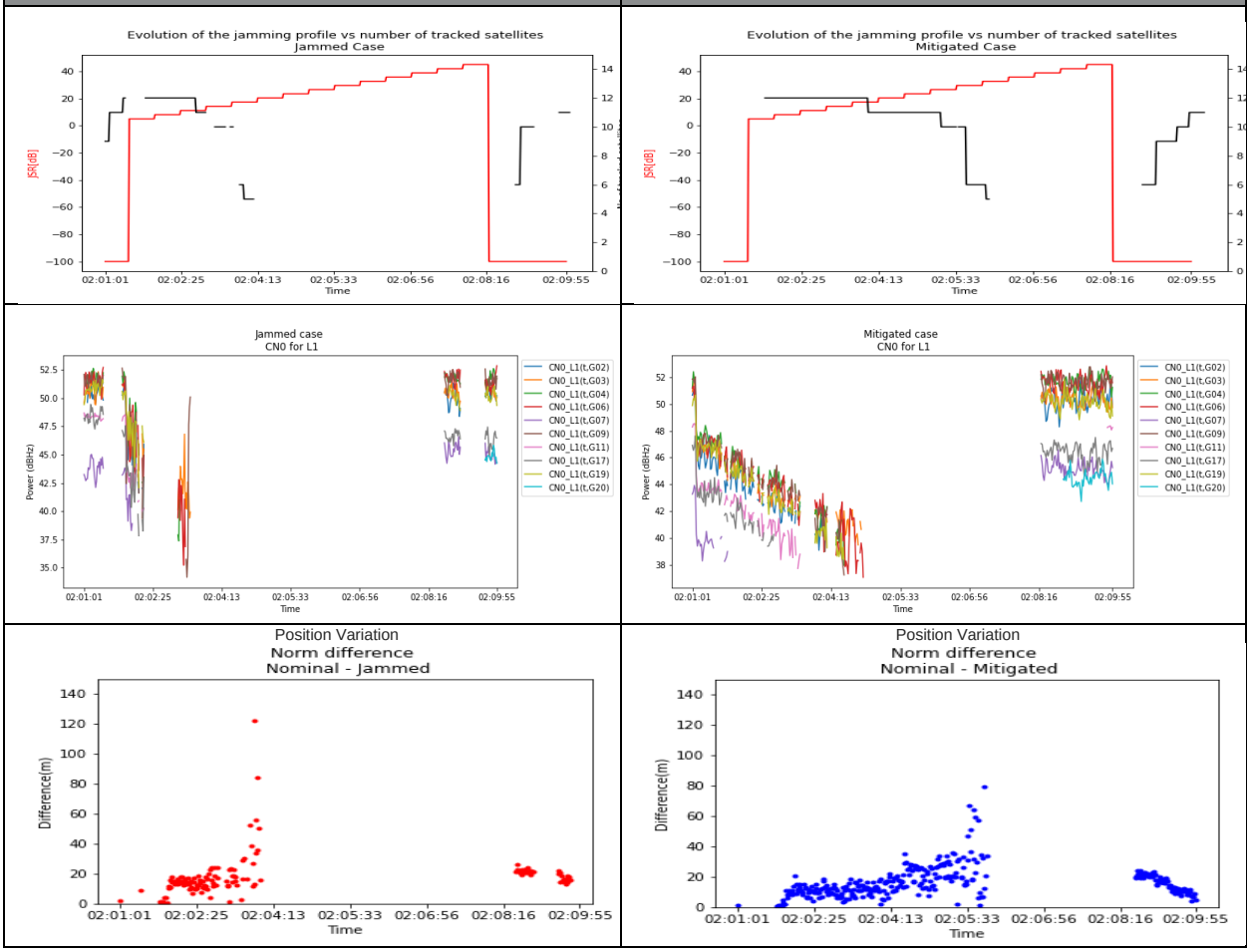
Table 5-3 Results of the laboratory tests for continuous wave interference PB mitigation techniques

Jammed (no mitigation)	Jammed with Mitigation
	
	
	

Hence, the results show that PB in frequency domain is effective against CW interference.

Figures in Table 6-4 show some of the ANF results obtained against chirp interference. Left column provides the results obtained without mitigation and right column with mitigation. Comparing the plots in the first and second rows, an improvement can be clearly observed for the mitigated case, as tracking is kept for more time, which allows the receiver to compute a PVT solution for longer time as it is clearly seen in the third row, where the figures show the position variation with respect to the nominal case (without jamming).

Table 5-4 Results of the laboratory tests for chirp ANF mitigation techniques

Jammed (no mitigation)	Jammed with Mitigation
	

Hence, the results show that ANF is effective against Chirp interference.

Other tested **jamming detection** techniques are the '**Chi-Square based**' and '**CN0 monitoring**'.

The best performing jamming detection technique that worked for all scenarios in laboratory and live demonstrations is the 'Chi-Square based technique' (identified also as AGC), because significant variation of power profile favors detection techniques that are measuring power of the signal. Chi-Square test is applied on the raw IQ sample distribution of the digitized signal.

The Chi-Square test is a statistical hypothesis test that compares the distribution between observed and expected data and creates a metric for distribution resemblance.

Next figure shows show results of the performed tests

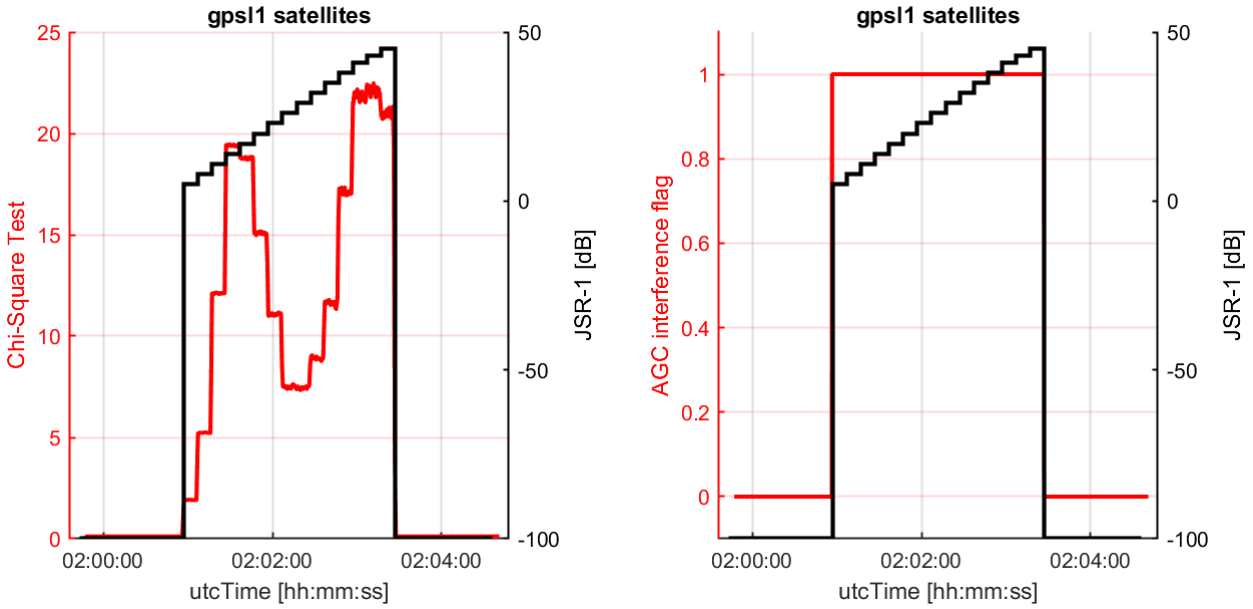


Figure 5-12 Chi-Square Test result (left) and interference detection flag (right) for GPS L1 signals in a jamming test scenario

Receiver observable-based technique, such as C/N0 monitoring based interference detection technique performed as the second-best detection technique in this outdoor simulation or live demonstration environment. The main limitation of C/N0 monitoring based technique is its sensitivity towards weak signal condition. In an operational environment where weak signal condition is expected (for example, road transportation, indoor, etc.), C/N0 monitoring based interference detection technique does not effectively work.

For **jamming mitigation**, **Multi-Frequency Multi-Constellation (MFMC) diversity** was implemented in the FGI-GSRx at the navigation stage based on Chi-Square based anomaly detection. In case of detected anomaly, the receiver flagged that signal(s) as corrupted and excluded the signal(s) from the PVT computation. It was shown that MFMC based mitigation worked very well for mitigating the impact of signal-frequency jamming. It is noteworthy that MFMC is fully reliant on the performance of jamming anomaly detection technique to decide on which GNSS signal is corrupted or not

Next figure shows an example of a test scenario in which MFMC diversity was tested.

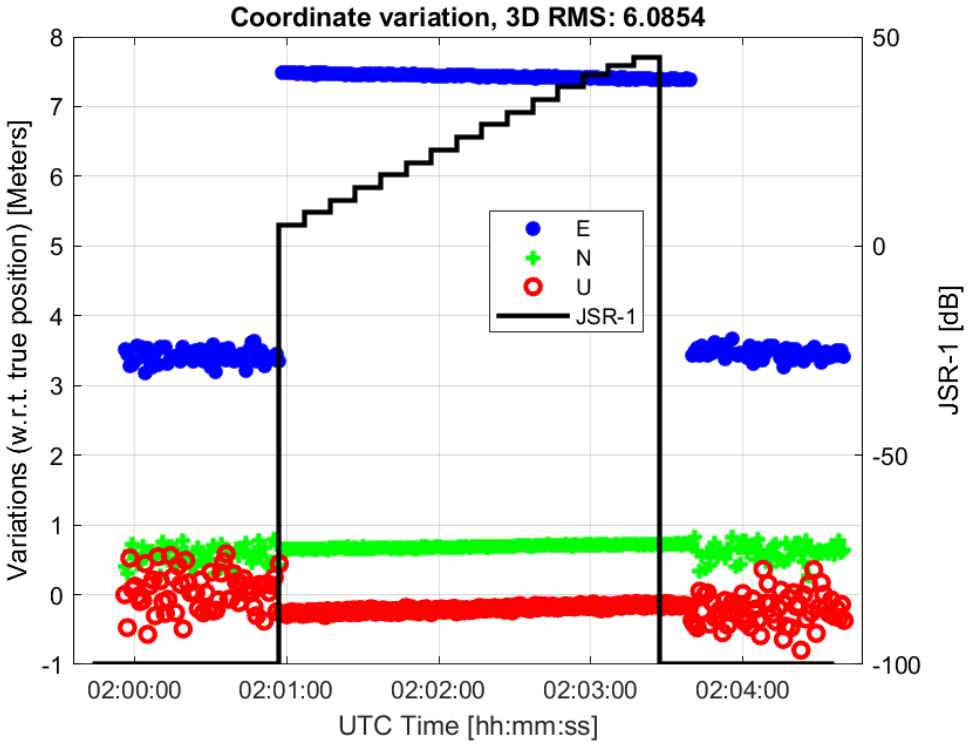


Figure 5-13 Variations of the obtained position solutions from true position using MFMC mitigation in a jamming scenario.

5.2. SPOOFING DETECTION AND MITIGATION

'Chi-Square based technique' outperformed all other techniques implemented in the FGI-GSRx for **spoofing detection** scenarios, such as **'CN/0 monitoring'**, **'Channel Quality Index (CQI)'** (a 'Correlation Peak Monitoring (CPM) technique), and **'RAIM Consistency Checks'** (CCH). This is mostly due to the fact that the power variations used in different power profiles (JSR, SSR) of the simulated and live demonstration scenarios were quite significant.

Some results of the tests performed are shown in the next figure

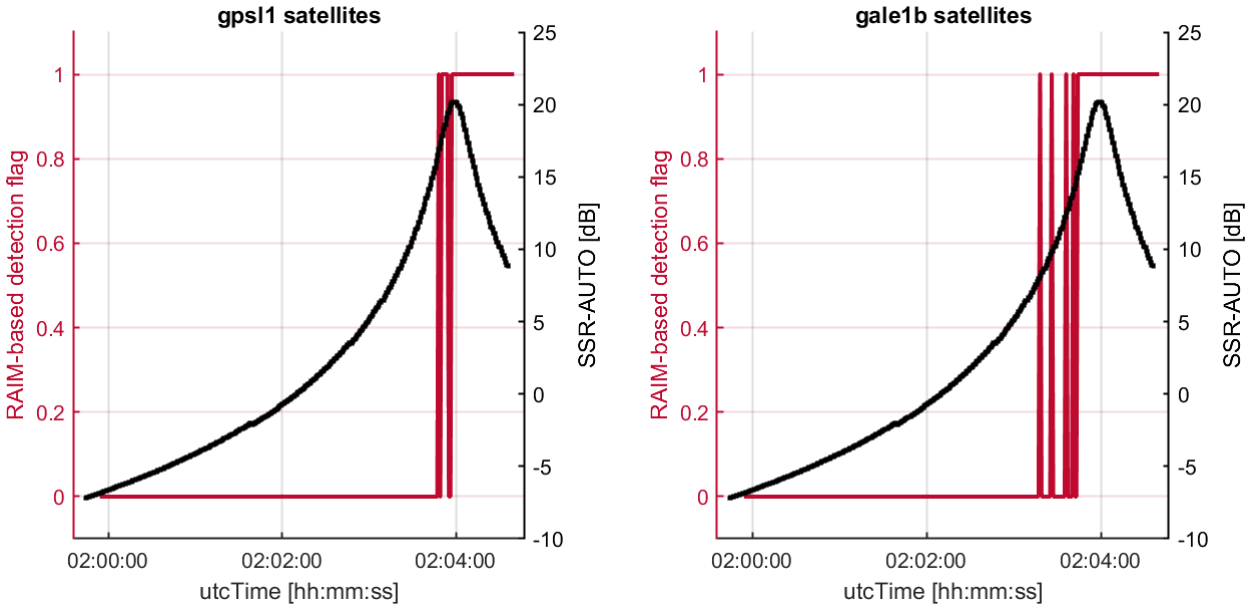


Figure 5-14 RAIM based detection flag for GPS L1 (left) and Galileo E1 (right) signals

On the other hand, the capability of an **OSNMA** receiver to **detect spoofing** was also tested. To carry out the spoofing test, a file was created by combining previously recorded live RF samples (with authentic OSNMA navigation data) with synthetic RF samples generated with a GNSS simulator emulating the same position and GNSS constellation (but without OSNMA data), thus enabling to test a synchronised and targeted spoofing attack. The obtained results show that OSNMA technique was able to detect the lack of valid OSNMA info when the spoofing attack started and how an authenticated PVT could be again provided after the spoofing attack finished.

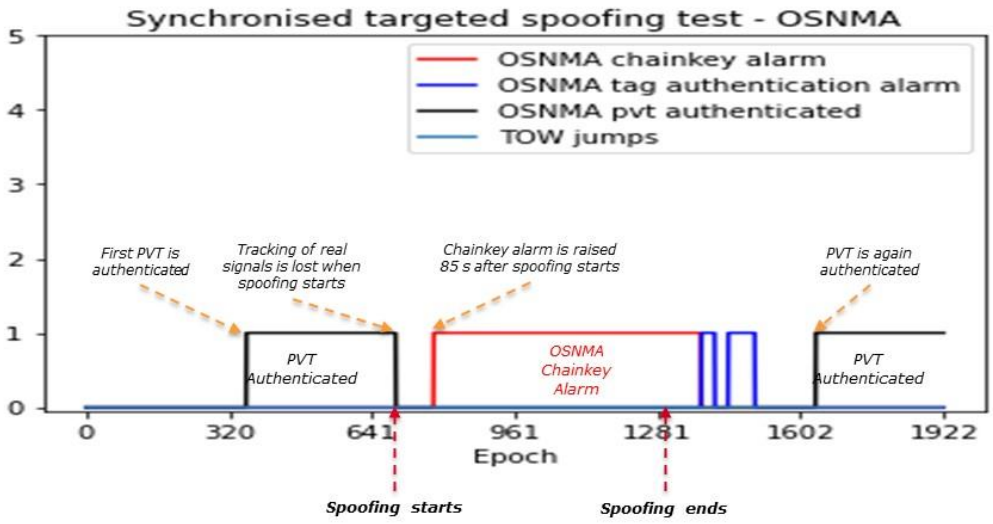


Figure 5-15 OSNMA test with a spoofing attack synchronized below 1 s

Despite the complexity of the attack, GMV's PRESENCE-OS receiver was able to correctly identify the existence of spoofing data and warn the users about the attack (see [REP14]).

Finally, it was shown that **MFMC** based mitigation worked also very well for **signal-frequency spoofing mitigation**. It is important to note here that MFMC is fully reliant on the performance of spoofing anomaly detection technique to decide on which GNSS signal is corrupted or not

5.3. DPA STUDY

A specific study has focused on a dual-polarized antenna (DPA). Such an antenna has two outputs, which separate left-hand and right-hand circular polarised signals (LHCP, RHCP) into two separate channels. GNSS signals are normally right-hand polarised by design (a feature of the antenna on the satellite). However, reflected signals will typically become left-hand polarised. Also, artificial signals such as interference or spoofing will typically have a different character: a simple antenna will produce a linear polarisation instead of a RHCP signal. The DPA antenna can therefore be used to distinguish between direct signals, reflected signals and potentially also spoofed signals or interference. Ultimately the DPA may even distinguish the elevation of the incoming signals by comparing left-hand and right-hand signals interacting with a ground plane.

For this specific study, a first characterisation of the DPA was performed on the outdoor NLR antenna test range where the antenna was mounted on a ground plane and irradiated from a distance of 160 m under various angles. The tests were successful in characterising the antenna reception pattern that is very similar to a conventional GNSS antenna reception pattern.

Next figures show some pictures of the DPA tests set-up and some of the obtained results

Figure 16: Matterwaves MAT-743GPSL1L5A-T1-RL Dual Polarization GNSS antenna

Figure 17: NLR's antenna test range (left), Ground plane and DPA on pedestal (right)

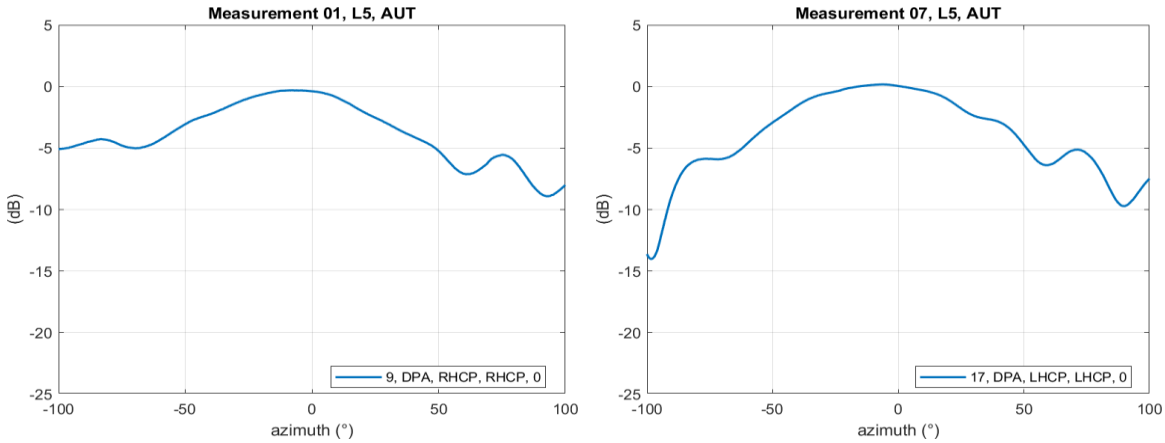


Figure 18: Co-polar radiation patterns in the RHCP (left) and LHCP (right) channels for the DPA without ground plane.

6. ANNEX B: LABORATORY ASSESSMENT OF GROUND TECHNOLOGIES

6.1. RFI MONITORING NETWORKS

Laboratory tests with COLOSSUS Detector device and DTRPRBV3 Detector device were carried out in GMVNSL. The purpose of the tests is to verify the capability of devices to detect the jamming (COLOSSUS and DTRPRBV3) and spoofing signals (COLOSSUS only) specified in the project in the controlled laboratory environment.

Four types of jamming signals – chirp in band, continuous wave, noise like and pulsed interference, were tested in six scenarios (see [REP14]).

Both the COLOSSUS unit and the DTRPRBV3 unit detected all the jamming signals above successfully in all scenarios apart from scenario for pulsed signal. Next figures show some examples of results.

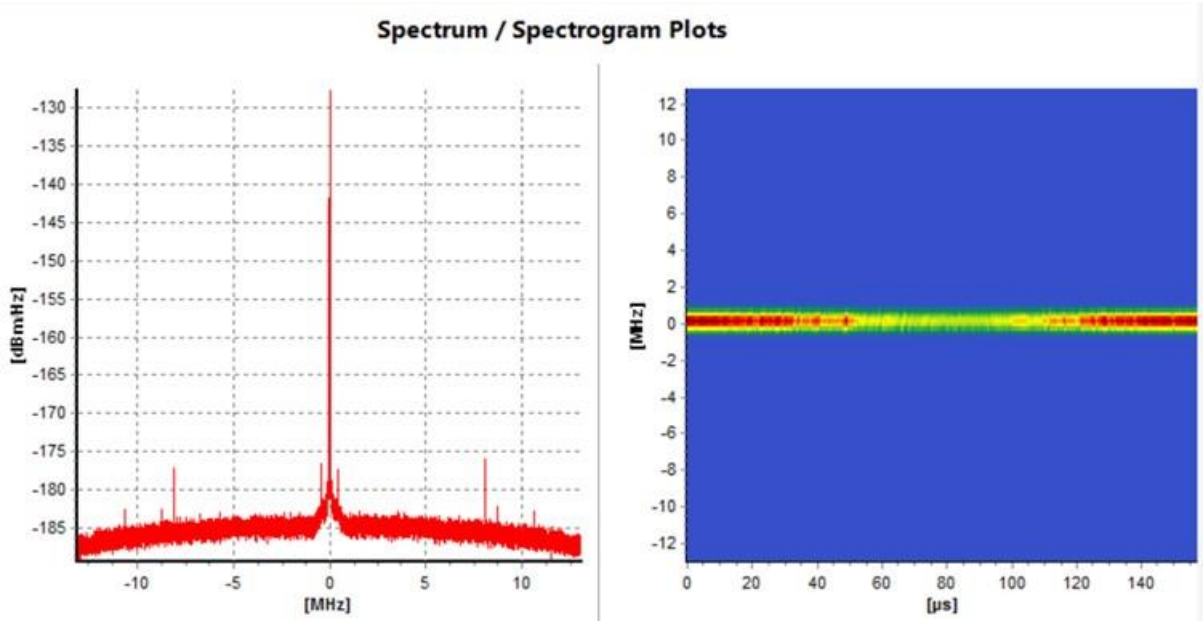


Figure 6-1 Spectrogram of an RFI event reported by COLOSSUS in one test scenario

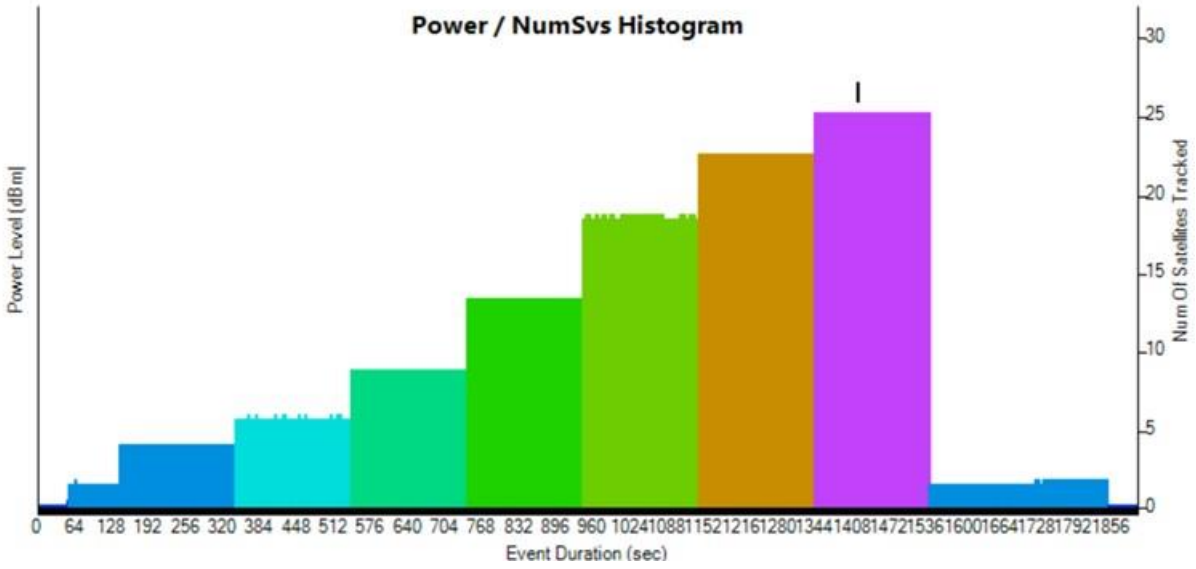


Figure 6-2 Power level of an RFI event reported by COLOSSUS in one test scenario

Both COLOSSUS unit and DTRPRBV3 unit did not detect the pulsed signal as expected, but rather it was classified as wide band noise. The reason is that the algorithm uses only 160μs of data to classify the interference, while the pulsed jamming signal in this scenario has a period of 12.5ms and duty cycle of 1%. It is the long period and the short duty cycle that caused the result of non-detection. Test results with a chirp-triangle signal which has reduced period of 30us, duty cycle 1/3 and bandwidth of 5 MHz proved this conclusion as it was successfully detected and correctly classified as pulsed interference by both devices.

In terms of spoofing tests or jamming + spoofing tests with COLOSSUS unit, no spoofing event was detected in any of the spoofing scenarios. Instead, the spoofing signal was identified as CDMA or wide band noise. By checking the recorded C/N0 by COLOSSUS unit, it was found that C/N0 values of some satellites are dropping steadily in steps with the increasing SSR profile, while the C/N0 values of some satellites are increasing in steps with the increasing JSR profile, which means the receiver inside the COLOSSUS unit tracks the spoofing signal, but because there are no PVT outputs and the COLOSSUS unit depends on the variation of the positions to detect the spoofing attack, there is no spoofing event being reported.

6.2. SURVEILLANCE-BASED SYSTEMS

The use of a surveillance-based system based on the processing of the ADS-B messages downlinked by aircraft has demonstrated that can be effective to detect when jamming is affecting an aircraft, and to localize the position of the RFI emitter on ground (by processing the ADS-B messages downlinked by multiple aircraft affected by the same jamming signal).

Next figures show some examples of the measured localization accuracy performances (see [REP14])

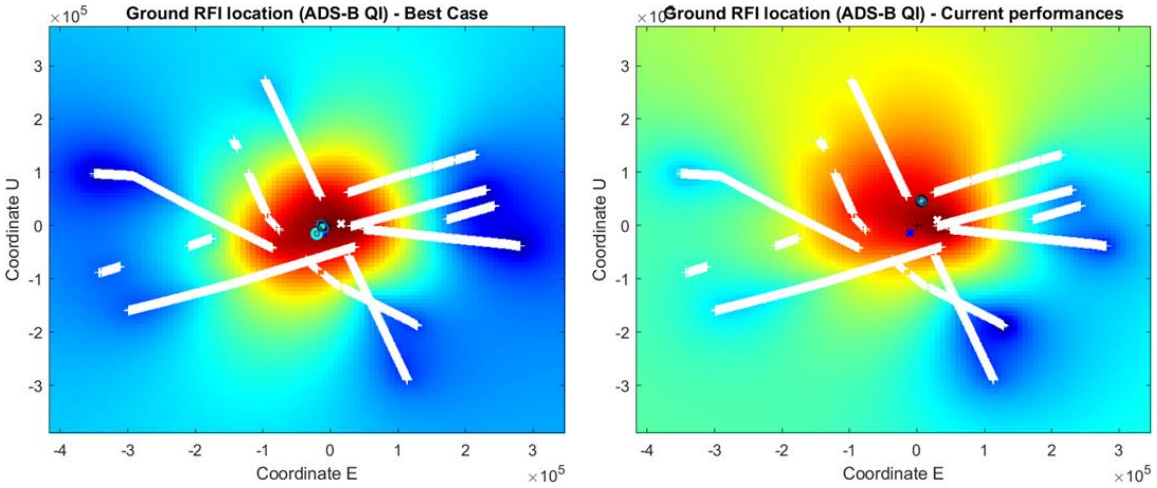


Figure 6-3 Localization heat map of a L1 RFI (capability feasible in the short-term)

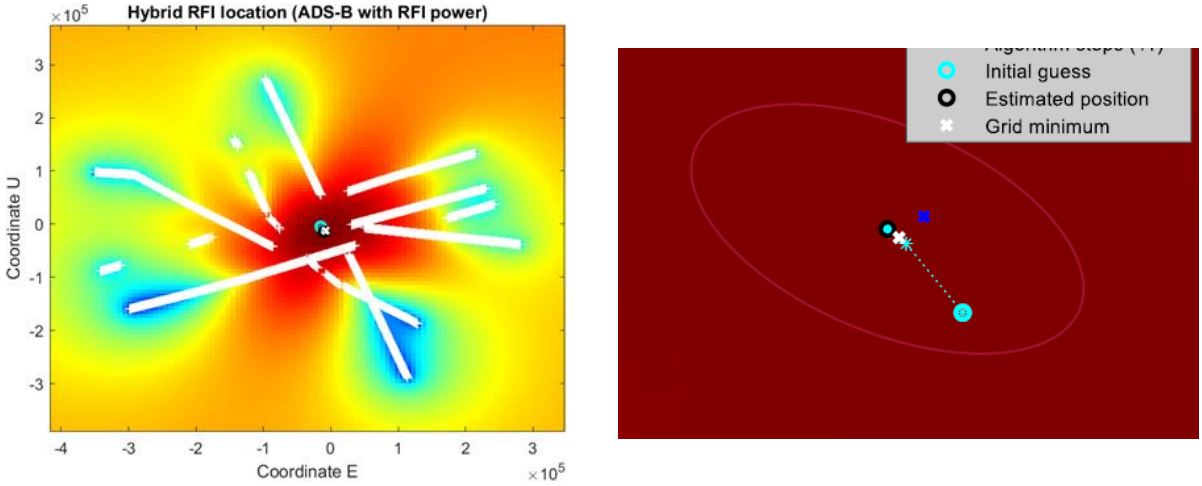


Figure 6-4 Localization heat map of a L1/L5 RFI (capability feasible in the mid-term)

More importantly, the different techniques analysed would allow the staggered implementation of this jamming detection and localization system, starting in the short term with a technique that performs both jamming detection and localization on ground (using the current ADS-B messages), and planning for the mid-term implementation of a technique (when a new ADS-B message format enables it) that assumes that jamming detection is performed on-board and that RFI localization is performed on ground

7. ANNEX C: OTHER ASSESSMENT RESULTS

7.1. OPEN FIELD TESTS

The open field tests were designed to show interference detection equipment working in real situations in the field in order to show the type of interference signals and events that occur in reality, and the sort of information that is available and that could be used for wide area monitoring. For the open field tests, two types of equipment are used: GSS100D interference monitoring units (monitoring in L1 band) and COLOSSUS Reference receivers (monitoring in L1 and L5 band).

During the AIRING project period, results are collected for 5 GSS100D units and 5 COLOSSUS units, deployed at 10 different sites (see [REP14]). Next figures show examples of the collected results

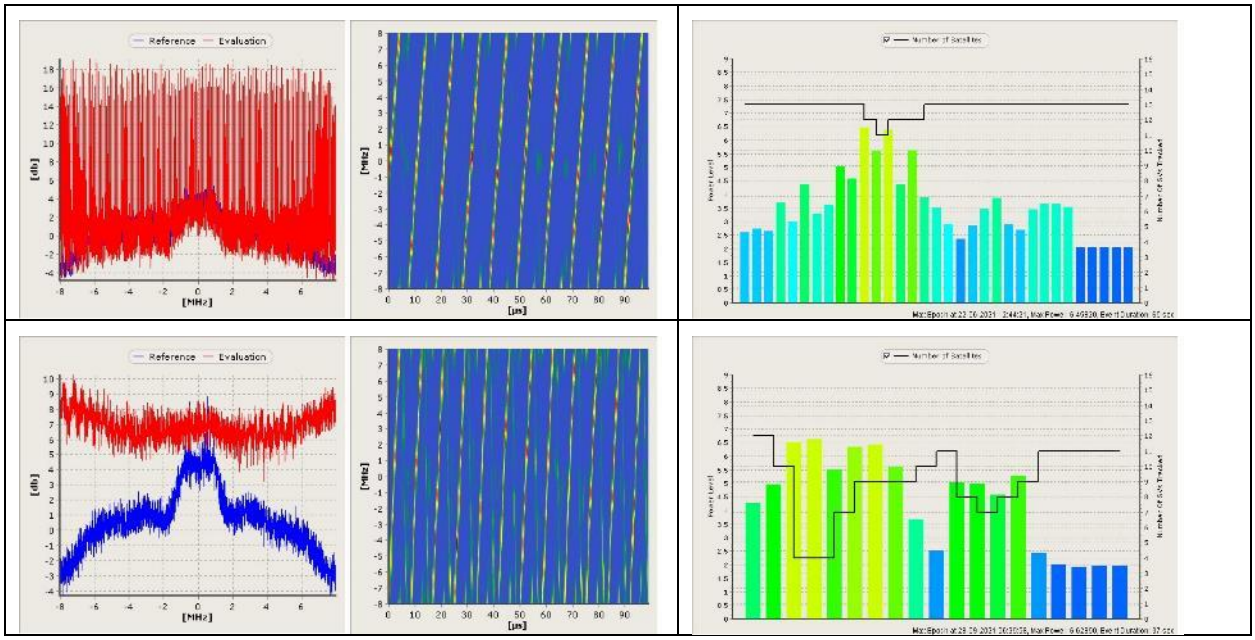


Figure 7-1: Example Events with Impact on Tracking at one site

Figure 7-2: Example breakdown of Medium and High Priority Events Detected at one site

As a summary, and with regards individual site results:

- All the sites show some interference and likely jammers
- Different sites have different levels of activity – some are very quiet, but some have many interference events per day
- The level of activity can change, and so just because a site is usually quiet does not mean this will always be the case. This means that a site survey prior to installation of some equipment is useful but continuous monitoring may still be required to detect such changes in activity, and to warn when that is the case.
- Linked to the level of activity, some sites are affected by a few types of interference signature – maybe even just a few jammers – but some detect many different types of signals, which points to a wider problem with jammers at those locations.
- The majority of events seem to be collateral jammers on L1 or perhaps high-power interference (but unintentional). However, there are some jamming signals detected on L5 as well. These are far rarer than L1 jamming signals but do point to some use of multi-band jammers.
- There is one site where there is a jamming signal that appears to be more targeted as it is the same signal on multiple days being switched on and off suddenly, rather than appearing to originate from a moving vehicle. However, without identifying the source it is difficult to know for sure if this is indeed a targeted event, and what it was targeted at.

When looking across the different sites rather than at individual sites:

- The results from multiple sites allow us to see many more different types of interference signal, which can be useful to collect information on which types are most common but also whether new ones are appearing that need to be tested for detection / mitigation performance.
- Having sites close together (within a few km) allows some protection of an area as it provides the ability to track interference events / jammers.

Finally, having a widespread network allows the detection of events that affect a wide area. One example signal in particular is detected on multiple occasions at sites that are hundreds of km apart, but the power level is relatively low, suggesting this may originate from a satellite rather than a ground-based emitter.

7.2. LIVE DEMONSTRATIONS

Several live demonstrations were performed at INTA's La Marasoña facilities (see [REP10] and [REP14]).

Figure 7-3: INTA's La Marañosa facilities

The goal of life demonstrations were twofold:

- To record RF data in different scenarios in order to assess in post-process the performances of several on-board technologies to detect and mitigate jamming and spoofing signals (Pre-Correlation Statistical detection, ANF and PB, AGC/RDS, C/N0 monitoring, CPM, and MFMC)
- To test in real-time and in different scenarios some ground solutions to detect and localize the source of a jamming signal based on RFI monitoring networks
    - GMV-NSL's Detector V3 probe units
    - ENAIRE's DYLEMA system (portable units)

The live demonstrations covered the following jamming and spoofing scenarios (jamming attacks on the L1/E1 band, and spoofing attacks on GPS L1 and Galileo E1 signals):

- To assess the on-board technologies
    - Jamming attack from a fixed location. GNSS receiver at a static location
    - Jamming attack from a fixed location. GNSS receiver mounted on a moving vehicle
    - Jamming and spoofing attack from a fixed location. GNSS receiver at a static location
- To assess the ground RFI monitoring networks

- Jamming attack from a fixed location
- Jamming attack from a RFI emitter mounted on a moving vehicle.

Next figures show some examples of the set-ups used for the live demonstrations, and some of the results obtained in the different jamming and spoofing scenarios.

Figure 7-4 RFI generation set-up (left) and vehicle and DUTs set-up (right)

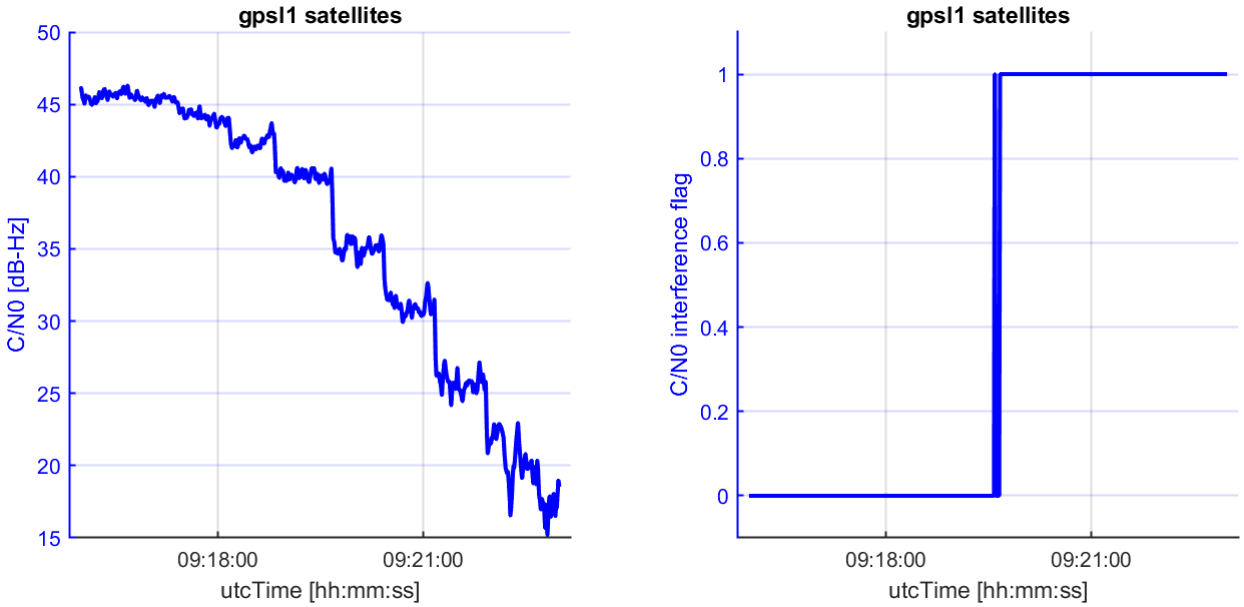


Figure 7-5 SNPR based mean C/N0 and C/N0 based detection flag (right) for GPS L1 signal

(a): Linear array connected to dual chain unit (b): U0004 unit deployed at test site

Figure 7-6 Deployed GMV-NSL's Detector test setup examples

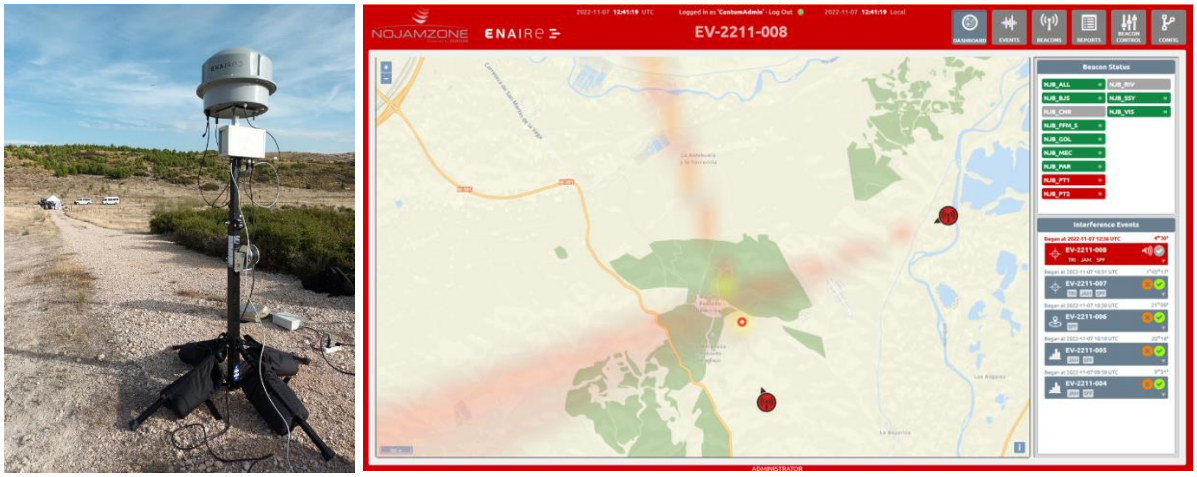


Figure 7-7 ENAIRE's DYLEMA monitoring station and HMI (successful RFI localization)

7.3. OPERATIONAL TESTS

NLR has performed an operational demonstration using its NARSIM tower radar simulator combined with its APERO cockpit simulator (see [REP14]). This demonstration was intended to showcase the impact of the technologies developed in the AIRING project on an Air Traffic Controller or a cockpit crew.

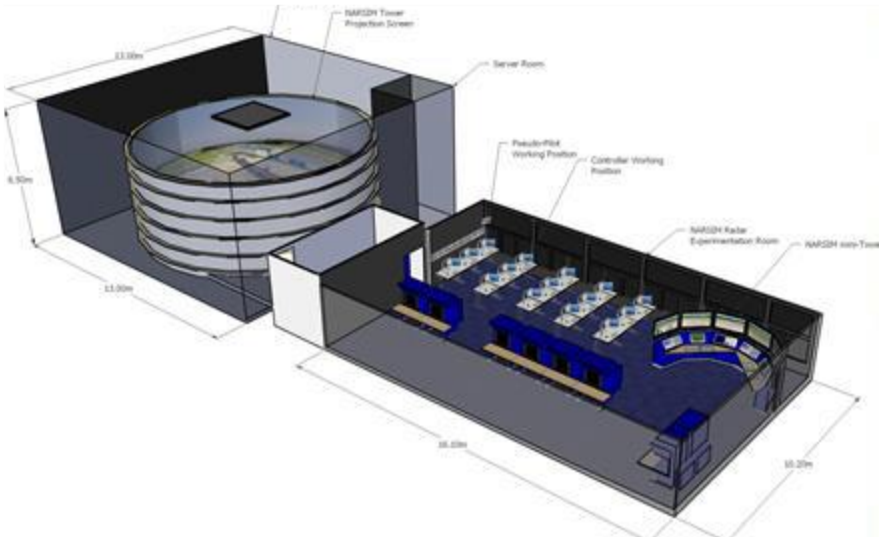


Figure 7-8 NARSIM simulator

Figure 7-9 APERO simulator

To demonstrate this impact, two scenarios were played out. In the first scenario, AIRING technology is not available and an interference source is detected by one of the approaching aircraft. The resulting impact on the ATC is significant: there is a period of uncertainty between receiving the first report of interference and having enough confirmation to decide that there is a problem. After that, the ATC switches methodology (from GNSS to radar + vectoring), and the workload for the ATC normalises. The cockpit crew was not strongly affected, as they rely mainly on the directions of the ATC which remained reliable.

The second scenario included AIRING technology, represented by a detection flag and a rough localisation of the interference source. In this scenario the workload of the ATC was significantly reduced, primarily because the window of uncertainty was reduced. The AIRING technology provides an early warning as well as a confirmation that something is wrong, which means the decision to switch guidance technology can be made quickly and reliably. After the switch, the workload returns to normal levels. For the pilots in the cockpit there was no significant difference in this scenario.

For the purpose of this AIRING demonstration an implementation of a fixed arrival and departure route system will be used, in line with the Dutch government's wish for its future operations (shift from vectoring to fixed PBN routes). The fixed arrival routes will have the RNAV1 navigation specification and will be connecting the three IAFs with the final approach path of a RNP approach. The fixed routes used for the demonstration are those currently used for the night-time operation at Schiphol. Day-time fixed arrival routes exist for Schiphol, however, are not yet ready to be published and used in projects with

external parties (i.e. non LVNL, NLR or Dutch ministry). The RNP approach will be available with LNAV/VNAV and LPV minima lines and makes use of RF legs.

Merging will be done by speed instructions, if needed a vectoring operation will be done to solve potential merging conflicts. and several air traffic controller support tools will be made available.

The arrival concept with fixed routes and PBN approach to runway 18R is detailed below:

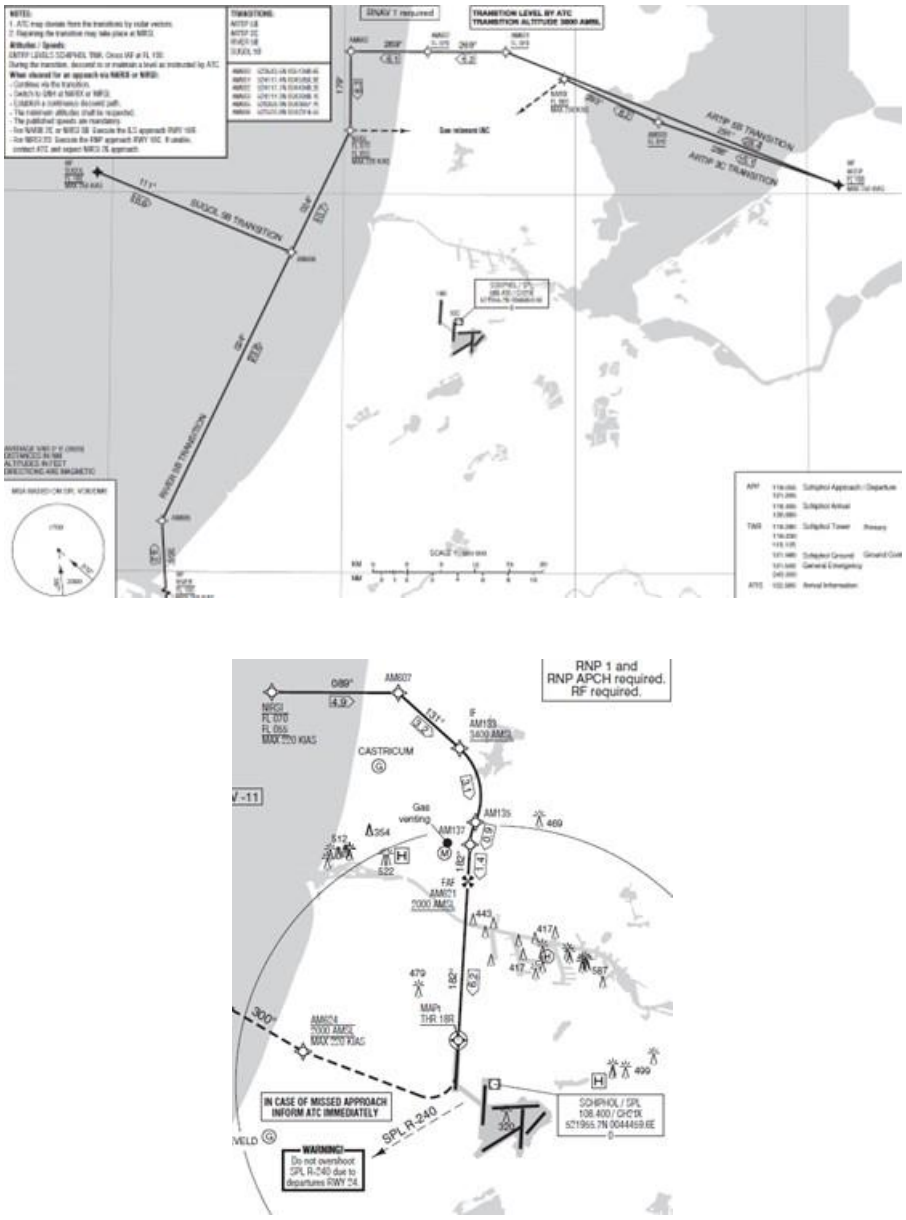


Figure 7-10 Arrival concept with fixed routes and PBN approach to runway 18R

The departure concept with fixed routes from runway 24 is detailed below (left picture for westward departure flows, right picture for eastward departure flows):

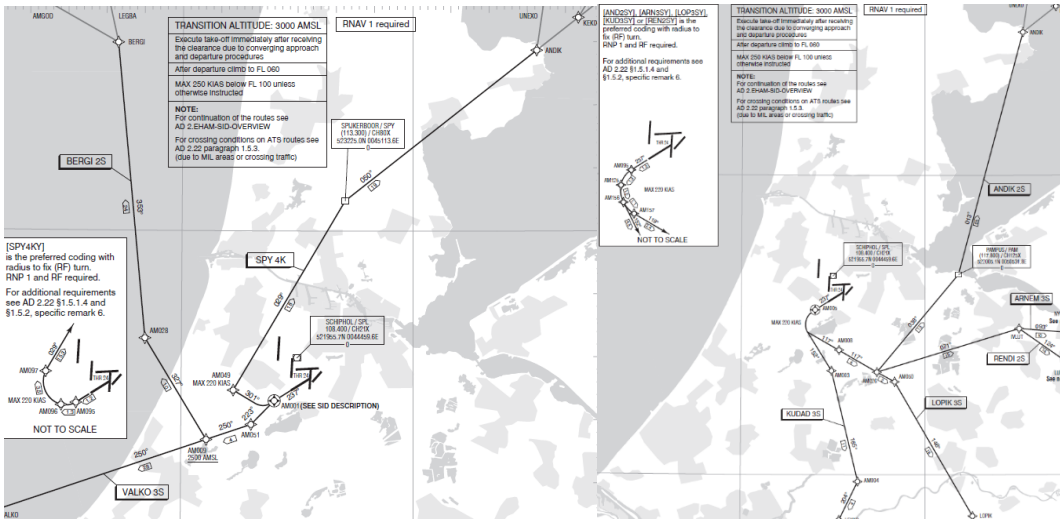


Figure 7-11 Departure concept with fixed routes from runway 24

Although the demonstration was not an in-depth assessment and validation of the AIRING concept, it did allow for some preliminary conclusions and general observations.

From the ATC side, following conclusions and observations were made:

- In general a non PBN environment leads to a higher workload. For the ATCO it is much easier to clear traffic in the normal situation on pre-defined PBN routes compared to the abnormal situation with GNSS RFI when aircraft need to be individually vectored. When using PBN approaches on fixed routes an airport can allow higher traffic loads. This volume might be challenging to handle when all flights need vectoring by ATC. However, in a busy TMA environment with GNSS unusable the vectoring of traffic remains the most optimum solution due to its flexibility and the control the ATCO has over the situation.
- The transition period between PBN and vectoring in combination with the uncertainty of the situation at hand, created a significant workload and some confusion for the ATCO.
- When operating in a PBN environment, the AIRING warnings help the ATCO significantly to increase awareness, trust in the decision making and consequently reduce his/her workload. In essence the ATCO gets positive confirmation of the situation. The ATCO has no uncertainty and does not need to check and try to confirm if there is an actual GNSS RFI event. The ATCO can anticipate much better the course of action to be taken.
- The overall confidence of the ATCO was higher with the availability of GNSS RFI warnings via the AIRING API.
- The ATCO appreciated the warning coming from the technical support officer, rather than having an AIRING interface directly accessible to the ATCO.
- The timing of the information about the GNSS event was deemed crucial. The stakeholders appreciate greatly to know when the GNSS RFI is really confirmed and when it has ended.
- The ATCO indicated that geographical information on the area affected by the GNSS RFI threat is marginally relevant. As soon as an GNSS RFI event is identified, regardless of whether the entire sector is impacted or not, the ATCO would switch all traffic to the backup means to have level playing field and to exclude further disturbances when threat would move, or other threats might start.

From the cockpit side, following conclusions and observations were made:

- The pilots indicated to have limited impact when GNSS RFI occurred in the trial. As in this busy TMA the ATCO was able to handle all traffic using vectoring. Vectoring worked well as it is currently still a common mode of operation. The switch from PBN to vectoring didn't change much for the aircrews. Which is a compliment to the ATC service. In case ATC would not be able to handle the traffic under GNSS RFI conditions the impact for aircrew might be bigger. The

pilots showed to have full confidence in the vector operation, as the surveillance solution remained intact as it is in this scenario not based on GNSS reports but on multi-lateration using transponder signals. As such the GNSS fall-out did not impact the ATCO radar image.

- The pilot appreciated having GNSS event information presented onboard the cockpit. It increases the pilots' awareness of the situation, even though the impact of the GNSS event was limited.

General conclusions:

- The current ATM system by design is already redundant and robust in a busy TMA scenario. None of the stakeholders in the demonstration experienced unacceptable workloads due to the loss of GNSS service. The mitigation procedures and fall-back technologies are the ones that are currently commonly used in today's operation. The AIRING information was perceived as most helpful from the ATC side, as just an information source from the cockpit side in this busy TMA scenario. In more remote areas the cockpit crew might appreciate the AIRING information to greater extend.

The confidence instilled by having a positive confirmation of the GNSS RFI situation makes a significant difference in the trust and focus of the stakeholders. Their line of action can be planned from the start of the warning to the end of the GNSS RFI event.

8. ANNEX D: RECOMMENDATIONS AND SUPPORT MATERIAL

Two main recommendations are provided to support the roadmap described in §4.7:

- In the short-term, **awareness and dissemination** activities (see §8.1), with the aim to:
  - Promote the implementation in the short-term of new technologies by industry (e.g. avionics and CNS systems manufacturers) by letting those actors self-assess the convenience of incorporating those techniques into their commercial systems
  - Promote the implementation of short-term technical measures by ANSPs based on the technical solutions already available in the market, as well as to promote the implementation of short-term operational measures based on the AIRING findings
- In the mid-term, **standardization and regulation** activities (see §8.2) to facilitate and drive the implementation of certain technical and operational measures

8.1. AWARENESS AND DISSEMINATION

The results of the AIRING project are positive and encouraging, however they are still far away from a change in operational procedures and equipment in civil aviation. Changes in aviation take time, primarily to ensure safety is preserved. To work toward such a change, several steps need to be taken.

The first step toward change is to inform stakeholders about the threats, possibilities and proposed technical solutions. By providing such information, awareness of the situation will increase and eventually also the acceptance of the need for change. information provision must be tuned to the target audience. The initial stakeholders to target are:

- Regulatory bodies (EASA, EC, National CAA's)
- Eurocontrol and national ANSPs
- Aircraft operators
- Aircraft manufacturer
- Supplemental type Certificate owner
- Aircraft avionics manufacturers (e.g. GNSS aviation receiver makers)
- GNSS antenna manufacturers
- Aircraft manufacturers (e.g. Airbus and Boeing, for integration of equipment in their aircraft)
- Maintenance and retrofit companies
- Flight schools and training organizations

Dissemination will be aimed at creating awareness and gaining initial acceptance and support for required change. Various possibilities exist, but the following steps are recommended:

- Share the AIRING results and the resulting future concept at relevant conferences.
- Present to EASA, Eurocontrol, national CAA's and other relevant organizations the intended concept at relevant meetings. Goal is to inform, discuss and create acceptance for the future concept.
- Present to industry the concept, future vision and timeline. Stakeholders should include aircraft manufactures, avionics manufacturers and maintenance companies, at relevant fora such as international trade shows or conferences.
- Present the concept to airlines to foster adoption. It is known that interference already hampers flights in certain areas, so obtaining their support is a valuable step toward adoption of a future new standard with associated costs. Relevant fora could be conferences or international stakeholder groups.

As a first step in dissemination, the results of the operational demonstration will be shared in April 2023 at the Combined 8th ICAO EUR PBN Consolidation Task Force and 35th EUROCONTROL Navigation Steering Group meeting in Paris. Similar venues could be used by EC to present and explain the future concept, for example the Airspace World conference.

Apart from dissemination directly toward stakeholders at conferences, EC may consider publication of (parts of) the AIRING results as relevant papers for the aviation industry. Possible candidates could include:

- Further publication of selected relevant AIRING results in scientific or technical journals. Potential candidates are ATC Network, GPS World and Inside GNSS.
- Publication of a white paper explaining the top-level problem, approach toward a solution and a presentation of EC's future vision on making aviation resilient to GNSS interference and spoofing.
- Publication of a roadmap demonstrating EC's vision toward a resilient aviation landscape and sketching the timeline when the various steps could happen in Europe or internationally.

Once the future concept is properly defined in terms of a roadmap and/or white paper defining the vision, further research will be required that will eventually lead to new standards or regulations that come into play. At this point, further dissemination will be required to create awareness and acceptance for the concrete changes in technology and regulations.

8.2. STANDARDIZATION AND REGULATION

8.2.1. ON-BOARD EQUIPMENT STANDARDS

This section identifies standards for the on-board equipment which are deemed necessary to be created/updated in order to allow incorporating findings made in scope of this project to the civil aviation.

The cornerstone for the aviation GNSS receivers' standardization is the receiver MOPS.

Some known RFI-related features to be defined in the next generation receiver standards are the on-board RFI detection functionality requirement, the recovery requirement specifying the maximum tolerable time to provide a valid navigation solution after removal of the interference, the introduction of DFMC signals to bring added resilience against GNSS vulnerabilities and the possibility to process independently each frequency.

Therefore, it is deemed crucial to finalize the requirements addressing the jamming and spoofing detection/mitigation including comprehensive testing procedures in DFMC [MOPS] ED-259 and release the standard. For instance, as reported in [REP03], the last available draft of the DFMC [MOPS] address untargeted spoofing threats but not targeted spoofing attacks (S5 and S6); it includes specific RFI detection requirements but not specific tests to verify them.

Furthermore, a better categorization of the levels of capability of the user equipment to detect and mitigate RFIs could be added to the standards. The labeling framework described in detail in [REP09] could provide some valuable ideas in that respect. On the other hand, it might be also beneficial to add examples of minimum baseline detection/mitigation techniques (or combination of the techniques) which satisfy the requirements stated for different user equipment categories.

One of the technologies which should be included in the aviation GNSS receivers to prevent spoofing of the navigation message data is the Navigation Message Authentication (NMA). Galileo provides OSNMA service and there were also plans to use SBAS L5 signals to support another service better suited for the aviation purposes. Usage of these services should be defined in ICAO SARPS and then propagated also to GNSS receiver MOPS.

Another important technology investigated in scope of AIRING project is the CRPA antenna. Although there are currently many obstacles for efficient usage of CRPA onboard the civil passenger aircraft, the results achieved with regard to the RFI detection and mitigation are very promising and to allow its usage at least in a longer-term horizon it might be beneficial to start preparing standards like antenna

MOPS specific to this type of antenna already. The same applies for possible usage of the dual polarization antennas if it proves to be efficient for the RFI detection.

Before the CRPA antenna technology is available for the civil aircrafts there is a possibility to reuse current dual antenna architecture for at least limited detection and mitigation of some RFI threats. To support standardized solution a new MOPS document should be developed and depending on the chosen solution the effects on the existing standards (ED-259, RTCA DO-384) should be investigated. Also, some additional receiver data outputs may be needed to share all parameters needed to process the direction of arrival (DOA) algorithms. Some update of ARINC 429 standard may be therefore necessary.

ARINC 429 standard might need to be updated also to support other data outputs from the GNSS receivers allowing reporting of the RFI detection (e.g. some additional measures would need to be taken to combine the data from the receivers to allow direction-of-arrival (DOA) based spoofing detection and mitigation)

8.2.2. OTHER INTERNATIONAL STANDARDS AND REGULATIONS

This section tries to identify the international standards and applicable regulation, beyond the on-board user equipment standard reviewed in 8.2.1, that should be updated to integrate the solutions developed in this project into the aviation system.

Standards and regulations

In order to reach a full V3 maturity an update of technical standards is recommended below:

- Precise guidance about the RFI reporting procedure in the GNSS Manual

  Given that the use of GNSS RFI detection, mitigation and localization systems is becoming widespread, additional guidance is advisable in ICAO GNSS Manual [Doc 9849] to describe the reporting procedure upon RFI detection including the coordination actions between the stakeholders.

  The GNSS Manual provides information about GNSS technology and operational applications to assist State regulators and ANSPs.

  Appendix F to the GNSS Manual contains the "GNSS RFI Mitigation Plan", where section 5.3.3 is devoted to the "deployment of mitigation measures". Inputs are necessary to better describe the reaction to GNSS service interruptions.

  > *5.3.3.5 Reacting to GNSS service interruptions*
  >
  > *5.3.3.5.1* ***If a GNSS service interruption due to an RFI event cannot be prevented, it must be ensured that the event is detected and stopped as quickly as possible****, especially if it has a detrimental operational impact.* ***This requires the ability to detect, identify, locate, and eliminate the RFI source.*** *Detection will be provided either by monitoring systems or by operational personnel directly. However, it may not be easy for operational personnel to establish whether a navigation service interruption is due to RFI or to other causes. Ideally, suitable systems should be deployed that do not depend on the ability of operational staff to identify such events. Nonetheless, as shown in section 2, it is important that pilots and air traffic controllers understand the potential adverse impact of RFI to GNSS and react appropriately. Effective reporting lines must also be in place to ensure that any navigation service anomaly can be investigated.* ***Technical guidance on RFI detection and localization is under preparation and will be included in Doc 8071, Volume II.***
  >
  > *5.3.3.5.2* ***Once it is positively confirmed that an RFI event has occurred, relevant airspace users and air traffic controllers should be promptly and appropriately informed****. Information relevant to the RFI cases should include, if available, the location and duration of the RFI event and related alternative operational procedures. Additionally, ANS provider engineering staff should contact the appropriate national radio regulatory and enforcement authority to resolve the RFI event. It will be helpful if as much data as possible is collected to allow the identification and classification of the RFI. Identification means association with a likely signal source in order to narrow the search space. For example, harmonic emissions from broadcast stations are a common potential source of unintentional RFI. Being able to*

identify the RFI as due to a broadcast signal and knowing the location of broadcast stations can significantly speed up the search for the signal source.

5.3.3.5.3 ***Furthermore, the signal source can also be triangulated using either an airborne or ground mobile platform****. While airborne capabilities are likely to be able to locate a source most quickly, they may also be prohibitively expensive. Consequently, the deployed countermeasures depend on the magnitude of the impact caused. In the case of smaller events such as those due to individual PPD, identification of the source through monitoring conducted over several weeks may be acceptable, whereas larger events may require specific measurement flights into the affected area. It should, however, be noted that RFI source localization by measurement flights can be more challenging because measurement flights themselves may be affected by the RFI.*

5.3.3.5.4 ***Once an RFI event has been resolved, States and/or ANS providers are encouraged to share lessons learned in corresponding aviation forums*** *(spectrum-related working groups).*

With the existing text, some aspects are not yet commonly addressed, such as the minimum duration of the RFI that should trigger a notification, or the time window for different short RFI events to be considered as a recurrent RFI event worthy of monitoring. Recommended practices should be included that address when the coordination with each stakeholder should take place or when the mitigation measures should be finished upon stop of the RFI detection.

Additionally, recommendations about when a detected RFI event should change from suspected event to confirmed event could be included. As a basic recommendation, confirmation of the real impact on the airspace users (degradation of the PVT solution of the on-board GNSS receivers) should be received before applying mitigation actions at ATS level (e.g. GNSS RFI NOTAM publication, RNP procedures cancellation, etc.).

The rationale is that low power RFI could trigger detection in the on-ground monitoring stations but not in the airspace used by the aircraft (basically around runways, airways, and SID/STAR procedures). In such cases, applying restrictions on GNSS use is not justified as it could lead to delays and capacity reduction in the air traffic, and even to safety issues. The confirmation of the "airborne impact" could be based on pilot reports to ATC via VHF voice communications or on ADS-B out messages analysed on ground in real-time or quasi-real-time (with a latency of less than 15 minutes).

Section 7.2 in [REP15] proposes a flowchart to clearly describe the stakeholders' actions based on the experience from operating a ground dedicated monitoring RFI network.

- Add RFI testing requirements in the "manual for testing of satellite-based radionavigation aids"

  ICAO [Doc 8071] volume II provides guidance on the extent of testing and inspection activities of GNSS-based procedures. The guidance is representative of practices existing in several States. A new chapter 5 on "RFI" is being proposed in the next updates to this volume to support the activities described in the GNSS RFI Mitigation Plan of the GNSS manual. Additional inputs could be provided on the "general methods for detecting and resolving interference problems", subject of section 5.4 in preparation.

- Generate technical standards for GNSS RFI detection and localization systems

  Since RFI events pose a threat to GNSS services used by the civil aviation, minimum operational performance standards (MOPS) could be defined for ground GNSS RFI detection and localization systems. The MOPS establish the basis for required performance and are useful for designers, manufacturers, installers, and users of such systems. Currently, there are joint EUROCAE and RTCA [MOPS] for DFMC GNSS (SBAS and GBAS) airborne receivers (document ED-259) which include some RFI airborne detection and mitigation capabilities but there is not yet available any similar MOPS activity (neither on going nor planned) for on ground GNSS RFI detection and localization systems.

- Standardize the interface for the automatic exchange and storage of RFI information

  This will aid to support the exchange and storage of information between stakeholders either from different organizations (ANSPs, NM, National Spectrum Agency, Airport Operators, CNS

service providers, State Security Forces) or from different units within an organization (e.g. ATC units, ATSEP and engineering staff within the ANSP).

The interface standardization has been proposed in [REP11] through a RESTful API (basically an HTTP interface that allows request of data with authentication of the users), with API web servers at each ANSP and at the NM. The API allows to notify the user with relevant RFI information in real time.

The reporting and retrieval of "GNSS RFI events" and "airspace impact" by each stakeholder should be defined by means of the API. The user access to the API web server should be protected with authentication and the user given the right to subscribe or unsubscribe to different services.

Such optional interface specification might be processed as part of the technical standards for GNSS RFI detection, mitigation, and localization systems or as a separate standard.

- Propose updates of the phraseology to report GNSS RFI events

  A phraseology update is proposed in [REP11] for the ATCO transmission in the reporting of GNSS outages or degradations due to RFI events. Slight updates are proposed depending on the information made available to ATC (whether it is based on the reports from other flights or based on other detection means). Such proposal may be processed as an amendment to ICAO PANS-ATM [Doc 4444], in section 12.3.1.14 on GNSS service status.

8.3. INDUSTRIALIZATION SUPPORT MATERIAL

This section summarizes some material elaborated in AIRING that could be used to support industrialization (note that the short-term roadmap in §4.7.1 recommends to further develop it)

8.3.1. LABELLING FRAMEWORK

To proposed **labelling framework for the on-board equipment** (i.e. GNSS receivers) has taken into account the following criteria (see [REP09]):

- Any labelling qualification should be voluntary, i.e. manufacturers of user equipment would decide whether to qualify their equipment for a labelling level or not.

  This approach means that the implementation of a labelling scheme should not necessarily affect the applicable certification standards.

- The labelling scheme should apply independently to the detection capability, the localization capability, and to the mitigation capability.

  Recall that in AIRING we are considering on-board user equipment to which both detection and mitigation capability labelling levels would apply, and ground equipment specifically designed to detect and localize RFIs and, therefore, to which only detection and localisation capability labelling levels would apply. As a matter of fact, the labelling scheme should be, ideally, the same for on-board and ground user equipment.

- The labelling scheme should address the following features of the tests to be performed:
  - RFI types than can be addressed

    We propose defining RFI types ordered by a decreasing likelihood of occurrence: the relative likelihood of the jamming RFI types could be based on collected statistics, whereas, as far as the spoofing RFIs are concerned, we can assume that the less complex the RFI generation the more likely its occurrence (so the spoofing RFI types should be ordered by an increasing complexity of the RFI generation)

    Testing a user equipment subject to a RFI could be performed in:

    - Fixed conditions (e.g. RFI power, duration of the RFI)
    - Variable conditions

- Level of performance achieved
  - When the conditions of the tests are fixed, the assessment of the user equipment should be based on complying with certain pass/fail test criteria.

    Consequently, the labelling level should be determined by the more unlikely RFI type that the user equipment is able to comply with those pass/fail criteria.

    In this case, the labelling levels should be defined, ideally, to make that one intermediate labelling level has a correspondence with what is required to certify a user equipment to the most demanding on-board equipment standards (e.g. a labelling level of 3 may mean the user equipment is able to pass the RFI tests defined in the DFMC MOPS), but defining also other lower levels to account for less performant on-board equipment or for low-end ground equipment, and higher levels to account for high-end ground equipment.
  - On the other hand, when the test conditions are variable, the assessment of the user equipment should be based on some RFIs measured in the test.

    The resultant labelling level should be based on the RFI values achieved when the user equipment is subject to the different RFI types.

    Note that this labelling scheme is more complex because it would need to assess two variables (KPI values, RFI types) at the same time. On the other hand, it would allow to provide more information on the capabilities of a user equipment.

    Furthermore, when more than one KPIs are defined (e.g. to measure the withstanding and recovery capability of a user equipment), for the sake of simplicity they should be assessed together to determine the labelling level of a user equipment.

For the definition of the RFI detection and mitigation labelling levels of a GNSS receiver we propose to follow the approach of defining a set of tests in which a user equipment is subject to RFI types ordered by descending likelihood (or by increasing generation complexity for the spoofing RFIs), compute some KPIs in each of those tests, and then define a labelling level of the form XYa.b, where "X" refers to the capability assessed (i.e. either "D" for detection or "M" for mitigation), "Y" refers to the type of RFI (i.e. either "J" for jamming and "S" for spoofing), "a" refers to the more unlikely RFI type that the user equipment is able to address (i.e. the user equipment achieves at least the minimum KPIs value ranges for this RFI type as well as for all the preceding more likely RFI types), and "b" refers to the maximum KPIs value ranges that the user equipment is able to reach when subject to each of those RFI types.

Next figure presents an example to illustrate the concept, in which 5 "a" categories (each comprising several RFI types) and 4 "b" categories (assessing two KPIs at the same time) are defined, and which yields a labelling level of XY3.2.

		"b category"				
		1	2	3	4	5
"a" category	RFI type	k1.1 ≤ KPI-1 < k1.2 k2.1 ≤ KPI-2 < k2.2	k1.2 ≤ KPI-1 < k1.3 k2.2 ≤ KPI-2 < k2.3	k1.3 ≤ KPI-1 < k1.4 k2.3 ≤ KPI-2 < k2.4	k1.4 ≤ KPI-1 < k1.5 k2.4 ≤ KPI-2 < k2.5	k1.5 ≤ KPI-1 k2.5 ≤ KPI-2
1	RFI type #1					
	RFI type #2					
	RFI type #3					
	RFI type #4					
2	RFI type #5					
	RFI type #6					
	RFI type #7					
3	RFI type #8					
	RFI type #9					
	RFI type #10					
4	RFI type #11					
	RFI type #12					
5	RFI type #13					
	RFI type #14					
	The user equipment satisifies these KPIs value ranges when subject to this RFI type					
	The user equipment does NOT satisify these KPIs value ranges when subject to this RFI type					

Labelling level = XY3.2

Figure 8-1: Example of the proposed GNSS receiver labelling concept

Note that the table above could be defined in such a way that a user equipment certified against the DFMC MOPS could attain a given labelling level (e.g. DJ3.3, DS3.3, etc.)

Some clarifications about the table above are worthy:

- In all the levels of the "b category" (from 1 to 5) the same set of KPIs would be used to assess the level attained. One or several KPIs could be used (in the example, two KPIs are shown, KPI-1 and KPI-2). For each level of the "b category" a range of values must be defined for each of the KPIs to be assessed. The upper range of any KPI in one category must coincide with the lower range of that KPI in the next category.
- To declare that a certain "b category" level has been achieved for a given RFI type that belongs to a specific "a category" (a "green box" in the table above), all the defined KPIs in the "b category" must comply with their defined ranges for that level
- To identify the labelling level "a.b" for a certain capability and RFI threat (3.2 in the example above), one must find the combinations of "a category" and "b category" in which all the cells of their intersection in the table above are compliant (in the example above: 1.1, 1.2, 1.3, 2.1, 2.2, 2.3, 3.1 and 3.2), chose the combinations with the highest "a category" (3.1 and 3.2), and then pick the combination with the highest "b category" (3.2)

  This method priorities the capability of a user equipment to address more types of RFIs, rather than increasing the capability of the equipment to address fewer RFI types

To assess the jamming and spoofing detection and mitigation capabilities (i.e. to assess the "b" category) we propose to use, at least, the following KPIs:

Table 8-1: Minimum set of KPIs to assess RFI detection and mitigation capabilities

	Detection	Mitigation	
		Withholding	Recovery
Jamming	• Minimum JSR (at the Rx port) above which the RFI is detected	• Maximum JSR up to which the PVT performances stay nominal • Maximum JSR up to which the PVT is usable (including the compliance with the integrity requirements)	• TTRP (with integrity)

	Detection	Mitigation	
		Withholding	Recovery
Spoofing	• Minimum SSR (at the Rx port) above which the RFI is detected	• Maximum SSR up to which the PVT performances stay nominal • Maximum SSR up to which the PVT is usable (including the compliance with the integrity requirements) and only true GNSS signals are used to compute the PVT	• TTRP (with integrity)

Regarding the RFI types (or RFI scenarios) that should be considered to define the tests to assess the jamming and spoofing detection and mitigation capabilities, it is not the goal of this document to define a detailed list, but to identify the features of the RFI scenarios that should considered.

So, to define the jamming RFI scenarios, the following features are proposed:

- To generate a jamming RFI in L1 and/or L5 bands
- To use a jamming RFI with different waveform and characteristics (e.g. those defined in sections 5.3.5, 5.3.6.1 to 5.3.6.6, and 5.3.7 of the DFMC MOPS)
- To use a jamming RFI that follows different JSR time-profiles (e.g. with different duration)

Regarding the spoofing RFI scenarios, the following features are proposed (the scenarios defined in sections 5.3.6.7 to 5.3.6.8 of the DFMC MOPS could be taken as a starting point):

- To generate a spoofing RFI in one or several GNSS signals (e.g. GPS L1/L5, Galileo E1/E5a)
- To generate a spoofing RFI with similar or different CN0s as the true GNSS signal
- To generate a spoofing RFI with the same or different almanac as the true GNSS signal
- To generate a spoofing RFI aligned or not in time with the true GNSS signals (e.g. with different time differences, either forward or backwards)
- To generate a spoofing RFI aligned or not in with the position of the GNSS receiver (e.g. with different initial position errors)

Though the detailed definition of "a category" and "b category" levels for the detection and mitigation capabilities of a user equipment to address jamming and spoofing threats is out of the scope of this document, next table shows how the generic GNSS receiver labelling concept of Figure 9-2 could be applied, as an example, to the jamming mitigation capability of a user equipment taking into account the KPIs proposed in Table 8-1, where:

- KPI-1 = Maximum JSR up to which the PVT performances stay nominal (JSR-N)
- KPI-2 = Maximum JSR up to which the PVT is usable (JSR-U)
- KPI-3 = TTRP (with integrity)

		"b category"				
		1	2	3	4	5
"a" category	JAMMING type	k1.1 ≤ JSR-N < k1.2 k2.1 ≤ JSR-U < k2.2 k3.2 < TTRP ≤ k3.1	k1.2 ≤ JSR-N < k1.3 k2.2 ≤ JSR-U < k2.3 k3.3 < TTRP ≤ k3.2	k1.3 ≤ JSR-N < k1.4 k2.3 ≤ JSR-U < k2.4 k3.4 < TTRP ≤ k3.3	k1.4 ≤ JSR-N < k1.5 k2.4 ≤ JSR-U < k2.5 k3.5 < TTRP ≤ k3.4	k1.5 ≤ JSR-N k2.5 ≤ JSR-U TTRP ≤ k3.5
1	JAM type #1					
	JAM type #2					
	JAM type #3					
	JAM type #4					
2	JAM type #5					
	JAM type #6					
	JAM type #7					
3	JAM type #8					
	JAM type #9					
	JAM type #10					
4	JAM type #11					
	JAM type #12					
5	JAM type #13					
	JAM type #14					

Figure 8-2: Example of the GNSS receiver labelling concept applied to jamming mitigation

This section describes the GNSS **labelling concept** that would be applicable to the **ground equipment** specifically designed to detect RFI threats and, optionally, also locate the source of the RFI.

That is, the ground equipment considered here are those that form part of ground RFI monitoring stations (or networks), but not the GNSS receivers that are used for other purposes (e.g. to provide PVT to a ground vehicle, to provide a timing signal to CNS, or to be part of a GBAS, RIMS or GSS station)

The labelling concept proposed previously in this section for on-board user equipment could also be applied to those other ground GNSS receivers.

The same generic GNSS receiver labelling concept proposed for on-board user equipment to assess its detection capabilities could be applied to characterize ground user equipment (i.e. same "a category" levels, same RFI types, same "b category" levels, same KPIs and same KPI ranges in each level).

Thus, the only additional information to be defined to describe the GNSS labelling concept for ground equipment is the KPIs to characterize the RFI source location performances of the equipment.

For the sake of completeness, next table describes the KPIs proposed for detection and localization

Table 8-2: Minimum set of KPIs to assess RFI detection and location capabilities

	Detection	Location
Jamming	• Minimum JSR (at the Rx port) above which the RFI is detected	• Horizontal accuracy (95%) of the RFI source location
Spoofing	• Minimum SSR (at the Rx port) above which the RFI is detected	• Horizontal accuracy (95%) of the RFI source location

8.3.2. INTEROPERABILITY TECHNICAL SPECIFICATIONS

Though not described in this document, [REP06] includes a description of the following proposed minimum set of requirements (as a reference for the industrialization of the proposed technologies)

- For on-board GNSS receivers
  - Minimum set of RFI detection requirements
  - Minimum set of RFI mitigation requirements
- For ground RFI monitoring networks
  - Minimum set of RFI detection and localization requirements
- For surveillance data processing systems
  - Minimum set of RFI detection and localization requirements