EUROCONTROL Guidelines on a Process for Civil and Military GNSS Interference Testing

Edition: 2.0
Edition date: 6-March-2023
Reference nr: EUROCONTROL-GUID-190
ISBN: 978-2-87497-120-4

EUROCONTROL

EUROCONTROL Guidelines on a Process for Civil and Military GNSS Interference Testing

DOCUMENT IDENTIFIER: EUROCONTROL - GUID - 190

Edition Number	**:**	**2.0**
Edition Date	**:**	**6 March 2023**
Status	**:**	**Released Issue**
Intended for	**:**	**General Public**
Category	**:**	**EUROCONTROL Guidelines**

DOCUMENT CHARACTERISTICS

TITLE		
EUROCONTROL Guidelines on a Process for Civil and Military GNSS Interference Testing		
	Publication Reference:	GUID - 190
	ISBN Number:	978-2-87497-120-4
Document identifier	**Edition Number:**	2.0
EUROCONTROL - GUID - 190	**Edition Date:**	6 March 2023

Abstract

This document describes a process for the planning, notification and execution of GNSS interference testing performed by state authorised organisations. It takes into account international standards, regulations, civil-military coordination and best practices.
The process recommends an initial impact assessment to be coordinated with civil and military authorities as well as service providers before its approval and notification to airspace users.

Keywords

GNSS	Interference Testing	Process	NOTAM
Civil-Military	Coordination		ANSP
National Security Entity	Radio Regulators	CAA	MoD

Contact Person(s)	E-mail
Hamdi NASSER Ricardo OLIVEIRA Bart VAN DEN EINDEN Gerhard BERZ	standardisation@eurocontrol.int

STATUS, AUDIENCE AND ACCESSIBILITY					
Status		**Intended for**		**Accessible via**	
Working Draft	☐	General Public	☒	Intranet	☐
Draft	☐	EUROCONTROL	☐	Extranet	☐
Proposed issue	☐	Restricted	☐	Internet (www.eurocontrol.int)	☒
Released issue	☒				

DOCUMENT APPROVAL

AUTHORITY	NAME AND SIGNATURE	DATE
Director General	 Raúl MEDINA CABALLERO	06 MAR 2023

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
1.0	17/09/2021	First version of the document	All
2.0	06/03/2023	Clarification on the scope of the process affecting civil and military	Title
		Consideration of the comments received from stakeholders (ARIA, NSG, CNS FG)	All
		Expansion of the scope to include for any state authorised RFI activities by defining the 'national security entity'	1.3
		Review of the impact assessment prior to GNSS interference testing	2.1.1
		Introduction of other notification means to impacted airspace users (AIP SUP, AIC)	2.2.1.3, 2.2.1.4
		Introduction of spoofing	2.1.1
		Introduction of danger and restricted areas	2.1.1, 2.2.1.2, 2.3.2
		Annex B – review of ITU-R references	

CONTENTS

DOCUMENT CHARACTERISTICS 2
DOCUMENT APPROVAL 3
DOCUMENT CHANGE RECORD 4
CONTENTS 5
EXECUTIVE SUMMARY 6
1 Introduction 7
1.1 Purpose of the document 7
1.2 Scope of the document 7
1.3 Applicability 8
1.4 Conventions 8
1.5 Maintenance of the Specification 9
1.6 Target audience 9
1.7 Abbreviations 9
1.8 Definitions 11
1.9 Reference material 12
1.10 Document structure 13
2 GNSS interference testing process 14
2.1 Planning of GNSS interference testing 15
2.1.1 Impact Assessment 15
2.1.2 Approval Process 18
2.1.3 Coordination of the GNSS Interference 20
2.2 GNSS Interference testing notification 21
2.2.1 AIS 21
2.2.2 Reporting to the Network Manager 27
2.2.3 Notification to other impacted GNSS users 27
2.3 GNSS interference testing execution 27
2.3.1 Airspace users 27
2.3.2 ANSPs 28
Annex A - GNSS receivers and antennas characteristics 30
Annex B - ITU Radio Regulations - interference 35
Annex C - Joint Restricted Frequency List 37
Annex D - GNSS user support centres 38
Annex E - Document update procedures 39

EXECUTIVE SUMMARY

Civil and military entities conduct Global Navigation Satellite System (GNSS) receiver performance tests in peacetime to verify the resilience and behaviour of the tested systems against jamming and spoofing. To improve their readiness to operate in a degraded environment or in the event of total loss of GNSS signal in space, civil and military GNSS interference testing might need to be conducted by applying GNSS jamming or spoofing techniques.

Such GNSS interference testing can have an adverse impact on many user segments (aviation, maritime, or terrestrial). Therefore, uncoordinated GNSS interference testing activities might seriously impact aviation as well as other sectors of activity relying on GNSS as a positioning and/or timing source (e.g. railway, sea transport, power grids, mobile telecommunications, etc) especially if those testing activities go beyond their intended geographical scope. Therefore, such tests require prior risk analysis, coordination with all involved parties, and compliance with national regulations and procedures.

Regarding aviation, most civilian aircraft in operation are Global Positioning System (GPS) equipped. GNSS provides a positioning and timing solution which is not only used for navigation, but also for aeronautical communication and surveillance applications. Therefore, GNSS interference testing activities need to be well planned, reported and executed to avoid placing aeronautical GNSS users in a hazardous environment which would impact the safety of operations.

This document describes a process on the planning, notification and execution of GNSS interference testing activities, to minimise their impact on aviation. The process has been developed based on international standards, regulations, existing civil-military coordination arrangements, and best practices, and is dependent on the geographic scope of the GNSS interference tests:

- Within national borders;
- Cross border(s);
- High seas.

This document may be applied by any state authorised entity performing GNSS interference tests, such as military, police or customs.

1 Introduction

Regulation (EU) 2018/1048 of 18 July 2018 (PBN-IR) [RD 19] requires a transition towards the exclusive use of Performance Based Navigation (PBN) as the nominal mode of operation in all phases of flight by June 2030. GNSS is the primary enabler for PBN applications and is therefore becoming an essential technology used in air navigation systems.

Despite its proven benefits, GNSS is vulnerable to radio frequency interference (RFI) which can be either intentional or unintentional. Unintentional interference to GNSS signals could arise from several sources such as Very High Frequency (VHF) communications, television signals, cell towers, radars, mobile satellite communications, military systems, microwave links, GNSS repeaters or certain systems on board the aircraft [RD 9].

Based on operational reports from pilots relating to GPS outages, a variety of subsequent effects on avionics and displays have been observed [RD 5]. The analysis of the reported cases[1] starting 2014 of GNSS interference reveals that a significant number are likely caused by intentional interference sources. In absence of alternative means of CNS, GNSS interference may lead to hazardous situations impacting the safety of flight operations.

Any GNSS jamming and/or spoofing activities, whether they originate or not from conflict areas [RD 16] and that impact non-conflict areas, are considered in this document as a GNSS interference testing activity. Coordination between national security and civil authorities is essential to mitigate the impact of GNSS interference testing on flight operations of civil and military aircraft.

This document describes a process to support national security organisations in performing any State authorised GNSS jamming and/or spoofing activities based on international standards, regulations, existing civil-military coordination arrangements and best practices.

1.1 Purpose of the document

The purpose of this document is to describe a process for the planning, notification and execution of GNSS interference testing for the harmonization of procedures among EUROCONTROL Member States.

For such purpose, three cases of GNSS interference testing are taken into account:

- Within national borders;
- Cross borders;
- High seas.

The sharing of best practices among States facilitates and ensures that the potential impact of GNSS interference testing on the safety of flights is minimised or mitigated.

1.2 Scope of the document

This document addresses the impact of GNSS interference testing on aviation. It considers the roles of the various civil and national security authorities as well as ANSPs in assessing, approving, coordinating and notifying GNSS interference tests. The document also considers the role of airspace users and ANSPs and the operational aspects during the execution of GNSS interference testing.

[1] The reports are filed through EUROCONTROL Voluntary ATM reporting System (EVAIR). [RD 1] and [RD 11] also highlight the increase of GNSS interference reporting.

The impact of GNSS interference testing on other user segments (e.g. maritime, terrestrial) is not addressed in this document as they should be alerted through the GNSS users support services (the European GNSS Service Centre (GSC) for GALILEO users, the Navigation Center of the US Department of Homeland Security (NAVCEN) for GPS users - see Annex D, the GLONASS user support centre for GLONASS users and any other appropriate national procedures).

1.3 Applicability

These guidelines are intended to be used by national security organisations performing GNSS interference testing. The below listed entities are part of the process described in these guidelines. However, their involvement may vary depending on the state and national arrangements.

- The national security entity planning and executing the GNSS interference testing activity (e.g. military organisations, police, customs, etc);
- The Ministry of Defence (MoD) or the National security authority as the organisation with authority over the entity owner of the GNSS interference testing activity;
- Military Aviation Authority (MAA) who is consulted as the competent authority for military aviation;
- Civil Aviation Authority (CAA) who is consulted as the competent authority for civil aviation;
- Air Navigation Service Provider(s) (ANSPs) with whom the testing needs to be consulted and coordinated;
- Airspace users and airport operators who need to be notified of the tests;
- National Radio Regulator as the national competent authority approving the use and/or licensing of radio frequencies;
- National frequency manager who is required to report interference cases to the Network Manager (for States subject to SES regulations);
- The GNSS service centres who need to be notified of the tests.

This document may be applied by any state authorised entity performing GNSS interference tests, such as military, police, customs or private organizations performing RFI tests in outdoor facilities.

1.4 Conventions

EUROCONTROL guidelines, as defined in EUROCONTROL Regulatory and Advisory Framework (ERAF), are advisory materials and contain:

“Any information or provisions for physical characteristic, configuration, material, performance, personnel or procedure, the use of which is recognised as contributing to the establishment and operation of safe and efficient systems and services related to ATM in the EUROCONTROL Member States.”

In addition, EUROCONTROL Regulatory and Advisory Framework specifies that:

“EUROCONTROL Guidelines may be used, inter alia, to support implementation and operation of ATM systems and services, and to:

- complement EUROCONTROL Rules and Specifications;
- complement ICAO Recommended Practices and Procedures;
- complement EC legislation;
- indicate harmonisation targets for ATM Procedures;

- encourage the application of best practice;
- provide detailed procedural information."

Therefore, the application of EUROCONTROL guidelines document is not mandatory.

The specific guidance material developed for the purpose of this document is identifiable by the prefix **GNSSTEST-GMx**, where **x** is a numerical value.

The operative verb "should" indicates that they are recommended to achieve the best possible implementation of this guidance material.

Referenced documents are listed in section 1.9 and are crossed-referenced by their label **[RD x]**, where **x** is a numerical value.

1.5 Maintenance of the Specification

This EUROCONTROL Guidelines document has been developed under the EUROCONTROL Regulatory and Advisory Framework (ERAF) and is maintained by EUROCONTROL in accordance with this Framework and in line with the EUROCONTROL Standards Development Procedures. The procedures are described in detail in Annex E.

1.6 Target audience

The target audience for this specification includes, but is not limited to:

- National security organisations including military organisations/units
- Ministries of Defence (MoD) or Ministries of national security
- Military Aviation Authorities (MAA)
- Civil Aviation Authorities (CAA)
- Air navigation service provider(s) (ANSPs)
- Airspace users and Airport operators
- National radio regulators
- National frequency manager[2] as appointed for the network functions regulation [RD 14]

1.7 Abbreviations

Abbreviation	Description
ADS-B	Automatic Dependant Surveillance - Broadcast
ADS-C	Automatic Dependant Surveillance - Contract
ACARS	Aircraft Communications, Addressing and Reporting System
AIC	Aeronautical Information Circular
AIP SUP	Aeronautical Information Publication Supplement
AIS	Aeronautical Information Services
AHRS	Attitude and Heading Reference System
ARIA	Aeronautical Radio Interferences Analysis group
ATC	Air Traffic Control
ATCO	Air Traffic Control Officer

[2] In some states, the national frequency manager is only in charge of aviation frequency matters.

ANSP	Air Navigation Service Provider
ATM	Air Traffic Management
CAA	Civil Aviation Authority
CNS	Communication Navigation Surveillance
CPDLC	Controller Pilot Data Link Communications
EASA	European Union Aviation Safety Agency
EFVS	Enhanced Flight Vision System
EGPWS	Enhanced Ground Proximity Warning System
EIRP	Effective Isotropic Radiated Power
FG	Focus Group
FIR	Flight Information Region
FL	Flight Level
FSPL	Free Space Path Loss
GBAS	Ground Based Augmentation System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSC	European GNSS Service Centre
HF	High Frequency
ICAO	International Civil Aviation Organization
ILS	Instrument Landing System
IR	Implementation Rule
IRS	Inertial Reference System
ITU	International Telecommunication Union
ITU-R	ITU Regulations
ITU RR	ITU Radio Regulations
JRFL	Joint Restricted Frequency List
LPV	Localizer Performance with Vertical guidance
MAA	Military Aviation Authority
MoD	Ministry of Defence
NATO	North Atlantic Treaty Organization
NAVCEN	Navigation Center of the US department of homeland security
NOK	Not OK
PBN	Performance-Based Navigation
PNT	Position Navigation Timing

RFI	Radio Frequency Interference
RNSS	Radio Navigation Satellite Services
SARPS	ICAO Standards and Recommended Practices
SES	Single European Sky
SVS	Synthetic Vision System
TAWS	Terrain Avoidance and Warning System
VHF	Very High Frequency

1.8 Definitions

The below definitions relevant to GNSS interference testing are applied by this document.

Term	Definition
GNSS interference testing	Any state authorised GNSS frequency/frequencies jamming and/or spoofing activity that causes a degradation or an unavailability of the GNSS service in a non-conflict area.
Approving Authority	Depending on the country, the approving authority can be the national radio regulator, or another entity designated by the state as the approving authority of GNSS interference testing.
National Security Entity	Any state authorised entity planning and executing a GNSS interference testing activity, such as military organisations, police, customs, etc.
Restricted area	An airspace of defined dimensions, above the land areas or territorial waters of a State, within which the flight of aircraft is restricted in accordance with specific conditions.
Danger area	An airspace of defined dimensions within which activities dangerous to the flight of aircraft may exist at specified times [RD 20] .
GNSS MAY BE UNUSABLE	The on-board GNSS receiver may not be able to provide a usable PNT solution due to jamming within the specified area.
GNSS MAY BE MISLEADING	The on-board GNSS receiver may output incorrect PNT information based on unauthentic GNSS signals (spoofing signals) transmitted within the specified area.
NOTAM	Notice distributed by means of telecommunication containing information concerning the establishment, condition or change in any aeronautical facility, service, procedure or hazard, the timely knowledge of which is essential to personnel concerned with flight operations
ANSP	The term ANSP refers to the entity responsible for the provision ATM and/or other air navigation services which includes communications, navigation and surveillance systems (CNS), meteorological services for air navigation (MET), search and rescue (SAR) and aeronautical information

	services/aeronautical information management (AIS/AIM) [RD 20] . For the purpose of these guidelines, an ANSP can be civil or a military entity.

1.9 Reference material

[RD 1] ICAO. Assembly – 41st Session Technical Commission, Agenda Item 31: improving communication navigation and surveillance (CNS) resilience through global navigation satellite system (GNSS) interference mitigation. 28/7/2022.

[RD 2] US Department of Homeland Security. GPS Interference Test Approval Process, International Committee on GNSS. 2/12/2017.

[RD 3] ICAO. Annex 10, Volume I, Aeronautical Telecommunications, Radio navigation Aids, Seventh Edition, July 2018.

[RD 4] EUROCONTROL. Guidelines Operating Procedures for AIS Dynamic Data (OPADD), Edition 4.1, 17/12/2020.

[RD 5] EUROCONTROL. European GNSS Contingency/Reversion Handbook for PBN Operations, Edition 1.1, 16/04/2020.

[RD 6] ICAO. Annex 15, Aeronautical Information Services. Sixteenth Edition, July 2018.

[RD 7] ITU. Radio Regulation Chapter IV, Article 15 – Interferences. Edition 2020.

[RD 8] ITU. Presentation on Harmful Interference and Infringements of the Radio Regulations. May 2015.

[RD 9] ICAO. Global Navigation Satellite System (GNSS) Manual - Doc 9849. Third Edition, 2017.

[RD 10] ICAO. Working paper on provisions, policy and guidance material on the delegation of airspace over the high seas. 22/07/2019.

[RD 11] ICAO. GNSS Vulnerability presentation in ITU Satellite Symposium. 26/09/2019.

[RD 12] ICAO. ICAO Location indicators - Doc 7910.

[RD 13] EASA. Certification Specifications and Acceptable Means of Compliance for Airborne Communications, Navigation and Surveillance CS-ACNS. Issue 4, 05/04/2022.

[RD 14] European Commission. Regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions.

[RD 15] NATO. Guidance Procedures and Planning Timetable for Civil-Military Coordination of NATO Air Exercises, AC/92-D(2016)0008-REV2. 06/06/2016 (controlled document).

[RD 16] EASA. Conflict Zone Information Bulletin (CZIB's):

https://www.easa.europa.eu/domains/air-operations/czibs/map

[RD 17] RTCA DO-235C Assessment of Radio Frequency Interference Relevant to the GNSS L1 Frequency Band, 17/03/2022.

[RD 18] ITU-R M.1903-1 (09/2019) Characteristics and protection criteria for receiving earth stations in the radionavigation-satellite service (space-to-Earth) and receivers in the aeronautical radionavigation service operating in the band 1 559-1 610 MHz.

[RD 19] Commission Implementing Regulation (EU) 2018/1048 of 18 July 2018 laying down airspace usage requirements and operating procedures concerning performance-based navigation.

[RD 20] ICAO. Annex 11: Air Traffic Services.

[RD 21] ECC Report 129, Technical and operational provisions required for the use of GNSS repeaters, Dublin, Jan. 2009.

1.10 Document structure

This document is organised as follows:

Section 1: Introduces the guidance material for GNSS interference testing;

Section 2: Details the GNSS interference testing process;

Annex A: Extract of relevant GNSS receivers and antennas characteristics related to interference from the current standards;

Annex B: Extract of relevant ITU interference regulations;

Annex C: Describes the Joint Restricted Frequency List;

Annex D: NAVCEN and GSC contact details;

Annex E: Maintenance procedures for the present document.

2 GNSS interference testing process

Peacetime testing of degradable navigation capabilities, including the operation of GNSS jamming and/or spoofing equipment, needs to be properly planned and coordinated with civil and military aviation authorities. It is essential for the safety of airspace users that the location, duration, and scale of such radio frequency interference (RFI) is known and fully coordinated beforehand. Establishing coordination procedures will improve the ability of the military and civil authorities in detecting accidental interferences and jamming/spoofing hostile attacks from planned GNSS interference testing.

As part of the planning phase, the impact of a GNSS interference test on aviation need to be assessed and coordinated, leading to the issue of aeronautical information publications such as NOTAMs, activation of airspace reservations (ARES), the establishment of temporary restricted (R-areas) or danger areas (D-areas) and/or other appropriate measures. Well-coordinated and mitigated GNSS interference tests are likely to have limited impact[3] on airspace users.

As a result, a process covering the planning, coordination and execution of GNSS interference testing, will support authorities in maintaining the safety of flights and will prevent airspace users of facing hazardous situations.

This chapter details the complete process for the conduction of GNSS interference testing in the form of recommendations. The overview of the planning and notification steps is presented in Figure 1.

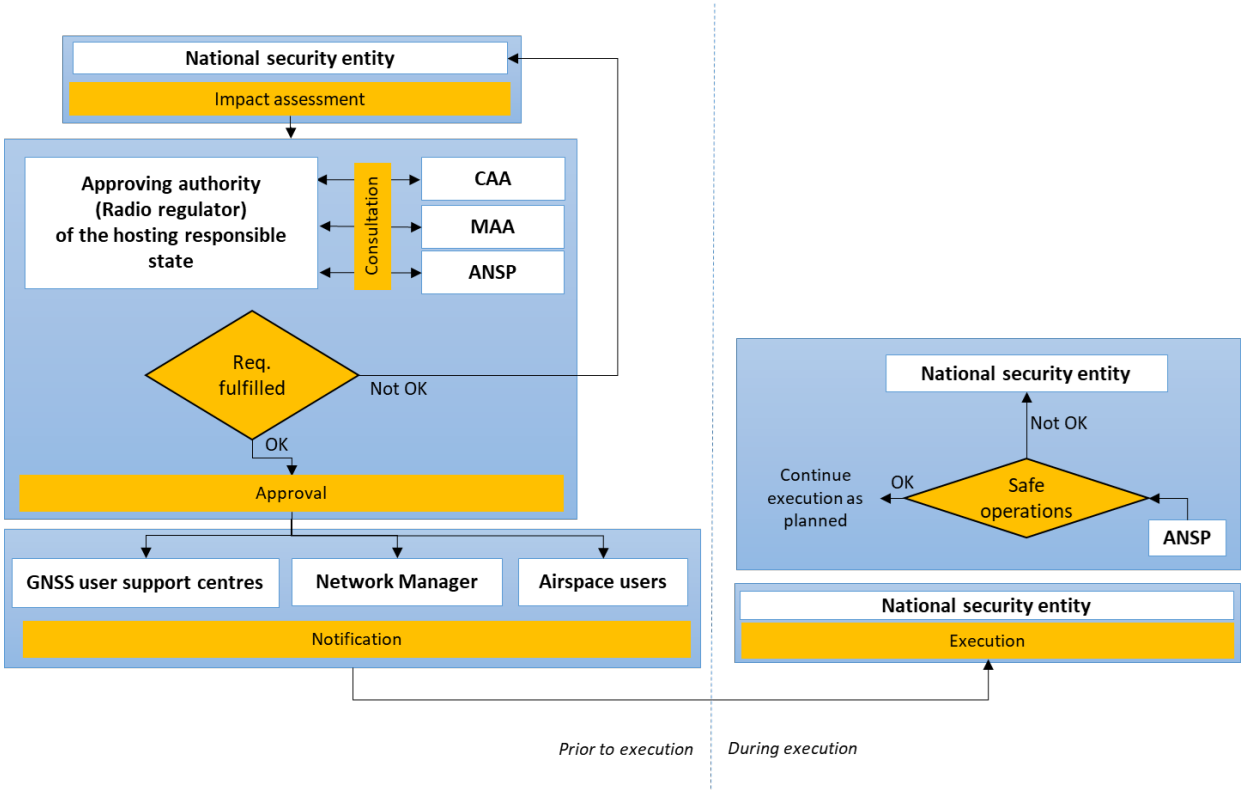


Figure 1: GNSS interference testing process

[3] The impact depends on the horizontal and vertical dimensions of the airspace and the types of aircraft operations conducted therein.

2.1 Planning of GNSS interference testing

2.1.1 Impact Assessment

The planning of GNSS interference testing activities begins with an initial impact assessment to determine the operational impacted area of the event and subsequent coordination actions.

GNSSTEST-GM1: The impact of GNSS interference testing on airspace users should be assessed by the national security entity intending to perform the GNSS interference tests so that accurate information about its location, scope of the area, and duration is identified.

GNSSTEST-GM2: If for national security reasons, the specific location of interference source cannot be revealed, an indication of the encompassing area should be provided to the approving authority and the associated uncertainty should be added to the impact area radius.

GNSSTEST-GM3: A sky view map containing the impacted area and taking into consideration the propagation calculation from the location of the interference source should be provided to the approving authority by the national security entity intending to perform the testing activity.

GNSSTEST-GM4: The planned range of interference should match the agreed national security need for the GNSS interference testing activity, considering a free space path loss model or if available a more precise model, or computer simulation software that takes into account the effect of terrain, vegetation or urban areas.

Note: The range depends on the potentially impacted altitudes/flight levels (FLs) (see section 2.2 for details).

GNSSTEST-GM5: The vertical dimension (altitudes/FL) in which air traffic operations will be impacted should be defined.

GNSSTEST-GM6: The received interference power should not exceed the interference sensitivity thresholds defined in [RD 3] for airspace users outside the specified range.

GNSSTEST-GM7: The national security entity performing the GNSS interference tests can consider higher power levels exceeding the sensitivity thresholds defined in [RD 3] as long as it provides, based on practical trials, solid proof and engineering evidence that such power levels have no adverse effect on non-participating GNSS receivers supporting safety critical functions. To use higher levels of interference power, the entity performing the GNSS interference tests needs approval beforehand from the entity designated by the state as the approving authority of GNSS interference tests. It is up to this entity to decide what standard of engineering evidence is acceptable.

GNSSTEST-GM8: The transmitted power complying with those thresholds should be computed considering a free space path loss model using the Friis transmission formula:

$$FSPL = \left(\frac{4\pi D}{\lambda}\right)^2$$

$$P_t = FSPL * \frac{P_r}{G_t G_r}$$

Where: D is the maximum jammer range;

λ is the wavelength ($\lambda = \frac{C}{f}$, for L1 frequency, $\lambda = 0.19\ m$);

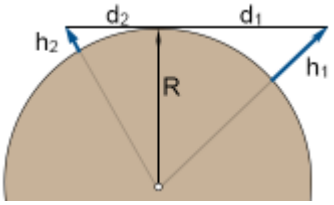
P_t is the transmitted interference power;

G_t is the transmitting antenna gain in the direction of the receiving antenna;

P_r is the received interference power. This value corresponds to the GNSS receiver resistance to interference defined in [RD 3] Appendix B.3.7 for jamming tests. The receiver interference mask depends on the interference type and the processed signals. For in band jamming, GPS and SBAS L1 receivers can resist, without significant degradation altering its functioning, up to -150.5 dBW [RD 18] jamming power after steady-state navigation has been established. The maximum tolerable received interference power for spoofing tests is 10 dB lower than authentic signal power level of an individual GNSS satellite (i.e. -170 dBW according to [RD 21]); and

G_r is the receiving antenna gain in the direction of the transmitting antenna. The GNSS receiving antenna gain depends on the direction of the received signal. It is defined in [RD 17] (See Annex A - A). If the interference source is below the aircraft, a worst case of -5dBi antenna gain can be considered.

Note: The reception of the interfering signal depends also on the line-of-sight propagation and refraction effects. Under normal weather conditions, the maximum transmission range (Radio Horizon) is D ≈ 4.12 $(\sqrt{h})$ (where h is the aircraft antenna altitude in m and D the maximum range in km) when the jammer is not located on a very high position compared to the nearby surroundings. A "high position" means that the jammer is at least 300m above mean sea level when located near the coast or above the average terrain level[4] in a horizontal range of 30 km. In that case, the radio horizon radius shall consider the following expressions:



$$Radio\ Horizon\ Radius\ (Km) = d_1 + d_2 = 4.12\ (\sqrt{h1} + \sqrt{h2})$$

$$where:$$

$$h_1 is\ the\ aircraft\ altitude\ in\ meters$$

$$h_2\ is\ the\ jammer\ altitude\ in\ meters$$

GNSSTEST-GM9: The entity conducting the impact assessment should determine which ICAO Annex 10 [RD 3] jamming type (CW, pulsed, noise-like) best matches the intended GNSS interference test.

GNSSTEST-GM10: For spoofing tests, the spoofing signal power level at the receiver port of a spoofing signal simulating an individual GNSS satellite should be at least 10 dB below the authentic signal power level of an individual GNSS satellite (i.e. -170 dBW [5] according to [RD 21]).

[4] The height above average terrain can be computed considering the intended RFI antenna site and a sectorisation of the surrounding landscape. The difference between the altitude of the antenna site and the average altitude of all the specified sectors constitutes the height above average terrain.

[5] Typical GNSS signal levels at the aircraft receiver are in the order of –160 dBW.

GNSSTEST-GM11: The transmitted interference power and the associated range should be computed for the GNSS systems listed in the national AIPs, Part 2, sections ENR4.3 (and/or GEN3.4.3[6]) of the affected States.

GNSSTEST-GM12: For a mobile interference source, the computation of the range should cover the impacted areas based on the predefined test platform trajectory.

GNSSTEST-GM13: The GNSS interference testing should be planned in an area where:

- A suitable navigation alternative to GNSS (e.g. DME/DME) and/or other means (e.g. a GNSS-independent surveillance system allowing radar vectoring) are available to manage the fleet mix in that airspace.
- Potentially impacted airports have non GNSS-based approach/departure procedures available (e.g. ILS procedures).

GNSSTEST-GM14: In exceptional circumstances where the GNSS interference testing cannot be executed in the above-mentioned areas, the national security entity intending to perform the GNSS interference testing should apply for the establishment of temporary restricted or danger areas or permission to use existing permanent restricted or danger areas.

GNSSTEST-GM15: An INTERRUPTION procedure should be in place to halt immediately the GNSS interference testing when unforeseeable events occur, such as reported impacts on airspace users beyond the specified interference range causing hazardous situations.

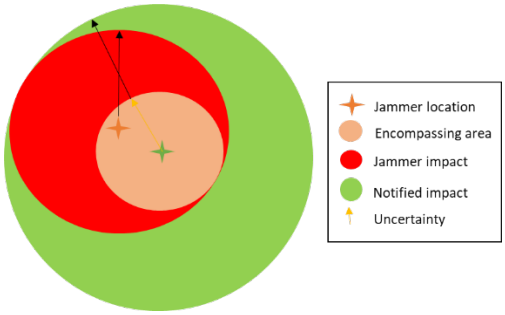
GNSSTEST-GM16: Clear criteria triggering the INTERRUPTION procedure should be agreed beforehand between the National Security Authority in charge of the testing activity and the concerned ANSPs.

GNSSTEST-GM17: The person in charge of the INTERRUPTION procedure should be available and continuously reachable by the potentially impacted ANSP(s) while the GNSS interference testing is being executed.

GNSSTEST-GM18: The contact information of the person in charge of the INTERRUPTION procedure should be made available to the concerned ANSP(s).

GNSSTEST-GM19: The national security entity in charge of the testing should prepare a documented impact assessment of the intended GNSS interference test for the approval process, including information about its location, scope of the area[7], duration, identified stakeholders (Radio regulator, CAA, MAA, ANSP(s)), specific procedures and contact information.

Note: Example for an omnidirectional jammer:



[6] AD2.19/3.18 may contain additional information related to GNSS complementing the information contained in ENR4.3 and/or GEN3.4.3.

[7] See GNSSTEST-GM3.

2.1.2 Approval Process

2.1.2.1 National Testing

GNSSTEST-GM20: The GNSS interference testing activity should be approved by the national approving authority.

GNSSTEST-GM21: Before taking a decision, the civil aviation authority, the military aviation authority (or equivalent parties) and the ANSP(s) should be consulted[8] by the approving authority.

GNSSTEST-GM22: After the approval of the GNSS interference testing activity, the national ANSPs should be informed by the national approving authority at least four weeks or any other nationally agreed period before the GNSS interference testing execution.

Note: The ANSP can request to the national approving authority the cancellation or the rescheduling of the testing prior to its commencement, preferably with as much notice as possible, if a safety-related reason justifies it. The possible reason for the cancellation of the testing activity during the planning phase will be an impact on the safety of air operations due to an unexpected event, a change in circumstances or a forecast of adverse weather expected to cause traffic disruption.

GNSSTEST-GM23: The GNSS interference testing should not be approved if any of the recommendations in section 2.1.1 are unfulfilled.

GNSSTEST-GM24: In case of conflict, the Ministry or Regulator with authority over the national security entity should, in coordination with the Authority in charge of civil aviation, provide a decision by considering the following aspects, at minimum:

- The involved safety impact issue;
- The number of impacted aircraft and passengers on board[9];
- The means of CNS alternative to GNSS for the impacted aircraft;
- The national security justification for performing the GNSS interference testing.

GNSSTEST-GM25: The Ministry or Regulator with authority over the entity owner of the GNSS interference testing activity (e.g. Ministry/Department responsible for Defence) and the Authority in charge of civil aviation should establish and agree on quantifiable and clear criteria (e.g. safety risk scale, security need urgency classification) for the arbitration in case of conflict.

Cross Borders Testing

GNSS interference testing is considered cross border if the impacted area covers a part of another country (land, territorial waters, or airspace) even if that source is located within the national borders. In this case, both recommendations for national (2.1.2.1) and cross border (2.1.2.2) testing are applicable.

GNSSTEST-GM26: The GNSS interference testing should be approved by the approving authority(ies) of the state(s) in which the GNSS interference testing takes place. Both the national

[8] The opinions of the aviation authorities need to be taken into consideration in the course of the decision-making process.

[9] The number of impacted aircraft and passengers on board can be derived from the traffic forecast corresponding to the duration of the requested testing activity.

and the impacted neighbouring States need to be consulted. The national testing approval processes of the hosting country(ies) is applicable.

GNSSTEST-GM27: The national security entity performing the GNSS interference testing should provide all the relevant information (see section 2.1.1) to the appropriate civil and military aviation authorities of the country where the GNSS interference testing takes place, at least four weeks or any other agreed period before the GNSS interference testing execution.

GNSSTEST-GM28: Neighbouring states should establish and approve a clear coordinated process to be followed in case of conflict on the impact of the GNSS interference testing (deciding authority of each state, point of contact, quantifiable and clear criteria for the decision in case of conflict).

GNSSTEST-GM29: The final approval of the GNSS interference testing should rest solely with the authorities of the states impacted by the GNSS interference testing.

2.1.2.2 High Seas Testing

All waters beyond the territorial waters (up to 12 NM) are considered as high seas and the airspace over the high seas is considered as an international airspace. A country may assume responsibility for controlling parts of the international airspace by international agreement. Each portion of the high seas airspace (FIR) is run by an appropriate ANSP, which is designated by the state responsible for providing ATS in that concerned airspace [RD 10]. The FIRs horizontal boundaries of EUROCONTROL Member States are shown below.

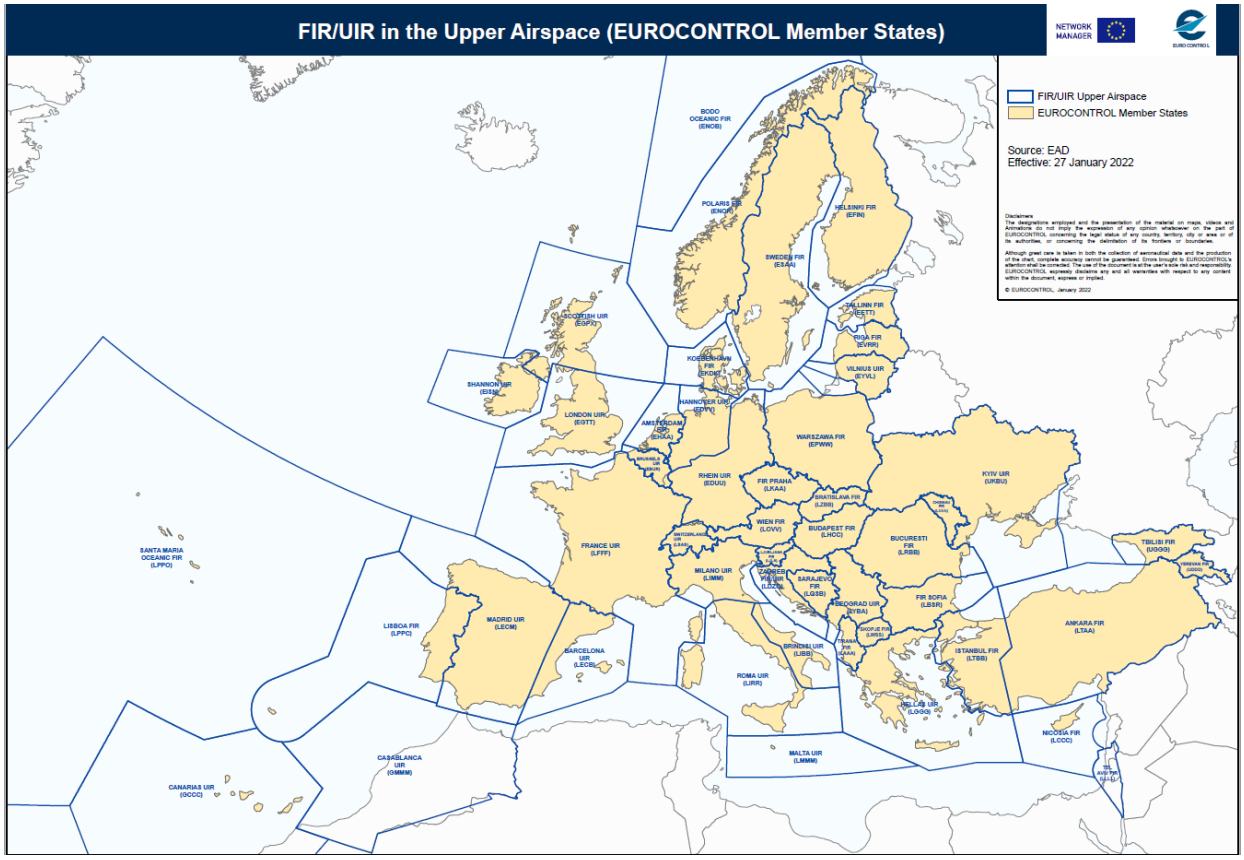


Figure 2: FIR/UIR in Upper Airspace (EUROCONTROL Member States)

GNSSTEST-GM30: The GNSS interference testing should be approved by the state with the responsibility to provide air traffic services in such portions of airspace. The national testing approval process of the hosting country is applicable.

GNSSTEST-GM31: When the high seas GNSS interference testing is approved, the ANSP in charge of providing air traffic services in such portions of airspace should be informed by the approving authority for that approval at least four weeks, or any other agreed period, before the execution of the testing.

2.1.3 Coordination of the GNSS Interference

GNSSTEST-GM32: The relevant entities in the country(ies) where the GNSS interference testing[10] is planned should be informed by the approving authority before the GNSS interference testing is performed, in particular:

- National Radio Regulator
- Civil Aviation Authority / National Supervisory Authority
- ANSP(s)
- Ministry of Defence or the National Security Authority
- Military Aviation Authority

GNSSTEST-GM33: The communications between administrations should be transmitted by the quickest means available, while ensuring the usage of official channels.

GNSSTEST-GM34: The recipient administration should, as soon as possible, acknowledge receipt and start the associated approval/notification process.

Note: The above recommendations are in line with the [RD 15] recommendations on the coordination of electronic countermeasures activities.

GNSSTEST-GM35: If it is considered necessary, and particularly if the steps taken in accordance with the procedures described above do not produce satisfactory results, the impacted national radio regulator should forward details of the interference case to the Radio communication Bureau of ITU [RD 7] and request assistance providing all the technical and operational details and copies of the correspondence.

Note: ITU has an online application aiming to facilitate report of harmful interference affecting space services and to request assistance from the Radiocommunication Bureau: https://www.itu.int/en/ITU-R/space/SIRRS/Pages/default.aspx

[10] Ground based or sea based or airborne tests

2.2 GNSS Interference testing notification

2.2.1 AIS

2.2.1.1 GNSS RFI NOTAM

GNSSTEST-GM36: NOTAMs containing all relevant information to alert airspace users should be issued by all the concerned ANSPs[11] before the execution of the GNSS interference testing.

GNSSTEST-GM37: At least, Items Q, A, B, C and E should be clearly mentioned in the NOTAM [RD 4][RD 6].

2.2.1.1.1 Item Q – Qualifier

GNSSTEST-GM38: The following qualifiers should be mentioned in item Q:

- *Qualifier FIR*: This Item should contain the ICAO location indicator of the FIR [RD 12] within which the flights may be impacted by the interference. If more than one FIR of the same country is concerned, the ICAO nationality letters of that country (e.g. ED) should be followed by 'XX'. If more than one FIR of different countries are concerned the ICAO nationality letters of the responsible State (e.g. LI) should be followed by 'XX'.
- *Qualifier NOTAM CODE*: the following NOTAM codes should be used for GNSS RFI event notification:
  - "QGAAU" if the interference is impacting only an aerodrome environment, or
  - "QGWAU" if the interference is impacting wider area(s)
- *Qualifier TRAFFIC*: the « IV » should be used as a traffic qualifier, indicating that both IFR and VFR traffic may be impacted by the RFI
- *Qualifier PURPOSE*: the code NBO should be used to notify RFI events:
  - N = NOTAM selected for the immediate attention of flight crew members. Due to their importance, these NOTAM require the immediate attention of flight crew members. Flight crew members may request specific delivery of such NOTAM or their inclusion in specific Pre-flight Information Bulletins.
  - B = NOTAM of operational significance selected for PIB entry. The NOTAM will appear in a Pre-flight Information Bulletin containing all NOTAM relevant to a general Pre-flight Information Bulletin query. NOTAM qualified B, BO, or NBO will appear in the Pre-flight Information Bulletin.
  - O = NOTAM concerning flight operations. The NOTAM will appear in a PIB containing all relevant NOTAM. NOTAM with qualifiers BO or NBO will appear in the PIB.
- *Qualifier SCOPE*: Depending on the impacted area, one of the following codes should be used :
  - A = if the testing event only impacts aerodrome(s) operations
  - E = if the testing event only impacts en-route traffic
  - AE = if the testing event only impacts both Aerodrome and En-route traffic
- *Qualifier LOWER/UPPER*: Depending on the intended jamming range and the traffic in the impacted area. The Upper limit corresponds to the computed jammer range. The lower limit depends on the type of traffic in the impacted area and the minimum altitude

[11] Issuing a NOTAM is a state responsibility. However, the state can delegate the authority for the provision of the AIS to a non-governmental agency provided that the SARPS of [RD 6] are adequately met.

of flying aircraft. Example: if the SCOPE is “En-route”, the minimum En-route altitude of the concerned airspace is FL300 and the jamming range is 12192m then the LOWER/UPPER qualifier is ‘Q) …/300/400/…’ (from ‘Lower’ FL300 up to ‘Upper’ FL400) To be noted that the limits specified in these qualifiers should be given as ‘flight levels’ only.

- *Qualifier GEOGRAPHICAL REFERENCE – Coordinates*: this qualifier indicates the interference source coordinates. For NOTAM with ‘Scope’ ‘A’ the Aerodrome Reference Point (ARP) coordinates should be inserted. For NOTAM with ‘Scope’ ‘AE’ or ‘E’ the centre of a circle whose radius encompasses the whole area of interference should be inserted.
- *Qualifier ‘GEOGRAPHICAL REFERENCE’ – Radius:* The radius of the impacted area should be inserted in this field. The value should be derived from the jammer range and altitude. It should take into consideration the ‘lower’ qualifier.

$$Radius\ (NM) = \frac{Minumum(Free\ Space\ Radius\ (Km), Radio\ Horizon\ Radius\ (Km))}{1.852}$$

Where

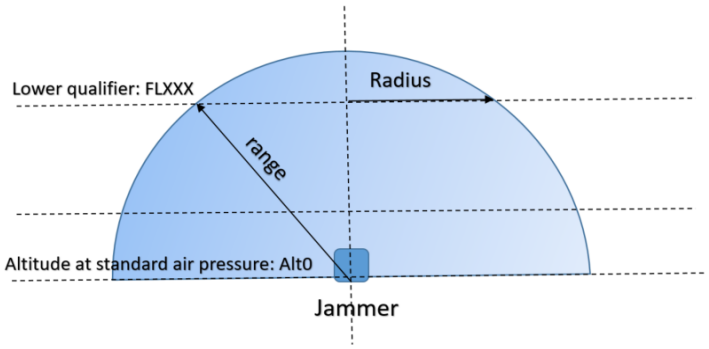
$$Free\ Space\ Radius\ (Km) = \sqrt{(range(Km)^2 - (LowerQualifier(Km) - Alt0(Km))^2)}$$

$$Radio\ Horizon\ Radius\ (Km)\ is\ computed\ as\ described\ in\ 2.1.1$$

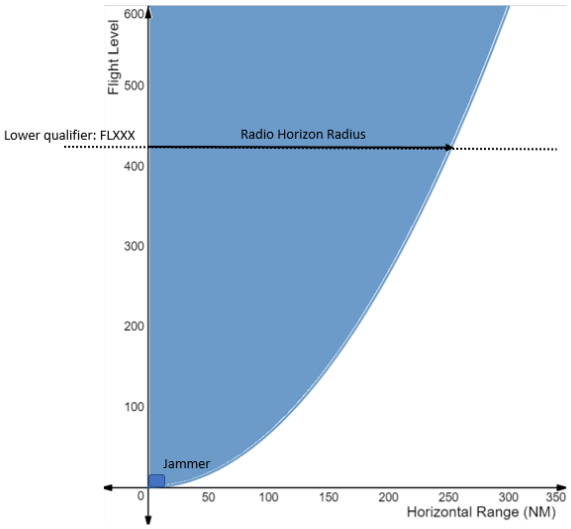
Notes:

1) *For jammer EIRP above 5 W and at -150.5 dBW of received interference power threshold, the radio horizon radius generally prevails over the free space radius.*
2) *Example: Jammer range = 10 km, Altitude Jammer = 500 m, Lower qualifier = FL300 → Radius= 5028m = 2.715 NM*

Free space radius diagram:



Radio horizon diagram:



$$x = 4.12 \cdot \frac{\sqrt{y \cdot 100 \cdot 0.3048}}{1.852}$$

3) Example of item: Q) EGGX/QGWAU/IV/NBO/E /300/400/5800N01413W003

2.2.1.1.2 Item A – Location

GNSSTEST-GM39: All FIR location indicators affected by the information should be entered in Item A), each separated by a space.

In the case of a single FIR, the Item A) entry must be identical to the 'FIR' qualifier entered in Item Q). When an aerodrome indicator is given in Item A), it must be an aerodrome/heliport situated in the FIR entered in Item Q).

2.2.1.1.3 Item B – Start of Activity

GNSSTEST-GM40: A ten-digit date-time group giving the year, month, day, hour and minutes, at which the NOTAM comes into force, should be mentioned in Item B). Example: B) 2107011200 (1 July 2021, 12:00 UTC).

2.2.1.1.4 Item C – End of Validity

GNSSTEST-GM41: A ten-digit date-time group giving the year, month, day, hour and minute, at which the NOTAM ceases to be in force and becomes invalid, should be mentioned in Item C). This date and time should be later than that given in Item B). Example: C) 2107011430 (1 July 2021, 14:30 UTC).

2.2.1.1.5 Item E – NOTAM Text

GNSSTEST-GM42: The following sentences should be used in Item E:

- "GNSS MAY BE UNUSABLE WITHIN" for jamming tests, or
- "GNSS MAY BE MISLEADING WITHIN" for spoofing tests

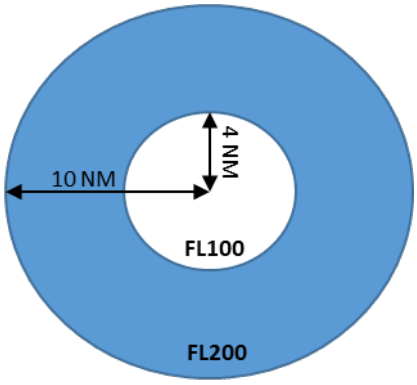
GNSSTEST-GM43: In order to further clarify the impact zone, it is recommended to either:

- mention the radius of the impacted zones for different flight levels[12] ; or
- describe the boundaries[13] of the impacted area for different flight levels.

Notes:

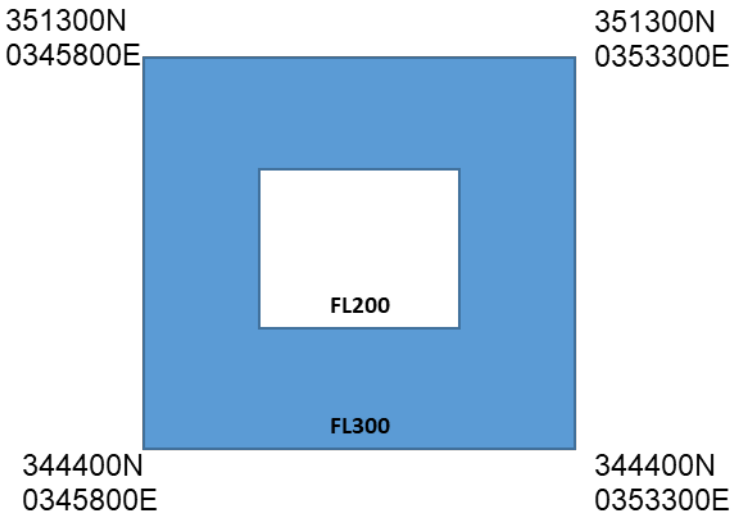
1) Radius example:

```
GNSS MAY BE UNUSABLE WITHIN:
4NM RADIUS AT FL100,
10NM RADIUS AT FL200,
CENTERED AT 413339N0193740W
```



2) Boundary example:

```
GNSS MAY BE MISLEADING WITHIN:
344359N 0345759E - 351259N 0345759E - 351259N 0353259E -
344359N 0353259E - 344359N 0345759E at FL200,
344400N 0345800E - 351300N 0345800E - 351300N 0353300E -
344400N 0353300E - 344400N 0345800E at FL300
```



[12] Each state can define the FL as adapted to their requirements and agreed local needs to describe simply and accurately the impact of the event.

[13] The boundaries may be represented by different shapes depending on needs (e.g. rectangle, triangle, polygons, etc)

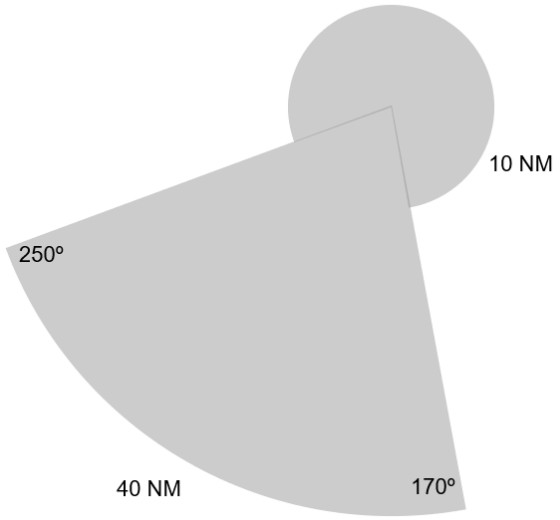
GNSSTEST-GM44: If the deployed jammer antenna is highly directional (e.g., horn antenna) and the direction of the radiation is planned and fixed, it is recommended to estimate two different ranges for the horizontal plane:

- a primary range for the main lobe of the antenna (maximum gain), the maximum gain should be extended in azimuth up to the first side nulls.
- a secondary range for the maximum gain of the side and back lobes.

The radiation diagram in the vertical plane should consider the maximum antenna gain.

Note: Example of a main lobe extending up to 40NM in the horizontal and vertical planes:

```
GNSS MAY BE UNUSABLE WITHIN:
10NM RADIUS FROM AZIMUTH 250 UP TO 170 DEGREES,
40NM RADIUS FROM AZIMUTH 170 UP TO 250 DEGREES,
CENTERED AT 413339N0193740W
```



2.2.1.1.6 Example of a GNSS interference testing NOTAM

```
Q) EGGX/QGWAU/IV/NBO/E /100/400/5800N01413W20
A) EGGX B) 2107011200 C) 2107011430
E) GNSS MAY BE UNUSABLE WITHIN:
5NM RADIUS AT FL100,
10NM RADIUS AT FL200,
15NM RADIUS AT FL300,
20NM RADIUS AT FL400,
CENTERED AT 5800N01413W
```

2.2.1.2 Temporary Danger or Restricted area activation NOTAM

GNSSTEST-GM45: If the GNSS interference testing requires the temporary activation of danger or restricted area, a NOTAM containing the elements detailed in section 2.2.1.1 should be issued by the ANSP[11].

GNSSTEST-GM46: The NOTAM indicating the activation of a temporary danger or restricted area should include the corresponding Q code:

- The “QRDCA” code to indicate an activation of a temporary danger area, or
- The “QRTCA” code to indicate an activation of a temporary restricted area.

GNSSTEST-GM47: The NOTAM indicating the activation of a temporary danger or restricted area should include the corresponding item E – NOTAM text:

- “DANGER AREA WITHIN … ACTIVATED” for an activation of a temporary danger area, or
- “RESTRICTED AREA WITHIN … ACTIVATED” for an activation of a temporary danger area.

2.2.1.3 AIP SUP

GNSSTEST-GM48: If the planned GNSS interference testing activity is of a long-term nature (three months or more) or if a NOTAM is not sufficient to describe the impacted area (e.g. explanatory graphics or extensive text are needed), an AIP SUP should be issued by the concerned ANSP(s) before the execution containing all relevant information, in particular:

- affected frequencies,
- affected area(s) supported by explanatory plots,
- dates, times and durations of the tests,
- potentially impacted systems and the recommended contingency procedures,
- contact details of the person in charge of the INTERRUPTION procedure, and
- references to the corresponding NOTAMs.

GNSSTEST-GM49: When a danger or restricted area is established for the GNSS interference testing activity and if it is of a long-term nature, an AIP SUP should be issued by the concerned ANSP(s) containing all relevant information, in particular:

- lateral and vertical limits,
- dates, times and durations of the tests,
- type of restriction and the entry conditions, and
- nature of the hazard.

2.2.1.4 AIC

GNSSTEST-GM50: If the GNSS interference testing information does neither qualify for the origination of a NOTAM nor for inclusion in the AIP, an AIC should be issued by the concerned ANSP(s) before the execution containing all relevant information, in particular:

- affected frequencies,
- affected area(s) supported by explanatory plots,
- dates, times and durations of the tests,
- potentially impacted systems and the recommended contingency procedures, and
- contact details of the person in charge of the INTERRUPTION procedure.

2.2.2 Reporting to the Network Manager

GNSSTEST-GM51: The national frequency managers should make use of the web interface[14] provided by NM in order to fulfil their reporting obligations of the radio interference cases that impact the European aviation network [RD 14].

2.2.3 Notification to other impacted GNSS users

GNSSTEST-GM52: Before the execution of GNSS interference testing, the radio regulator of the approving state should alert the GNSS users support services (e.g. the European GNSS Service Centre for Europe, the Navigation Center of the US department of homeland security (NAVCEN) for all GPS users, including non-US, the European Satellite Services Provider (ESSP) for EGNOS users – see Annex D), which will notify other potentially impacted users (e.g. terrestrial, maritime).

2.3 GNSS interference testing execution

2.3.1 Airspace users

The following guidelines are provided to complement existing procedures published in [RD 5] and [RD 9].

GNSSTEST-GM53: During the GNSS interference testing and in case of a GNSS loss on board the aircraft, the pilot should revert to dead reckoning or ask the ATCO for vectoring if the only available positioning source is GNSS.

GNSSTEST-GM54: If GNSS loss happens outside the area defined in the published RFI NOTAM, the pilot should report the loss of GNSS to the ANSP in charge of providing air traffic/navigation services in the impacted airspace.

GNSSTEST-GM55: During the GNSS interference testing and in case of a GNSS loss on board the aircraft while flying GNSS based procedures, if the aircraft is equipped with multi-sensor navigation systems, such as DME/DME[15] and/or IRS (see GNSSTEST-GM59), the pilot can continue navigating on the respective route provided that the related PBN procedure allows it, but should check other potentially impacted on-board systems (see GNSSTEST-GM58).

GNSSTEST-GM56: In case of a GNSS loss during a GNSS-based final approach (RNP APCH, RNP AR, GBAS), the pilot should initiate a missed approach procedure and switch to an alternative conventional approach procedure, such as ILS, for the second attempt.

GNSSTEST-GM57: In case of a GNSS loss during a GNSS-based final approach (LPV, GBAS, Baro VNAV) and if an alternative conventional approach procedure is not available (non-equipped aircraft or airport), the pilot should divert to another airport where an alternative approach can be flown.

GNSSTEST-GM58: In case of a GNSS loss and without an on-board IRS, the pilot should be aware that the on-board systems are impacted and should use other available means:

- SVS/EFVS: use other cockpit information available to get situational awareness. If the approach procedure is SVS dependant use ILS or divert if unavailable;
- Cockpit Display of Traffic Information (ADS-B IN as the source): do not rely on the displayed information and consider standard separation minima;
- CPDLC and ACARS: use voice messages via VHF or HF instead;

[14] https://ost.eurocontrol.int/sites/RFI/Lists/Interferences/All%20Items.aspx, The access to the reporting platform can be requested to the ARIA focal point.

[15] Radio updating (switch to ground NAVAIDs) is not automatic for some aircraft and will need to be enabled by the pilot in case of GNSS disruption.

- AHRS: ask ATCO for vectoring;
- TAWS/EGPWS: ask ATCO for vectoring and rerouting if flying over a mountainous terrain.

GNSSTEST-GM59: The pilot should be aware that if the aircraft is IRS equipped, the drift during GNSS losses is 2NM/h [RD 13] and that other on-board systems may be impacted if the loss is persisting (See GNSSTEST-GM58).

2.3.2 ANSPs

GNSSTEST-GM60: When applicable, the potential impact on the ATS personnel workload should be subject to assessment[16].

GNSSTEST-GM61: If the GNSS interference testing is taking place in an ADS-C surveillance only area (e.g. oceanic or remote areas), separation minima that does not rely on ADS-C should be applied.

GNSSTEST-GM62: If the GNSS interference testing is taking place in an ADS-B surveillance only area (e.g. oceanic or remote areas or in low density TMAs or airports with relatively low traffic levels), the procedural control should be used.

GNSSTEST-GM63: All the ATCOs in charge of controlling the GNSS interference testing surrounding area(s) should be informed before the testing activity.

GNSSTEST-GM64: All the ATCOs in charge of controlling the GNSS interference testing surrounding area(s) should be aware of the INTERRUPTION procedure and the person to contact in case of unanticipated circumstances.

GNSSTEST-GM65: The INTERRUPTION procedure should only be initiated when the GNSS interference testing is impacting[17] the safety of operations.

GNSSTEST-GM66: If unforeseeable events occur during the testing execution, the INTERRUPTION procedure should be used to take action (see GNSSTEST-GM15).

GNSSTEST-GM67: When requested by the pilot in command, the ATCO should re-route flights to avoid any active danger or restricted areas due to the GNNS interference testing.

GNSSTEST-GM68: In case of a GNSS loss, the air traffic controller should be aware that the following systems and capabilities are impacted and should use other available means[18]:

- Clock failures impacting position reporting and CPDLC communications: Use voice messages via VHF or HF and increase separation for trans-Atlantic flights if SATCOM are impacted.
- ADS-B surveillance: Use multi-sensor tracking systems including GNSS-independent Surveillance sources (e.g. Secondary Surveillance RADAR).
- ADS-C surveillance: Use of positional data reports coming from GNSS-independent Surveillance sources.
- Lateral navigation accuracy: Provide radar vectoring.
- Capability to fly ATS routes, including SIDs and STARs: Provide radar vectoring.

[16] Depending on the number of potentially impacted flights, extra ATCO(s) may be needed, especially for the areas/aircraft without a GNSS alternative. Specific ATCO response procedures may also need to be defined before the test.

[17] See GNSSTEST-GM16

[18] The contingency procedures need to defined for each specific operational environment in line with PANS-ATM (ICAO Doc4444)

- Capability to fly GNSS-based approaches: Offer alternative approach capabilities.

GNSSTEST-GM69: In case a temporary danger or restricted area has been activated for the GNSS interference testing activity, a NOTAM indicating its deactivation should be issued once the testing activity is over.

Annex A - GNSS receivers and antennas characteristics

A. GNSS antenna gain

The GNSS antenna gain depends on the direction of the received signal. It is defined in [RD 17] as follows:

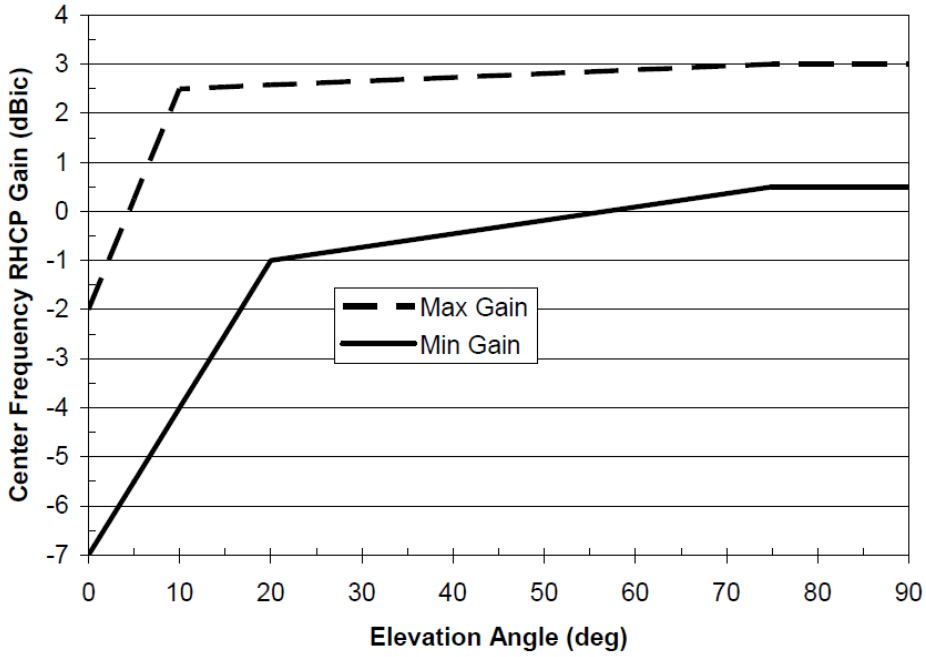


Figure 3: Upper hemisphere passive antenna gain limits

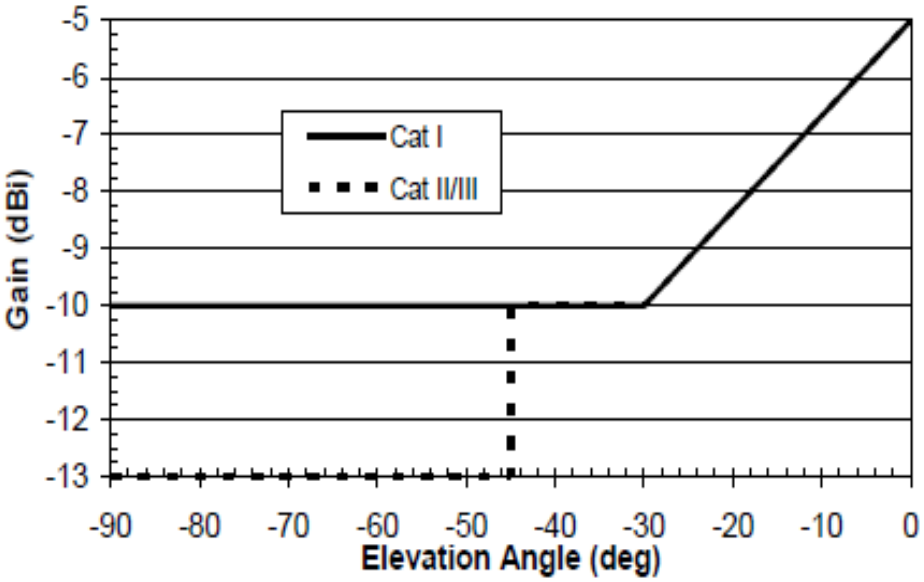


Figure 4: Lower Hemisphere passive antenna maximum gain

B. Resistance to interference

B.1. GPS and SBAS receivers

B.1.1. Continuous wave interference

After steady-state navigation has been established, GPS and SBAS receivers can resist CW interfering signals present with a power level at the antenna port equal to the interference thresholds defined by the following mask:

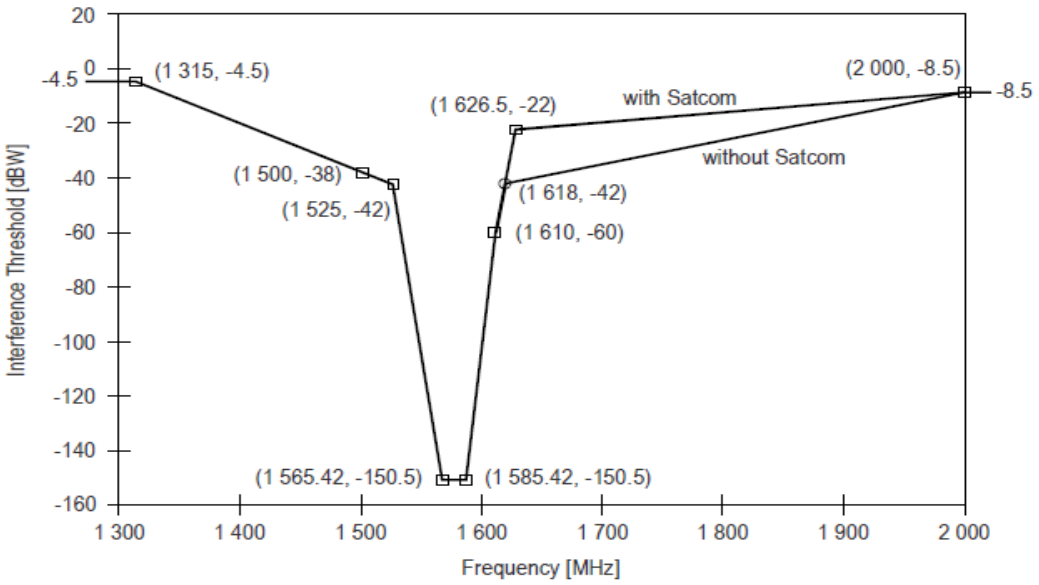


Figure 5: CW interference thresholds for GPS and SBAS receivers in steady-state navigation [RD 3]

So, for in band interference, the GPS and SBAS receivers can tolerate an interference power of -150.5 dBW [RD 18] without any impact on their performance during the steady navigation phase. However, during acquisition phase, receivers are more vulnerable and can only resist -156.5 dBW CW in band interference. Considering the most conservative case, the interference power at the receiver level should not exceed -156.5 dBW outside the jammer range. Knowing the intended CW jammer range, the transmitted power level can be easily computed. Here is an example computation considering an intended range of 10 km, a CW frequency of 1575.42MHz (L1) and isotropic antennas:

$$FSPL = \left(\frac{4\pi D}{\lambda}\right)^2 = 437433990075.9826 = 116.409\ dB$$

$$P_{t[dBW]} = FSPL_{[dB]} + P_{r[dBW]} = 116.409 - 156.5 = -40.09\ dBW \approx 0.1\ mW$$

B.1.2. Band limited noise-like interference

After steady-state navigation has been established, GPS and SBAS receivers can resist noise-like interfering signals present with a power level at the antenna port equal to the interference thresholds defined in the following figure:

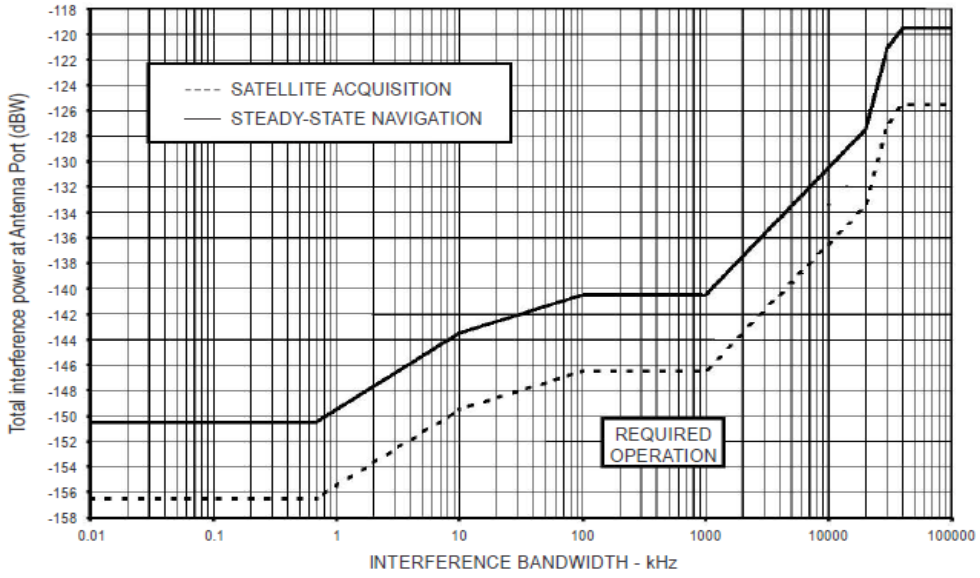


Figure 6: Interference thresholds versus bandwidth for GPS and SBAS receivers [RD 3]

For interference bandwidths greater than 1 MHz, the interference threshold does not exceed -140.5dBW/MHz in the frequency range 1 575.42 ± 10 MHz

For narrow band interference, the thresholds are similar to CW thresholds for in band interference. The same range computation method can therefore be used.

B.1.3. Pulsed interference

After steady-state navigation has been established, the receiver can resist pulsed interference signals with characteristics according to the following table:

Frequency range for in-band and near-band	1 575.42 MHz ± 20 MHz
Interference threshold (Pulse peak power) for in-band and near-band interference	–20 dBW
Interference threshold (Pulse peak power) outside the in-band and near-band frequency ranges (out-of-band interference)	0 dBW
Pulse width	≤125 µs
Pulse duty cycle	≤1%
Interference signal bandwidth for in-band and near-band interference	≥1 MHz

The transmitted pulsed in-band interference power should not then exceed (-20dBW+FSPL).

B.2. GLONASS receivers

B.2.1. CW interference

After steady-state navigation has been established, GLONASS receivers can resist CW interfering signals present with a power level at the antenna port equal to the interference thresholds defined by the following mask:

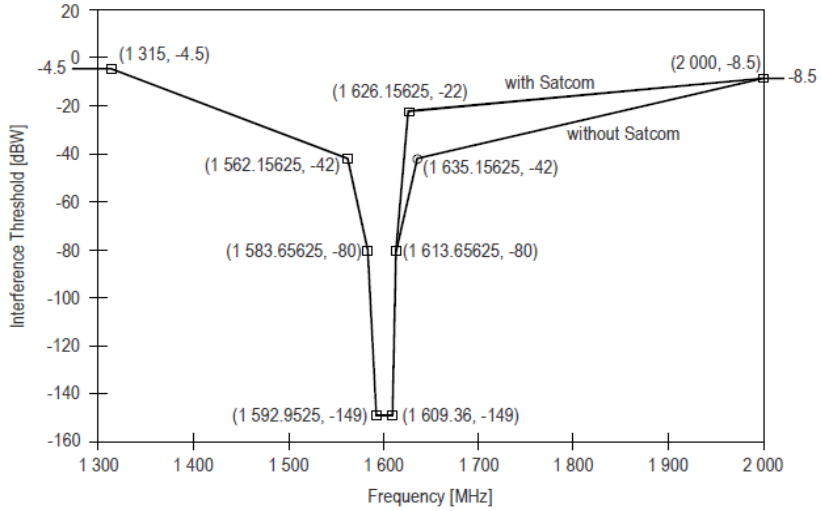


Figure 7: CW interference thresholds for GLONASS receivers in steady-state navigation [RD 3]

So, for in band interference, the GLONASS receivers can handle an interference power of -149 dBW without any impact on their performances during the steady navigation phase. However, during acquisition phase, receivers are more vulnerable and can only resist -155 dBW noise-like in band interference.

Similarly to GPS receivers, the interference power at the transmitter level can be computed according to the desired range using the free space path loss model. To be noted that GLONASS L1 signals are FDMA modulated and that the used frequencies are different from GPS L1 signals. A CW interference can therefore have impact on GPS L1 signals but not on GLONASS L1 signals and vice versa.

B.2.2. Band limited noise-like interference

After steady-state navigation has been established, GPS and SBAS receivers can resist noise-like interfering signals present with a power level at the antenna port equal to the interference thresholds defined in the following figure:

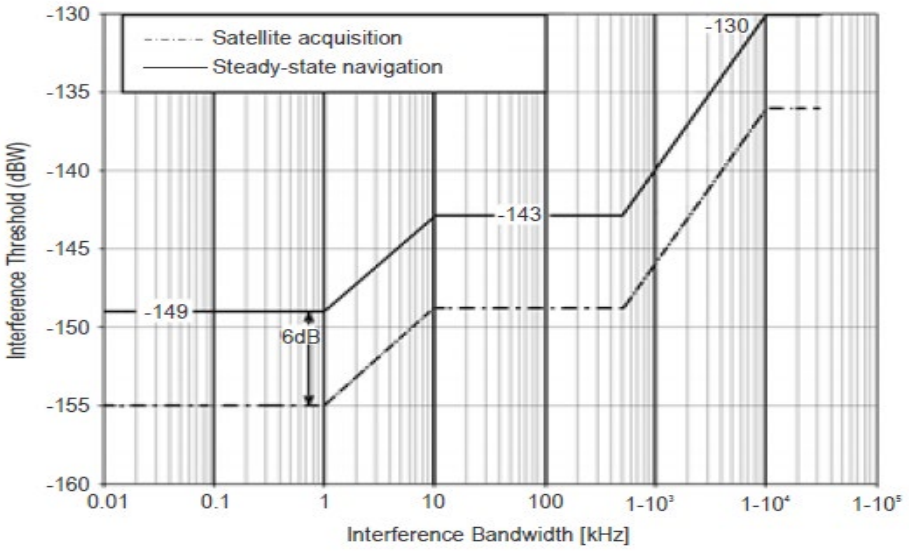


Figure 8: Interference thresholds versus bandwidth for GLONASS receivers [RD 3]

For narrow band interference, the thresholds are similar to CW thresholds for in band interference. The same range computation method can therefore be used.

B.2.3. Pulsed interference

After steady-state navigation has been established, the receiver can resist pulsed interference signals with characteristics according to the following table:

Frequency range for in-band and near-band	1 592.9525 MHz to 1 609.36 MHz
Interference threshold (Pulse peak power) for in-band and near-band interference	–20 dBW
Interference threshold (Pulse peak power) outside the in-band and near-band frequency ranges (out-of-band interference)	0 dBW
Pulse width	≤250 μs
Pulse duty cycle	≤1%
Interference signal bandwidth for in-band and near-band interference	≥500 kHz

The pulsed in-band interference power at the transmitter level should not then exceed (-20dBW+FSPL)

Annex B - ITU Radio Regulations - interference

The primary objective of the ITU-R is to enable radio communication services to operate without causing harmful interference, in particular, to a radio navigation or any other safety service operating in accordance with the provisions of the ITU RR. [RD 7] [RD 8].

The following terms have been used in these guidelines and for full definitions we direct the reader towards the ITU Radio Regulations (as published on the ITU website www.itu.int):

- radionavigation-satellite service (RNSS)
- safety service
- interference
- permissible interference
- accepted interference
- harmful interference

The aspects of harmful interference can be caused by:

- Out of band emissions
- Operation of non-coordinated frequency assignments
- Non-observance of limits of frequency tolerances or maximum permitted power levels for spurious emissions
- Operating with different technical parameters from those recorded in Plans or the Master Register
- Unnecessary transmissions
- Unauthorised emissions, etc.

Under the ITU Radio Regulations a number of obligations are detailed to avoid harmful interference and below these relevant to these guidelines are captured:

- The constitution where several provisions are related to stations capable of causing harmful interference (No 37, 38,197, 198)
- Article 4.10 and Article 4.4 on the appropriate assignment of frequencies to avoid harmful interference,
- Article 15.3 to Article 15.6 on the location, the radiation, the directivity and the main characteristics of the transmitter
- Article 15.8 on frequencies related to safety and regularity of flight
- Article 15.14 and 15.7 on tests and experiments
- Article 15.19 to 15.21 on the procedures in case of infringement of radio regulations

The procedure in case of harmful interference is set forth in Section VI of Article 15 of the Radio Regulations. It is highlighted that the problems of harmful interference are to be resolved on the basis of goodwill and mutual assistance, as stipulated in provision Article 15.22.

No. 15.22. The administrations should cooperate in the elimination of harmful interference. The case resolution may be dealt with directly by their monitoring stations or between the operators.

While it is true that spectrum management is a sovereign matter for each ITU member, the fact remains that radio waves cross borders. The coordination and mutual assistance between the concerned countries is a key to avoid harmful interference. However, as stipulated by Article 15.41.

> *Article No.15.41, If it is considered necessary, and particularly if the steps taken in accordance with the procedures described above have not produced satisfactory results, the administration concerned shall forward details of the case to the Bureau for its information.*

In such a case, the administration concerned may also request the Bureau to act in accordance with the provisions of Section I of Article 13 and should then supply the Bureau with the full facts of the case, including all the technical and operational details and copies of the correspondence (Article No. 15.42). The Bureau will contact the responsible administration in order to resolve the matter. If the harmful interference persists, the Bureau will prepare a report for consideration by the Radio Regulations Board [RD 7] [RD 8].

Annex C - Joint Restricted Frequency List

The Joint Restricted Frequency List (JRFL) is a time and geographically oriented listing of TABOO, PROTECTED and GUARDED functions, nets and frequencies which is used to minimise undesired effects of friendly force electronic countermeasures activity. It should be limited to the minimum number of frequencies necessary for friendly forces to accomplish their objectives.

The JRFL contains frequencies that fit into one of three categories, with the definitions of these types of frequencies given as follows:

a. Taboo: a friendly frequency on which jamming or other intentional interference is prohibited. Basically, this is any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces.

b. Protected: a friendly frequency on which interference must be minimised. This includes friendly frequencies used for a particular operation which are identified and protected to prevent inadvertent interference or jamming while operations such as active electronic efforts are directed against hostile forces.

c. Guarded: an enemy frequency used as a source of information, on which jamming is therefore controlled. This includes enemy frequencies that are currently being exploited for combat information and intelligence purposes.

Several JRFL frequency requirements may never change during the entire operation. Examples of these include, but are not limited to: GNSS system and other satellite-based frequencies, air traffic control frequencies, command net channels, radar system frequencies and international distress frequencies.

The National Military authorities are responsible for the compilation and maintenance of the JRFL. The JRFL is a controlled classified document.

Annex D - GNSS user support centres

The United States Coast Guard Navigation Information Service (NIS), operated by the USCG Navigation Center, is staffed 24 hours a day, 7 days a week. The NIS provides information on the current operational status, effective policies, and general information for GPS and DGPS. The NIS also disseminates Safety Broadcasts (BNM), Local Notice to Mariners (LNM), and the latest Notice Advisory to Navstar Users (NANU). The degradation or loss of GPS can be reported via any of the following [RD 2]:

https://www.navcen.uscg.gov

E-mail: TIS-PF-NISWS@navcen.uscg.mil

Phone: +1 703 313 5900

The European GNSS Service Centre (GSC) provides the single interface between the Galileo system and the users of the Galileo Open Service (OS), and the Galileo Commercial Service (CS). The GSC is conceived as a centre of expertise, knowledge sharing, custom performance assessment and information dissemination. The GSC issues NAGUs (Notice Advisory to Galileo Users) to inform about any activity/event in the Galileo system with impact on the Signal in Space (SiS) and/or on the performance. Any incident or degradation of service can be reported using the following link:

https://helpdesk.gsc-europa.eu/

Please note that you have to register before using the reporting tool:

urchttps://www.gsc-europa.eu/user/register

The GSC and the NAVCEN centres have an agreement on sharing GNSS loss/degradation reports. Any reported event affecting either GPS and Galileo signals anywhere in the world will be therefore shared between the two centres.

The European Satellite Services Provider (ESSP) is in charge of the operation and service provision of EGNOS, the European Geostationary Navigation Overlay System. The EGNOS Service Provision contract is funded by the European Union and managed through the European Union Agency for the Space Programme (EUSPA). ESSP supports GNSS users through performance monitoring, user support and real-time GNSS data dissemination via the Internet. . Any incident or degradation of service can be reported using the following link:

https://egnos-user-support.essp-sas.eu/new_egnos_ops/helpdesk

Annex E - Document update procedures

It is necessary to periodically check these EUROCONTROL Guidelines for consistency with referenced material. In addition, the content of these guidelines can evolve following feedback from implementation projects and field experience.

The main objectives of a regular review are:

a) to improve the quality of the guidance (e.g. clarity, testability, etc.);

b) to verify that the level of detail published is adequate;

c) to make all stakeholders including industry aware of the latest developments.

The update of these guidelines is expected to be initiated by stakeholders directly or through specific EUROCONTROL working arrangements such as the Civil-Military CNS Focus Group (CNS FG), the Military Harmonisation Group (MILHAG), the Military ATM Board (MAB) or the Joint CNS Stakeholder Platform (JCSP) (or its subgroups). Any stakeholder that wishes to request a change to these guidelines can submit a change request (CR) to the generic email address: standardisation@eurocontrol.int.

The CR needs to provide following minimum elements:

- Originator information (name, Organisation, contact details);
- Guideline title, number and edition date;
- Page, chapter, section (subsection) where the issue appears;
- Description of the issue and reason for change;
- Specific change proposal text (incl. potential alternatives, if any).

Main steps towards a revised version:

- EUROCONTROL will assess each CR and consult relevant working arrangements (e.g. CNS FG, MILHAG, MAB, JCSP);
- The CR will be classified in terms of urgency and impact;
- A resolution proposal(s) will be prepared and, if needed, discussed with the originator;
- Agreed changes will be integrated into a revised version “Proposed Issue” including a summarised list of changes in the document record;
- The “Proposed Issue” will be consulted with relevant working arrangements (e.g. CNS FG, MILHAG, MAB, JCSP).

Identified errors which may cause potential problems when implementing, may be corrected directly via separate “Corrigendum”.

EUROCONTROL

SUPPORTING EUROPEAN AVIATION

www.eurocontrol.int