CEPT ECC
Electronic Communications Committee

ECC Recommendation (26)01

On guidance for coordination measures to limit the impact of authorised GNSS jamming and spoofing operations

approved 5 June 2026

Edition 5 June 2026

INTRODUCTION

A growing number of applications rely on a Global Navigation Satellite System (GNSS). GNSS operate in frequency band with a Radio Navigation Satellite Service (RNSS) allocation. Despite its advantages, one of the main drawbacks of GNSS is its sensitivity to radio frequency interference.

Several applications that operate under a safety service as defined in No. 1.59 of the ITU Radio Regulations rely on GNSS. In this context, GNSS is used in a wide range of communication, navigation and surveillance systems as well as for maritime, air and ground transport traffic management. GNSS is therefore important to safe aviation operations, enabling for instance today's aircraft to rely on accurate and reliable position, speed or time at any point and without interruption. Consequently, any interruption to the GNSS causes a reduction of the efficiency of the overall system, placing a higher workload on captain, pilots and traffic controllers, and requiring complementary Communication, Navigation, and Surveillance (CNS) services to be deployed and maintained to support more demanding requirements. Other GNSS users, e.g. the maritime sector, may depend on GNSS in a similar fashion. Notwithstanding this, some GNSS users including the maritime and civil aviation sector have reported an increasing number of interference cases in recent years. This causes a serious threat on the safety and efficiency of these critical GNSS applications.

In response to these increasing interference cases, ITU-R WRC-23 decided to adopt Resolution 676 "Prevention and mitigation of harmful interference to the radionavigation-satellite service (RNSS) in the frequency bands 1164-1215 MHz and 1559-1610 MHz" [1]. Several issues are addressed in this Resolution: prevention against unauthorised transmitters that cause, or have the potential to cause, harmful interference to RNSS; interference risks to RNSS that may stem from the activities of security authorities; and report of cases of harmful interference.

The objective of this Recommendation is to provide technical material and guidance in order to limit the impact of approved and pre-planned jamming and spoofing operations and to help the implementation of Resolution 676 (WRC-23).

ECC RECOMMENDATION (26)01 OF 5 JUNE 2026 ON GUIDANCE FOR COORDINATION MEASURES TO LIMIT THE IMPACT OF AUTHORISED GNSS JAMMING AND SPOOFING OPERATIONS

"The European Conference of Postal and Telecommunications Administrations,

considering

a) that global and regional satellite navigation systems in the radionavigation-satellite service (RNSS) operate the frequency bands 1164-1215 MHz and 1559-1610 MHz, subject to No. 4.10 of the ITU Radio Regulations to ensure freedom from harmful interference for the reliable operation of the RNSS;

b) that RR No. 4.10 states that "the safety aspects of radionavigation and other safety service require special measures to ensure their freedom from harmful interference";

c) that disruption to the RNSS has been identified globally by the aeronautical community and the maritime community, and that there are different types of activities which may cause service disruption;

d) that the RNSS in the frequency bands 1164-1215 MHz and 1559-1610 MHz is used in several aeronautical and maritime communication, navigation and surveillance systems as a safety service. Further, the RNSS is used for scientific applications and in many applications and devices around the world and across all sectors of the global economy, as described in Report ITU-R M.2458 [2];

e) that the International Maritime Organization (IMO) through its Maritime Safety Committee (MSC), despite actions taken to mitigate the impact of harmful interference on the RNSS and its applications, has recognised that harmful interference impacting the RNSS poses a substantial risk to the safety of navigation, the safety of life and property, and the protection of the marine environment (see MSC.1/Circ. 1644 [10] on possible actions conducted by administrations);

f) that Interference Tolerance Masks (ITM) are defined by ICAO (Annex 10, Vol I) [7] for aeronautical receivers and by ETSI EN 303 413 [8] for non-aeronautical receivers;

g) that harmful interference to the RNSS has potential consequences for safety systems used by aeronautical and maritime applications, and for the regularity and efficiency of civil aviation operations;

h) that Article 47 of the ITU Constitution states that "Member States agree to take the steps required to prevent the transmission or circulation of false or deceptive distress, urgency, safety or identification signals, and to collaborate in locating and identifying stations under their jurisdiction transmitting such signals";

i) that ECC Recommendation (04)01 [9] supports the prohibition of jammers operated by the general public in CEPT countries;

j) that exemptions for defence and national security uses are often granted;

k) that jamming and spoofing are essential military capabilities that might also be used in peacetime in an operational context, e.g. training and exercises;

l) that Galileo and EGNOS will implement data authentication capability which contribute to improve the resilience of GNSS against spoofing;

m) that ITU-R Resolution 676 (WRC-23) [1] resolves to urge administrations "to encourage cooperation between aeronautical, maritime and security authorities, as well as spectrum regulators, as appropriate, to address interference risks to RNSS that may stem from the activities of these security authorities";

n) that the Maritime Safety Committee of IMO, in Circular MSC1/Circ.1644 [10], urges Member States to consider issuing warning notices or advisories to mariners specifying the time periods and areas impacted by any known interferences to minimise negative effects upon maritime operations;

o) that some CEPT countries have adopted procedures for authorised governmental jamming and spoofing activities impacting RNSS bands;

recommends

1. to strengthen cooperation between stakeholders including authorised governmental users of jamming and spoofing equipment and civil aviation authorities, maritime authorities, affected ministries and national radio regulator as appropriate to reduce as far as practicable interference risks stemming from the activities of these authorised governmental users on any GNSS receivers;

2. that the guidelines contained in Annex 1, or any other suitable and applicable guidelines and procedures agreed at the national level, should be followed when preparing and coordinating the use of GNSS jamming and spoofing;

3. that elements of Annex 2 should be taken into account when assessing the impact of GNSS jamming operations on GNSS users;

4. that elements of Annex 3 should be taken into account when assessing the impact of GNSS spoofing operations on GNSS users;

5. that the examples of warning notices in Annex 4 may be used as a template by administrations to minimise negative effects upon maritime and aeronautical operations."

Note:

Please check the ECO Documentation Database https://docdb.cept.org/ for the up to date position on the implementation of this and other ECC Recommendations.

ANNEX 1: RECOMMENDED PROCEDURE FOR PLANNED GNSS JAMMING AND SPOOFING OPERATIONS

This annex contains elements of best practice derived from existing coordination procedures across the CEPT region. These guidelines should be used and adapted to the local, national context and requirements as part of the coordination between the civil and security/military authorities. These elements are intended as guidance to assist CEPT administrations develop their own national procedures.

The overview of the planning and notification steps is presented in Figure 1. (CAA : Civil Aviation Authority, MAA : Military Aviation Authority, ANSP: Air Navigation Service Provider)

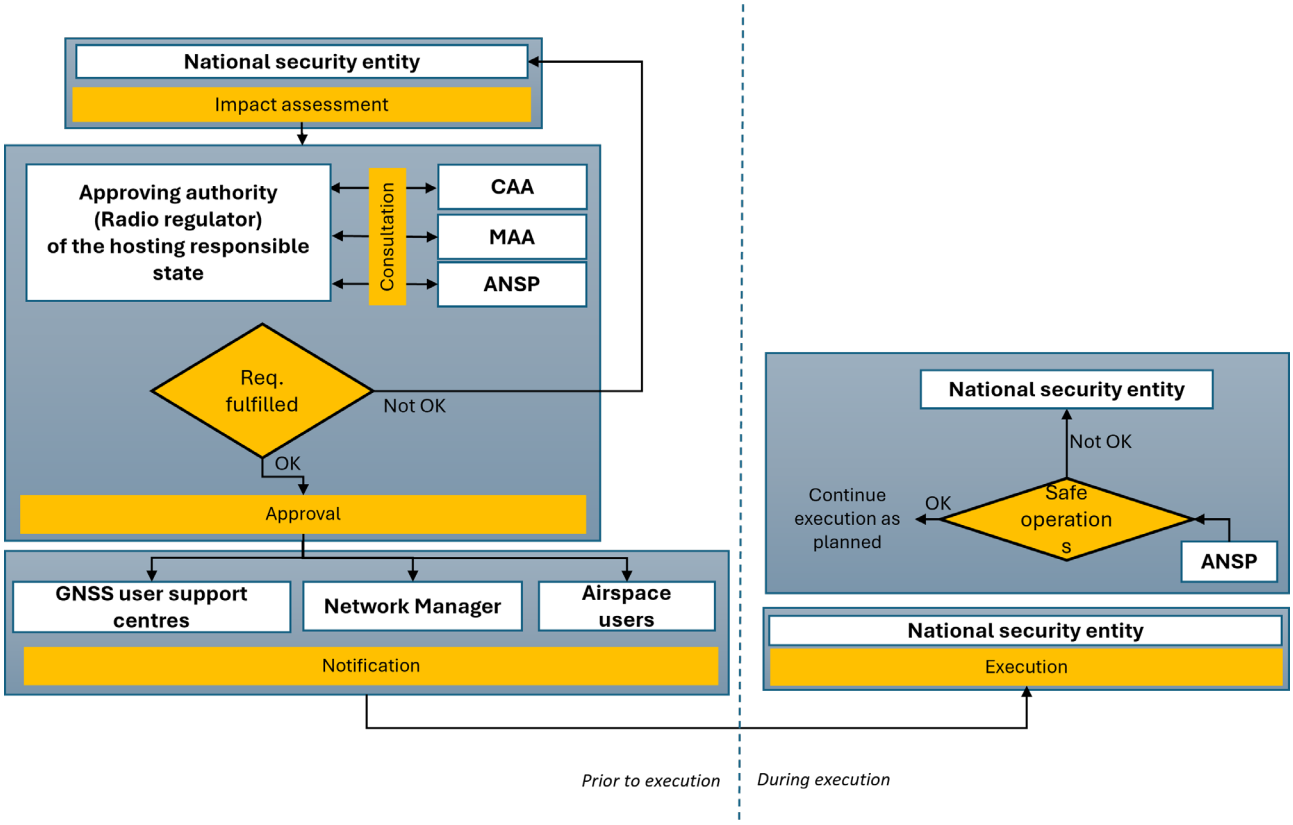


Figure 1: GNSS interference testing process

A1.1 PLANNING OF GNSS INTERFERENCE TESTING

A1.1.1 Impact Assessment

- The planning of GNSS interference testing activities should begin with an initial impact assessment to determine the operational volume impacted by the event and any subsequent coordination actions;
- Perform interference coverage calculations to determine the impacted volume of the authorised testing;
- The impact of GNSS interference testing on potentially affected users, e. g. the aviation sector and critical infrastructure such as power and telecom, should be assessed by the national security entity intending to perform the GNSS interference tests so that accurate information about its location, size of the volume, and duration is identified;
- If for national security reasons, the specific location of interference source cannot be revealed, an indication of the encompassing volume should be provided to the approving authority and the associated uncertainty should be added to the impact volume;
- The received interference power should not exceed the interference sensitivity thresholds defined in Annex 2 (jamming) and Annex 3 (spoofing) for GNSS users outside the approved test volume;

- An INTERRUPTION procedure should be in place to halt immediately the GNSS interference testing when unforeseeable events occur inside or beyond the specified interference volume causing hazardous situations, or if emergency services (e.g. ambulance helicopters) need to enter the interference volume;
- Clear criteria triggering the INTERRUPTION procedure should be agreed beforehand between the National Security Entity in charge of the testing activity and the potentially affected users of GNSS;
- The person in charge of the INTERRUPTION procedure should be available and continuously reachable by the potentially impacted users while the GNSS interference testing is being executed;
- The contact information of the person in charge of the INTERRUPTION procedure should be made available and acknowledged beforehand to the potentially affected users of GNSS and the relevant stakeholders;
- 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, size of the area[1], duration, identified stakeholders (such as civil aviation authorities, maritime authorities, affected ministries and national radio regulator), specific procedures and contact information.

It is also to be noted that some GNSS receivers may become unstable or behave unpredictable even after the interference exposure is discontinued. This may have to be taken into account when deciding upon how to set the status of the impacted volume.

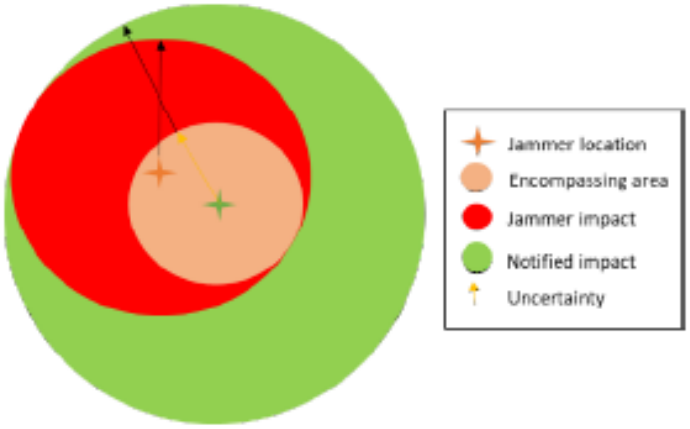


Figure 2: An illustrative 2-dimension example describing the size of a jamming area in the case of an omnidirectional jammer

A1.1.2 Approval process

The following steps are recommended in order to approve live testing:

- The impact assessment from A1.1.1 should be descriptive enough for the approving authority to thoroughly understand the test needs and the associated consequences;
- The GNSS interference testing activity must be approved by a national approving authority;
- Before taking a decision, all relevant stakeholders, including for instance the civil aviation authorities, maritime authorities, affected ministries and national radio regulator should be consulted by the approving authority. The views from the aforementioned stakeholders should to be taken into consideration over the course of the decision-making process.

A1.2 TEST EXECUTION

The following steps are recommended when conducting national testing:

- After the approval of the GNSS interference testing activity, all relevant stakeholders, including for instance the air navigation service provider (ANSP), should be informed by the national security entity at least four

[1] For the aviation sector see GNSSTEST-GM3 in [6].

weeks or any other nationally agreed period of time before the GNSS interference testing execution. When applicable, additional notification closer to the testing is advisable;

- The Ministry or Regulator with authority over the entity conducting the GNSS interference testing activity (e.g. Ministry/Department responsible for Defence) and the authorities responsible for the affected sectors or user groups 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;
- RF monitoring should be performed during the testing, to evaluate signal coverage of the test area versus calculated/predicted coverage, as well as ensuring that national frequency allocations and permissions are being followed;
- A directional antenna pattern should be used to limit the exposed area as much as possible, and an omnidirectional pattern should be used only when specifically needed.

A1.2.1 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 such a case, Section IV (“Tests”) of Article 15 of the Radio Regulations should be applied by the CEPT administration.

A1.2.2 International waters and airspace

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. Such case is out of scope of an ECC Recommendation that can only apply inside CEPT territories.

However, when the precalculated interference coverage spills into international airspace and waters, relevant national authorities should be notified.

A1.3 INTERFERENCE TESTING NOTIFICATION TO IMPACTED GNSS USERS

CEPT administrations should impose upon the national security entity to assess which GNSS users are impacted and take the necessary action to inform them. It is additionally recommended to inform users that are appropriately registered in the national frequency register.

GNSS users that may use RNSS for critical purposes are encouraged to register their earth stations at national level and notify their receiving station in the ITU MIFR.

Examples of established notification procedures for the maritime and aviation sectors are provided in Annex 4.

A1.4 SPECIFIC ACTIONS RECOMMENDED TO LIMIT IMPACT ON CIVIL AVIATION

Specific elements concerning aviation can be derived from the EUROCONTROL Guidelines on GNSS testing [6]. Some of these elements may be applicable to other GNSS users.

GNSS is used by a wide range of civil aviation Communication, Navigation, and Surveillance (CNS) systems. It is in particular one of the primary means of aeronautical navigation. In order not to fully disrupt navigation capabilities of aircraft, the GNSS interference testing should be planned in an area where:

- A suitable navigation alternative to GNSS (e.g. Distance Measurement Equipment (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. A particular attention should be given to make sure that DME navigation capability remains available, given that DME operate in the frequency band 960-1215 MHz which overlaps with GNSS band 1164-1215 MHz;
- Potentially impacted airports have non GNSS-based approach/departure procedures available (e.g. instrument landing system procedures).

In addition, the national ANSPs should be informed by the national approving authority at least four weeks or any other nationally agreed period before the planned jamming and spoofing operation.

Note: The ANSP can request to the national approving authority the cancellation or the rescheduling of the approved and pre-planned jamming and spoofing operation 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.

A1.4.1 Interference testing execution

The relevant EUROCONTROL Report (see [6]) outlines specific actions for the aeronautical users and air navigation service provider.

A1.4.2 Consideration for receiver antenna patterns for aeronautical GNSS receivers

The actual antenna gain of the victim GNSS receiver depends on the direction of the received signal. Representative antenna diagrams for aeronautical GNSS receivers are defined in RTCA DO-229 EUROCAE ED 259 [4] and DO-373 [12] as in Figure 3 (upper hemisphere antenna pattern) and in Figure 4 (lower hemisphere antenna pattern). The lower hemisphere antenna pattern includes aircraft fuselage shadowing.

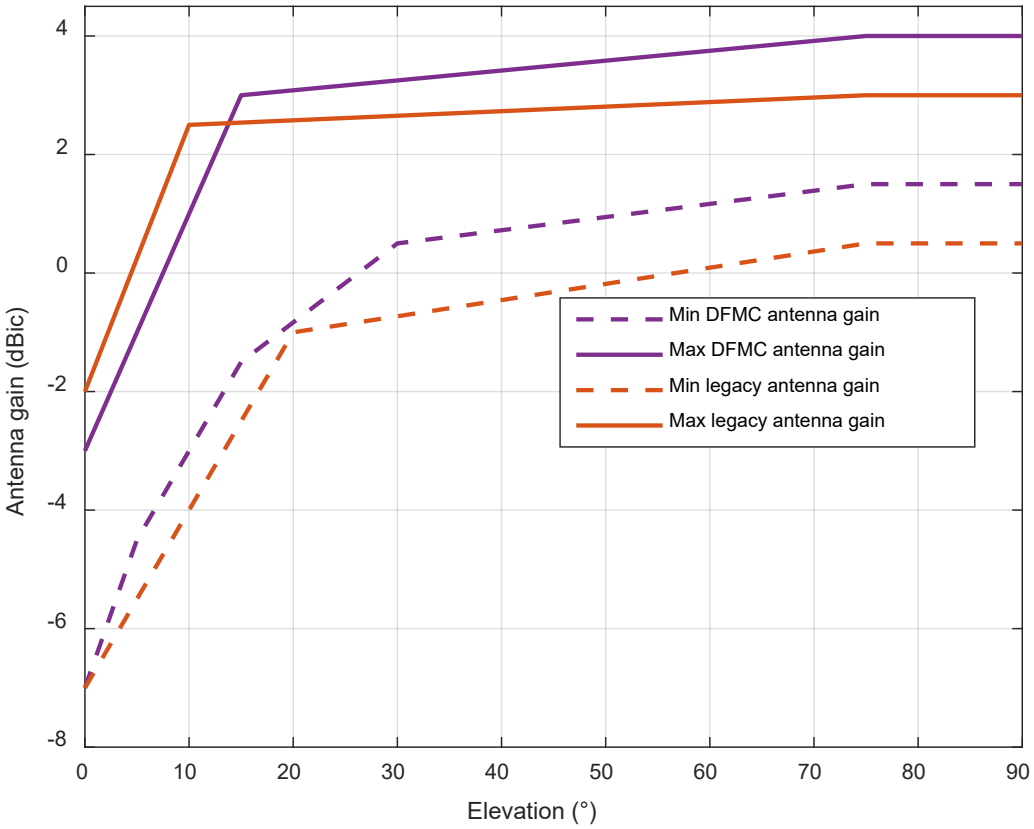


Figure 3: Upper hemisphere passive antenna gain limits

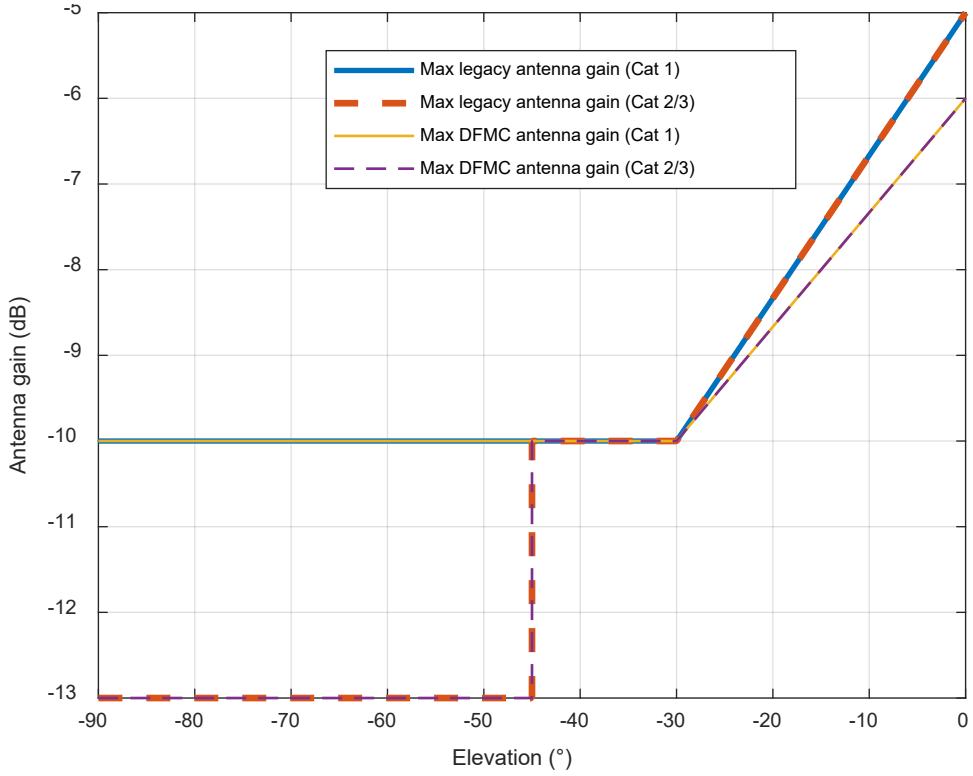


Figure 4: Lower hemisphere passive antenna maximum gain

A1.4.3 Impacted area

The distance at which the receiver may be impacted by the interference when the aircraft is at an altitude H is the minimum among the radio horizon line of sight and d_{impact} defined by equation (1):

$$d_{impact} = \sqrt{\frac{P_{Tx} G_{Tx} G_{Rx}}{Th_{Rx}} \left(\frac{c}{4\pi f}\right)^2 - H^2} \quad (1)$$

where:

- P_{Tx} is the jammer transmitting power (in W);
- G_{Tx} is the jammer antenna gain (linear unit);
- G_{Rx} is the GNSS receiver antenna gain (linear unit - see section A1.3.2);
- Th_{Rx} is the GNSS receiver interference threshold, as defined in Annex 2 and Annex 3 (in W);
- f is the carrier frequency of the jammer signal (in Hz);
- c is the speed of light (3×10^8 m/s).

In case the interferer transmitted power is low, then the above formula may not allow to compute $d_{impact.}$. In this case, this would imply that the vertical separation would be sufficient to ensure the protection of the receiver.

In order to further clarify the impact zone, it is recommended to mention the radius of the impacted zones for different flight levels.

If the deployed jammer antenna is highly directional (e.g. horn antenna) and the direction of the radiation is planned and fixed, it may be relevant 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.

ANNEX 2: IMPACT OF JAMMING OPERATIONS ON GNSS RECEIVERS.

This annex contains elements allowing to assess the impact of different kind of jamming on GNSS receivers. The limits are based on the interference criteria for the aeronautical GNSS receivers and applied for land, maritime and aeronautical cases.

This section contains interference masks characterising the resilience of civil aviation GNSS receivers to defined types interference. This is considered to provide a useful benchmark for other sectors, considering the sensitivity of interference impact on equipment used in aviation. These masks are used in certification testing procedures of GNSS civil aviation receiver and are taken from ICAO, annex 10, vol 1 [7]. Current civil aviation GNSS receiver are designed to process Global Positioning System (GPS) and Satellite-based Augmentation Systems (SBAS) signals in the 1559-1610 MHz band. A new generation of civil aviation GNSS receivers is under development, referred as Dual Frequency Multi Constellation (DFMC) GNSS receivers. The deployment of DFMC receivers is expected to start in the coming years. These receivers will have the capability to process signals from different constellations (GPS, Galileo and SBAS) in the frequency bands 1559-1610 MHz and 1164-1215 MHz.

Four interference thresholds exist depending on the nature (or type) of the interference:

- Threshold for continuous wave interference, whose central frequency is either within or outside the GNSS frequency bands;
- In-band noise-like interference threshold as a function of the interference bandwidth, assuming the interference central frequency is within the GNSS frequency range;
- Threshold for pulse interference;
- Experience based limits established from live-sky interference testing. The national security entity performing the GNSS interference tests can consider these experience-based thresholds 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.

A2.1.1 Resilience to continuous wave (CW) interference

After steady-state navigation has been established, GPS L1/SBAS L1 receivers and DFMC receivers can resist CW interfering signals present with a power level at the antenna port equal to the interference thresholds exemplified by the defined masks for aeronautical receivers shown in Figure 5 (for GPS L1/SBAS L1 receivers) and in Figure 6 (for DFMC receivers). The thresholds in Figure 5 and Figure 6 are defined to ensure that minimum performance for GNSS tracking and demodulation signal processing stages are fulfilled. The most constraining signal processing function in the 1559-1610 MHz band is identified as the pseudorange accuracy performance for a GPS satellite with 5° elevation. The most constraining signal processing function in the 1164-1215 MHz band is the demodulation of SBAS L5 signal.

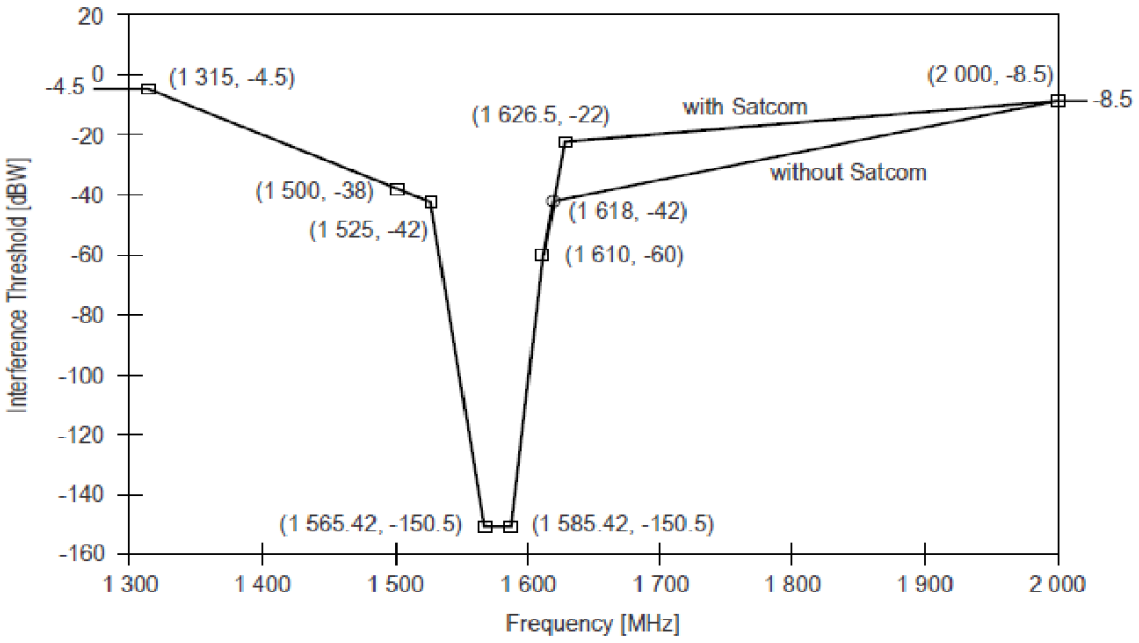


Figure 5: CW interference thresholds for GPS L1/SBAS L1 receivers in steady-state navigation

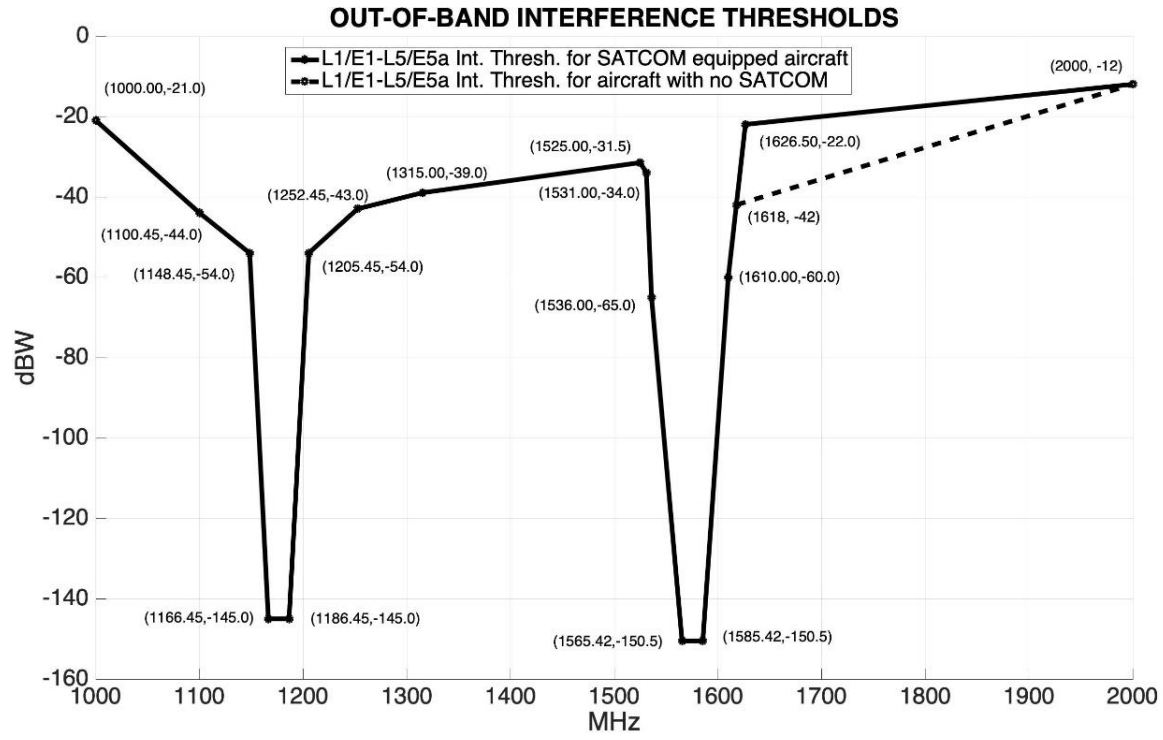


Figure 6: CW interference thresholds for DFMC receivers in steady-state navigation

In addition, during initial acquisition of GNSS signals in the band 1559-1610 MHz prior to steady-state navigation, GNSS receivers shall meet the performance objectives with interference thresholds 6 dB less than those of Figure 5 and Figure 6; as specified in ICAO, annex 10, vol 1 [7].

For example, for in band interference hitting the frequency band 1559-1610 MHz, GNSS receivers can tolerate an interference power of -150.5 dBW (see Recommendation ITU-R M.1903 [3]) 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 should not exceed -156.5 dBW.

A2.1.2 Band-limited noise-like interference

After steady-state navigation has been established, GNSS receivers can resist noise-like interfering signals within the range 1575.42 MHz $\pm$ $BW_i/2$ and present with a power level at the antenna port equal to the interference thresholds exemplified by the one for aeronautical receivers shown in Figure 7. BW_i is the interfering signal bandwidth. During initial acquisition of GNSS signals within the band 1559-1610 MHz before steady-state navigation has been established, GNSS receivers shall meet the performance objectives with interference thresholds 6 dB lower than those applicable for steady state navigation; as specified in ICAO, annex 10, vol. 1 [7].

Similarly, when the noise like interfering signal is within the range 1176.42 $\pm$ $BW_i/2$, GNSS receivers can tolerate a power level at the antenna port equal to the interference thresholds exemplified by the defined masks for aeronautical receivers shown in Figure 8. In this case, the mask of Figure 8 is applicable for initial acquisition as well as after steady state navigation has been established.

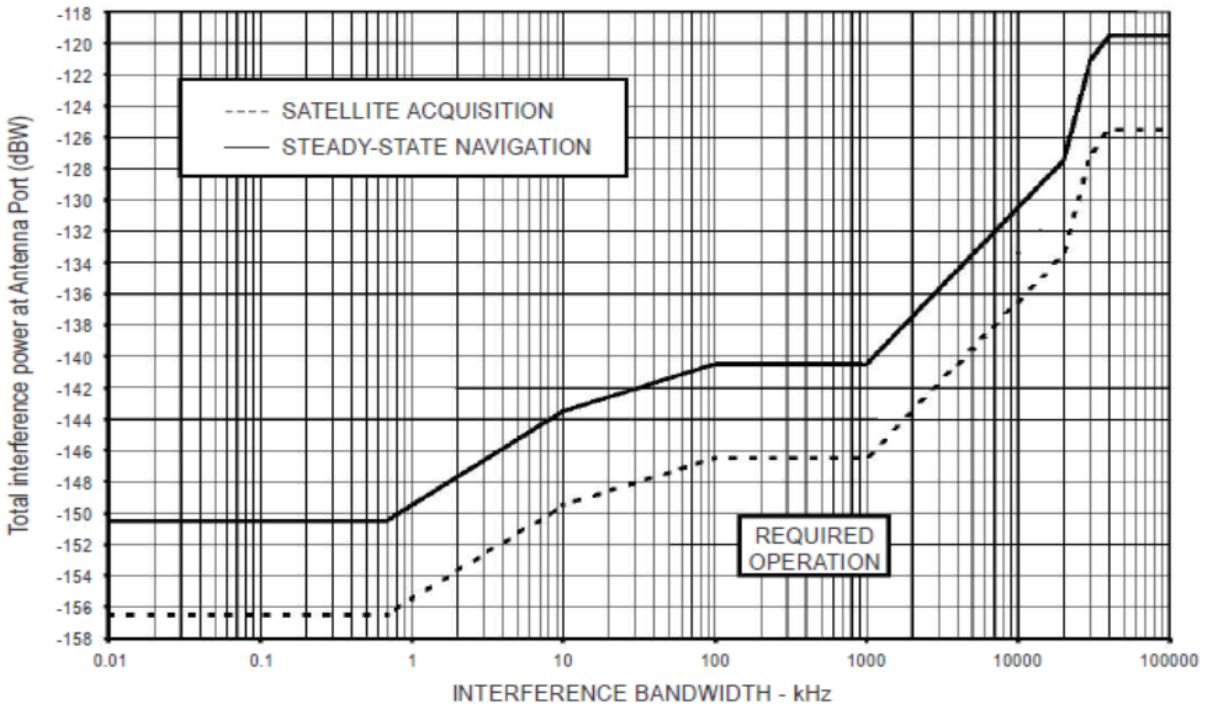


Figure 7: In-band interference thresholds versus bandwidth for GNSS receivers when the interference is in the frequency range 1575.42 MHz $\pm$ $BW_i/2$

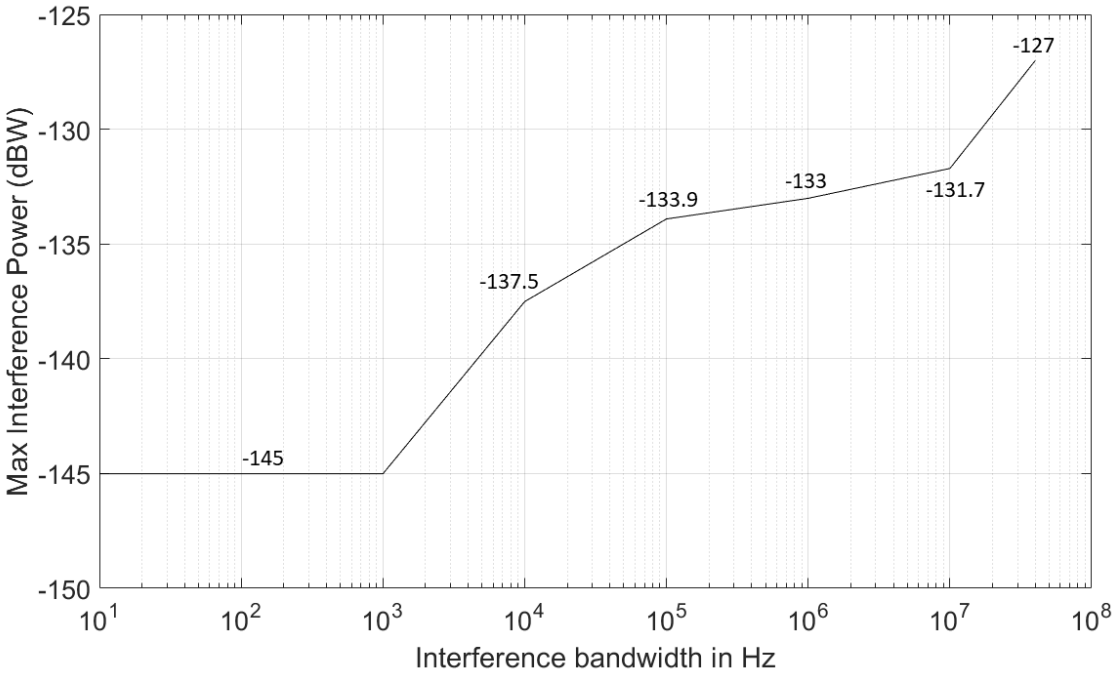


Figure 8: In-band interference thresholds versus bandwidth for GNSS receivers when the interference is in the frequency range 1176.45 MHz ± $BW_i/2$

In complement of the interference thresholds, GNSS receivers are tested and certified assuming that for interference bandwidths greater than 1 MHz, the interference threshold does not exceed -140.5 dBW/MHz in the frequency range 1575.42 ± 10 MHz and -134 dBW/MHz in the frequency range 1176.45 ± 10 MHz.

For narrow band interference, the thresholds in Figure 7 and Figure 8 are similar to CW thresholds for in band interference (Figure 5 and Figure 6 respectively).

A2.1.3 Pulsed interference

After steady-state navigation has been established, the GNSS receiver can resist pulsed interference signals with characteristics according to Table 1.

Table 1: Pulse interference threshold

Parameter	Value
Frequency range for in-band and near-band	1575.42 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 (Note 1)
Pulse width	≤ 125 µs
Pulse duty cycle	≤ 1%
Interference signal bandwidth for in-band and near-band interference	≥ 1 MHz

Note 1: When considering the L1 channel of an L1/L5 receiver, this value is related to non-aeronautical pulsed interferences with a carrier frequency within 1215-2000 MHz. This table does not describe non-aeronautical pulsed interferences in the environment to be considered for the L5 channel in an L1/L5 receiver.

A2.1.4 Experience based limits

One CEPT administration has conducted live-sky GNSS interference testing over the past 20 years, arranging interference testing both in national only events, and with international participation in the NATO context, as well as bi- and multi-lateral collaborations (e.g. the yearly Jammertests at Andøya, Norway, from 2022 to 2025).

In their campaigns with live-sky GNSS jamming, simulations of the J/S values (the ratio between the jamming signal and the authentic satellite signal) are calculated in advance using terrain models. The results showed J/S-thresholds based on the resilience of GNSS receivers as stated below and visualised in Figure 9:

- 24 dB J/S – Acquisition phase (receivers to acquire signals from startup (cold start));
- 43 dB J/S – Reduced performance when in steady-state;
- 54 dB J/S – Receivers lose fix.

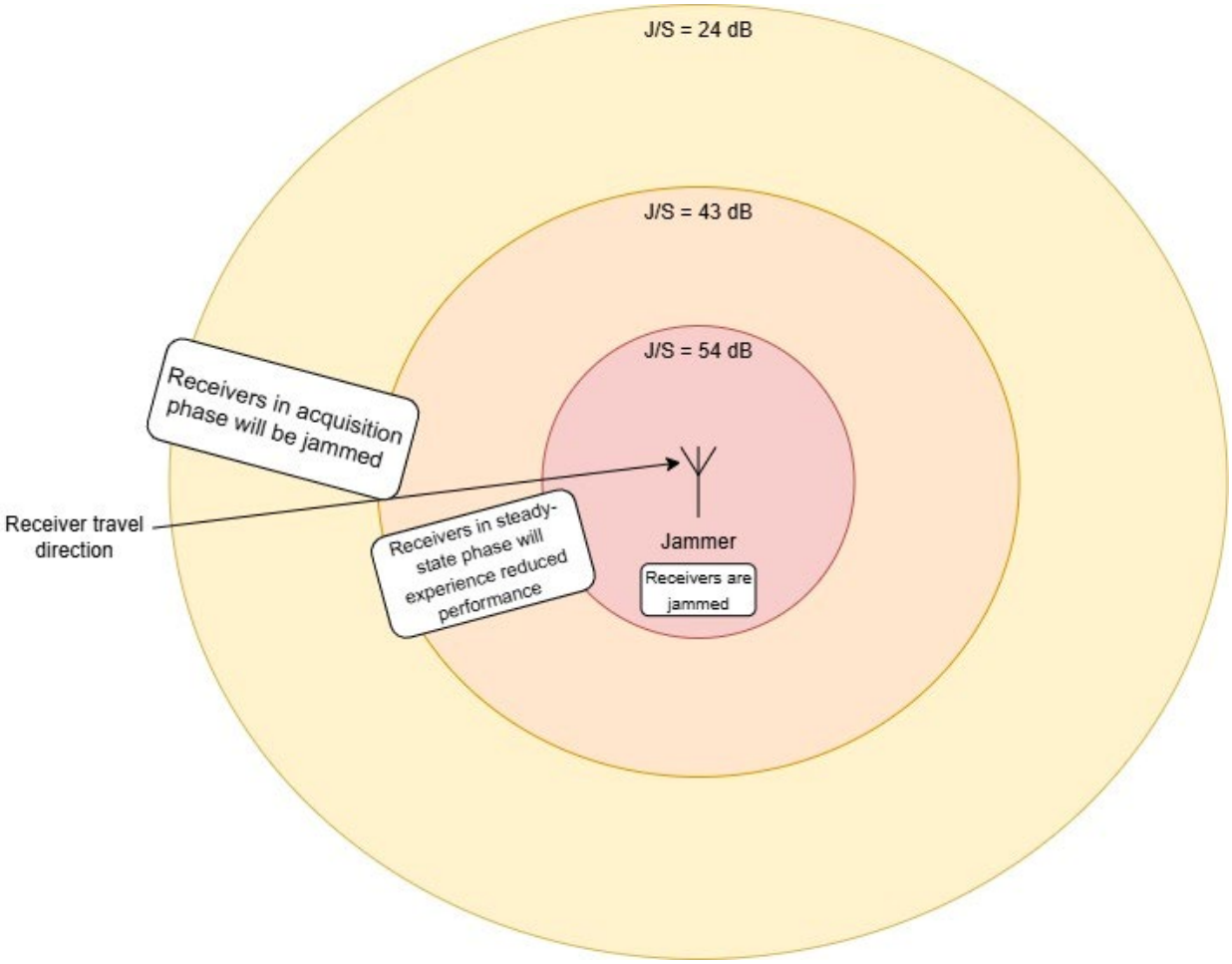


Figure 9: Visualisation of experience based limits

When assessing the possible impacts of a specific jamming operation, administrations may take into account these values to estimate interference exposure volume to complement the other thresholds presented in the previous section.

Reference for these J/S experience-based values are:

- Receiver using GPS L1 band, 1563-1587 MHz;
- Centre frequency of jamming signal 1575.42 MHz;
- Bandwidth of jamming signal 24 MHz;
- Ground-level reception at 1.5 metres.

Satellite reception power is assumed to be -160 dBW.

ANNEX 3: IMPACT OF SPOOFING OPERATION ON GNSS RECEIVERS

Spoofing is defined as the emission of GNSS-like signals that may be acquired and tracked in combination with or instead of the intended signals. The limits are based on the interference criteria for the aeronautical GNSS receivers and applied for land, maritime and aeronautical cases.

A3.1 IMPACT OF SPOOFING SIGNAL ON GNSS RECEIVERS

Spoofing consequences would be very different compared to jamming consequences, due to the different nature of the interference. While jamming degrades continuity and availability performance of GNSS receivers, spoofing can also have an impact on integrity performance by inducing misleading outputs. As a consequence, spoofing can lead to undetected errors on measurements, and consequently, to major safety risk, during and after having exposed a receiver to spoofed signals.

Currently, certification test procedures for GPS/SBAS L1 civil aviation GNSS receivers do not include testing of the receiver detection or robustness against spoofing. It is therefore difficult to predict the behaviour of GNSS receivers in presence of spoofing signals.

A3.1.1 Impact on tracking

ECC Report 129 [5] indicates that the maximum tolerable received interference power for spoofing tests is 10 dB lower than authentic signal power level of an individual GNSS satellite. ECC Report 129 expects that, provided that interference received power for spoofing tests remains 10 dB lower than authentic signal power level of an individual GNSS satellite, the maximum pseudo range error for one satellite would be 1.7 m. The error on the positioning, which is derived from several signals, would be even lower. However, ECC Report 129 addresses limited-latency repeaters only and assumes that no disruption in the GNSS service occurs. In addition, quantification of the degradation of key GNSS performance criteria for aviation (integrity, continuity, availability and accuracy) due to the repeater is not investigated. In addition, ECC Report 129 does not investigate the consequences of the degradation of some performance indicators (C/N0 estimations, signal quality monitoring, etc) on the GNSS receiver behaviour.

A3.1.2 Impact on acquisition

In case a disruption of the GNSS occurs, or when a new satellite becomes visible, the GNSS receiver must perform the acquisition of the new signal. The acquisition consists of detecting the presence of a GNSS signal, by estimating the code phase delay and frequency of this incoming GNSS signal.

Since the code phase delay and frequency of the GNSS signal to acquire are a priori unknown at the beginning of the acquisition process, a bi-dimensional matrix is explored to identify the transmission of a satellite. The acquisition is then performed by finding peaks in the acquisition matrix that exceeds the acquisition threshold.

In presence of spoofing and authentic signals, the acquisition matrix could contain two peaks (one for the signal of interest, one for the spoofing signal), as illustrated in Figure 10, even if the spoofed signal power is much lower than the real GNSS signal power. Depending on the architecture of the acquisition stage of the receiver, the receiver may therefore acquire the spoofed signal without detecting the correct signal.

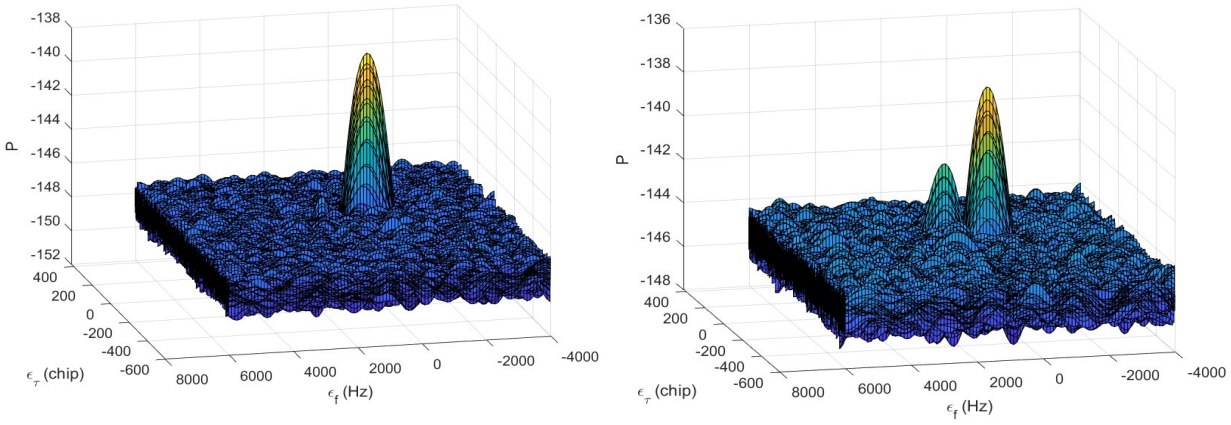


Figure 10: Acquisition matrix without spoofed signal (left) and in presence of a spoofed signal (right)

The maximum ratio of -10 dB between interference power and authentic signal power, as proposed in ECC Report 129 [5], is insufficient to prevent aeronautical GNSS receivers from acquiring the spoofing signals and should not be considered as a spoofing threshold for acquisition. Spoofing tests designed and conducted with this value for spoofing signal power may lead aviation receivers to acquire the spoofing signal, thereby compromising GNSS performance including integrity, as illustrated above.

A3.1.3 Experience based levels

Testing with spoofing (and meaconing) has only been done in the last 10 years and less experience have been gained with spoofing than jamming. There are many types of spoofing tests and variations on how the spoofing signals are created, i.e. dynamics, power levels, time coherence etc., which have vastly different effects on receivers. During testing, power levels were calibrated according to effects shown on a set of receivers at a given distance from the signal source ensuring no effects of the receiver set outside the established testing area. From this past experience, the spoofing signal power often needs to be 10 to 20 dB over the authentic signals. In a laboratory though, a few dB over the authentic signal have been stated to be effective.

It should be emphasized that these experiments were conducted on a limited subset of spoofing strategies, GNSS receivers, and satellite constellation geometries.

A3.1.4 Threshold to be considered

It is recommended that CEPT administrations use three criteria to identify the spoofing risk:

1 The susceptibility levels established based on experience from testing where impacts are experienced. When assessing the possible impacts of a spoofing operation, administrations could consider experience-based results to estimate interference exposure volume in complement to the other thresholds presented above, while also taking into account the difference of behaviour between devices in presence of spoofing signals.

2 The ratio between spoofed signal power and authentic GNSS signal power of -10 dB at the victim receiver (see EUROCONTROL Report [6], based on ECC Report 129 [5] and ETSI EN 302 645 [11] on GNSS repeaters) to limit the degradation on pseudorange accuracy caused by repeaters. According to EUROCONTROL Report [6], the limit of -170 dBW is used to limit the impact of short-latency repeaters on GNSS accuracy.

   The radio line of sight between the GNSS receiver and the spoofing transmitter, where it is considered that there exists a risk for the GNSS receiver to be adversely affected by spoofing effects. Such collateral effects on the service integrity may impact any function relying on GNSS. Such effects may persist after the end of exposure to the incriminated adverse RF signals. In this case the exposure area radius can be computed by equation (2):

$$Radio\ horizon\ radius(\text{km}) = 4.12\left(\sqrt{h_1} + \sqrt{h_2}\right) \quad (2)$$

where:

- h_1 is the aircraft altitude in meters;
- h_2 is the spoofing transmitter altitude in meters.

Considering those three criteria may better reflect the potential risks for CEPT administrations when authorising such GNSS spoofing operations.

The national security entity performing the GNSS interference tests can consider higher power levels exceeding the sensitivity thresholds recommended in this document 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.

ANNEX 4: EXAMPLES OF INTERFERENCE TESTING NOTIFICATION

A4.1 NOTIFICATION TO MARITIME USERS

The information below provides three examples of Navigation Warning Notices (NAVWARN) to inform maritime and other GNSS users about the temporary unavailability or degradation of GNSS services due to planned and approved jamming or spoofing operations.

The objective is to ensure that all potentially affected users are properly notified through appropriate maritime and information channels, minimising operational and safety risks. Navigation warnings should be issued through recognised national or international maritime communication systems, such as NAVTEX, SafetyNET, or equivalent coastal radio broadcasting services.

Notices should be concise, clear, and time-bound, indicating the affected geographic area, the expected period of impact, and the type of interference (GNSS jamming or spoofing). Warnings should be disseminated sufficiently in advance of the operation to allow mariners and other users to plan alternative navigation means. The notice should include a contact point for further information or for reporting unexpected GNSS degradation.

Table 2: Examples of Navigation Warning Notices (NAVWARN)

Example	Example in English	Example in Local Language
1	AVURNAV TOULON 432/25 AIDS TO NAVIGATION GNSS DEGRADATION 1. DUE TO SPOOFING AND JAMMING ACTIVITIES, SATELLITE NAVIGATION SIGNALS MAY BE DEGRADED, UNAVAILABLE OR MISLEADING IN AREA BOUNDED BY: A. 43-10.0N 006-00.0E B. 43-10.0N 006-30.0E C. 42-50.0N 006-30.0E D. 42-50.0N 006-00.0E 2. DO NOT RELY SOLELY ON GNSS BUT VERIFY POSITIONS USING RADAR, VISUAL REFERENCES, DEPTH SOUNDERS AND DR PLOTTING. DISABLE THE AUTOMATIC PILOT OR ROUTE FOLLOWING MODE OF ECDIS/GPS. TREAT AIS POSITIONS WITH CAUTION. NAVIGATE WITH CAUTION AT REDUCED SPEED. REPORT GNSS ANOMALIES TO THE NEAREST CROSS (VHF 16), INDICATING UTC TIME, POSITION AND SYMPTOMS. 3. CANCEL AVURNAV 417/25 4. CANCEL THIS MSG ON 291900 UTC AUG 25	AVURNAV TOULON 432/25 AIDES A LA NAVIGATION DEGRADATION GNSS 1. EN RAISON D'ACTIONS DE SPOOFING ET JAMMING, LES SIGNAUX DE NAVIGATION PAR SATELLITE PEUVENT ETRE DEGRADES, INDISPONIBLES OU TROMPEURS DANS LA ZONE : A. 43-10.0N 006-00.0E B. 43-10.0N 006-30.0E C. 42-50.0N 006-30.0E D. 42-50.0N 006-00.0E 2. NE PAS SE FIER UNIQUEMENT AU GNSS MAIS VERIFIER LES POSITIONS A L'AIDE DU RADAR, DES REPERES VISUELS, DES SONDES DE PROFONDEUR ET DE L'ESTIME. DESACTIVER LE MODE DE PILOTAGE AUTOMATIQUE OU DE SUIVI DE ROUTE DES ECDIS/GPS. TRAITER LES POSITIONS AIS AVEC PRUDENCE. VITESSE REDUITE ET VEILLE ATTENTIVE RECOMMANDEE. SIGNALER LES ANOMALIES GNSS AU CROSS LE PLUS PROCHE (VHF 16) EN INDIQUANT L'HEURE UTC, LA POSITION ET LES SYMPTOMES. 3. ANNULER AVURNAV 417/25 4. ANNULER CE MSG LE 291900 UTC AOU 25

Example	Example in English	Example in Local Language
2	AVURNAV BREST XXX/25 AIDS TO NAVIGATION GNSS DEGRADATION 1. DUE TO SPOOFING AND JAMMING ACTIVITIES, SATELLITE NAVIGATION SIGNALS MAY BE DEGRADED, UNAVAILABLE OR MISLEADING IN AREA BOUNDED BY: A. 46-00.0N 005-00.0W B. 46-00.0N 004-00.0W C. 45-20.0N 004-00.0W D. 45-20.0N 005-00.0W 2. DO NOT RELY SOLELY ON GNSS BUT VERIFY POSITIONS USING RADAR, VISUAL REFERENCES, DEPTH SOUNDERS AND DR PLOTTING. DISABLE THE AUTOMATIC PILOT OR ROUTE FOLLOWING MODE OF ECDIS/GPS. TREAT AIS POSITIONS WITH CAUTION. NAVIGATE WITH CAUTION AT REDUCED SPEED. REPORT GNSS ANOMALIES TO THE NEAREST CROSS (VHF 16), INDICATING UTC TIME, POSITION AND SYMPTOMS. 3. CANCEL AVURNAV 417/25 4. CANCEL THIS MSG ON 291900 UTC AUG 25	AVURNAV BREST XXX/25 AIDES A LA NAVIGATION DEGRADATION GNSS 1. EN RAISON D'ACTIONS DE SPOOFING ET JAMMING, LES SIGNAUX DE NAVIGATION PAR SATELLITE PEUVENT ETRE DEGRADES, INDISPONIBLES OU TROMPEURS DANS LA ZONE : A. 46-00.0N 005-00.0W B. 46-00.0N 004-00.0W C. 45-20.0N 004-00.0W D. 45-20.0N 005-00.0W 2. NE PAS SE FIER UNIQUEMENT AU GNSS MAIS VERIFIER LES POSITIONS A L'AIDE DU RADAR, DES REPERES VISUELS, DES SONDES DE PROFONDEUR ET DE L'ESTIME. DESACTIVER LE MODE DE PILOTAGE AUTOMATIQUE OU DE SUIVI DE ROUTE DES ECDIS/GPS. TRAITER LES POSITIONS AIS AVEC PRUDENCE. VITESSE REDUITE ET VEILLE ATTENTIVE RECOMMANDEE. SIGNALER LES ANOMALIES GNSS AU CROSS LE PLUS PROCHE (VHF 16) EN INDIQUANT L'HEURE UTC, LA POSITION ET LES SYMPTOMES. 3. ANNULER AVURNAV XXX/25 4. ANNULER CE MSG LE 291900 UTC AOU 25
3	AVURNAV CHERBOURG XXX/25 AIDS TO NAVIGATION GNSS DEGRADATION 1. DUE TO SPOOFING AND JAMMING ACTIVITIES, SATELLITE NAVIGATION SIGNALS MAY BE DEGRADED, UNAVAILABLE OR MISLEADING IN AREA BOUNDED BY: A. 49-45.0N 002-00.0W B. 49-45.0N 001-00.0W C. 49-15.0N 001-00.0W D. 49-15.0N 002-00.0W 2. DO NOT RELY SOLELY ON GNSS BUT VERIFY POSITIONS USING RADAR, VISUAL REFERENCES, DEPTH SOUNDERS AND DR PLOTTING. DISABLE THE AUTOMATIC PILOT OR ROUTE FOLLOWING MODE OF ECDIS/GPS.	AVURNAV CHERBOURG XXX/25 AIDES A LA NAVIGATION DEGRADATION GNSS 1. EN RAISON D'ACTIONS DE SPOOFING ET JAMMING, LES SIGNAUX DE NAVIGATION PAR SATELLITE PEUVENT ETRE DEGRADES, INDISPONIBLES OU TROMPEURS DANS LA ZONE : A. 49-45.0N 002-00.0W B. 49-45.0N 001-00.0W C. 49-15.0N 001-00.0W D. 49-15.0N 002-00.0W 2. NE PAS SE FIER UNIQUEMENT AU GNSS MAIS VERIFIER LES POSITIONS A L'AIDE DU RADAR, DES REPERES VISUELS, DES SONDES DE PROFONDEUR ET DE L'ESTIME.

Example	Example in English	Example in Local Language
	TREAT AIS POSITIONS WITH CAUTION. NAVIGATE WITH CAUTION AT REDUCED SPEED. REPORT GNSS ANOMALIES TO THE NEAREST CROSS (VHF 16), INDICATING UTC TIME, POSITION AND SYMPTOMS. 3. CANCEL AVURNAV 417/25 4. CANCEL THIS MSG ON 291900 UTC AUG 25	DESACTIVER LE MODE DE PILOTAGE AUTOMATIQUE OU DE SUIVI DE ROUTE DES ECDIS/GPS. TRAITER LES POSITIONS AIS AVEC PRUDENCE. VITESSE REDUITE ET VEILLE ATTENTIVE RECOMMANDEE. SIGNALER LES ANOMALIES GNSS AU CROSS LE PLUS PROCHE (VHF 16) EN INDIQUANT L'HEURE UTC, LA POSITION ET LES SYMPTOMES. 3. ANNULER AVURNAV XXX/25 4. ANNULER CE MSG LE 291900 UTC AOU 25

A4.2 NOTIFICATION TO AERONAUTICAL USERS

A4.2.1 Aeronautical Information Services (AIS) – GNSS RFI NOTAM[2]

Sector-specific notifications, e.g. NOTAMs for the aviation sector, containing all relevant information for potential users should be issued by the responsible authorities or service providers before the execution of the GNSS interference testing.

If the GNSS interference testing requires the temporary activation of danger or restricted areas, an appropriate notification, e.g. a NOTAM containing the elements detailed in section A4.2.2 should be issued by the responsible authority or service provider.

A4.2.2 Aeronautical Information Publication Supplement (AIP SUP)

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;
- references to the corresponding NOTAMs;
- GNSSTEST-GM49: see EUROCONTROL Report for the details;
- Aeronautical Information Circular (AIC).

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;

[2] Further information on the use of NOTAMs can be found in [6].

- contact details of the person in charge of the INTERRUPTION procedure;
- Reporting to the Network Manager.

CEPT administration may report RF interference originating outside their country through the official ITU tool satellite interference reporting and resolution system (SIRRS). RF Interference may be based on a regular notified RNSS station to the ITU.

A4.2.3 Examples of NOTAM

This section contains examples of NOTAMs.

A4.2.3.1 Jamming testing

DISTURBANCE OF THE SIGNAL RECEIVED BY GPS RECEIVERS IN DIFFERENT POSITIONS
CENTERED ON THE POINT 421346N 0064500E - POSSIBLE GNSS JAMMING, IMPACT VOLUME CENTERED ON THE ABOVE COORDINATES :
324NM FOR FL400
273NM FOR FL250
229NM FOR FL150
201NM FOR FL100
156NM AT 4000FT
- INFO 'CCMAR MEDITERRANEE FANNY CONTROL' 127.975MHZ/375.350MHZ
- IN CASE OF OBSERVED GPS INTERFERENCE, REPORT THE INFORMATION TO THE COMPETENT ATS SERVICES.

FROM: 29 SEP 2025 08:00 **TO:** 03 OCT 2025 10:00

A4.2.3.2 Spoofing testing

EPWW-C0824/25
DU: 12 09 2025 08:38 AU: 12 12 2025 23:50 EST
A) EPWW
Q) EPWW / QAFXX / IV / NBO / E / 000/999 / 5202N01855E999
E) GNSS JAMMING AND SPOOFING OCCURRENCES CAN BE EXPECTED WITHIN FIR EPWW. AIR CREWS TO REMAIN VIGILANT AND TO REPORT TO ATS. CONVENTIONAL NAVIGATION AIDS AVAILABLE.

EYVN-A5899/25
DU: 30 10 2025 09:15 AU: 30 01 2026 23:59 EST
A) EYVL
Q) EYVL / QGWXX / IV / NBO / E / 000/999 / 5546N02229E155
E) PRECAUTION-GNSS SIGNAL JAMMING AND SPOOFING CAN BE EXPECTED IN VILNIUS FIR MOSTLY IN WESTERN AND SOUTHERN PARTS. CONVENTIONAL NAV AIDS AVAILABLE AND MAY BE USED AS RECOMENDED IN EASA SIB 2022-02. AIR CREW ARE ASKED TO INFORM AN ATC OF ANY GNSS NTERFERENCE DETECTED

ANNEX 5: LIST OF REFERENCES

[1] Resolution 676 (WRC-23): “Prevention and mitigation of harmful interference to the radionavigation-satellite service in the frequency bands 1 164-1 215 MHz and 1 559-1 610 MHz”

[2] Report ITU-R M.2458: ”Radionavigation-satellite service applications in the 1 164-1 215 MHz, 1 215-1 300 MHz and 1 559-1 610 MHz frequency bands”

[3] Recommendation ITU-R M.1903: “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”

[4] RTCA DO-229/ED259: “Minimum Operational Performance Standards (MOPS) for Global Positioning System/Satellite-Based Augmentation System Airborne Equipment”

[5] ECC Report 129: “Technical and operational provisions required for the use of GNSS repeaters”, approved January 2009

[6] “EUROCONTROL Guidelines on a Process for Civil and Military GNSS Interference Testing”, 2023

[7] ICAO Annex 10, Aeronautical Telecommunications, Volume I, “Radio Navigation Aids”, 7th Edition including Amendment 92, 2020

[8] ETSI EN 303 413: “Satellite Earth Stations and Systems (SES); Global Navigation Satellite System (GNSS) receivers; Radio equipment operating in the 1 164 MHz to 1 300 MHz and 1 559 MHz to 1 610 MHz frequency bands; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU”

[9] ECC Recommendation (04)01: “With regard to the prohibition of jammers in the CEPT countries”, approved February 2004, latest amendment February 2025

[10] IMO MSC.1/Circ.1644 Deliberate interference with the United States' global positioning system (GPS) and other global navigation satellite systems (GNSS)

[11] ETSI EN 302 645: “Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices; Global Navigation Satellite Systems (GNSS) Repeaters; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive” (currently under revision towards a Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU)

[12] RTCA DO-373: "MOPS for GNSS Airborne Active Antenna Equipment for the L1/E1 and L5/E5a Frequency Bands "