PD CEN/TR 17475:2020



BSI Standards Publication

Space — Use of GNSS-based positioning for road Intelligent Transport System (ITS) — Specification of the test facilities, definition of test scenarios, description and validation of the procedures for field tests related to security performance of GNSS-based positioning terminals

bsi.

Documents
Document Sharing Hub

Full document details: PD CEN/TR 17475:2020

National foreword

This Published Document is the UK implementation of CEN/TR 17475:2020.

The UK participation in its preparation was entrusted to Technical Committee ACE/68, Space systems and operations.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 06987 7

ICS 03.220.20; 33.060.30; 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2020.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD CEN/TR 17475:2020

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 17475

April 2020

ICS 33.060.30; 03.220.20; 35.240.60

English version

Space - Use of GNSS-based positioning for road Intelligent Transport System (ITS) - Specification of the test facilities, definition of test scenarios, description and validation of the procedures for field tests related to security performance of GNSS-based positioning terminals

Espace - Utilisation de la localisation basée sur les GNSS pour les systèmes de transports routiers intelligents (ITS) - Spécification des installations d'essais, définition des scénarios d'essais, description et validation des procédures d'essais sur le terrain en matière de performances de sécurité des terminaux de positionnement basés sur les GNSS

Spezifikation der Testeinrichtungen, Definition von Testszenarien, Beschreibung und Validierung der Verfahren für Feldtests in Bezug auf die Sicherheitsleistung von GNSS-basierten Ortungsterminals

This Technical Report was approved by CEN on 7 March 2020. It has been drawn up by the Technical Committee CEN/CLC/JTC 5.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.





CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

© 2020 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members.

Ref. No. CEN/TR 17475:2020 E

Documents
Document Sharing Hub

Full document details: PD CEN/TR 17475:2020

Contents

Page

European foreword ... 4
1 Scope ... 5
1.1 Purpose of the document ... 5
1.2 Overview of the document ... 5
2 Normative references ... 5
3 Terms and definitions ... 6
4 List of acronyms ... 10
5 GNSS Threats overview ... 11
5.1 General ... 11
5.2 Denial of service: jamming ... 11
5.3 Deception of service: spoofing and meaconing ... 13
6 Security metrics ... 16
6.1 General approach ... 16
6.1.1 Introduction ... 16
6.1.2 Notes on empirical CDF ... 17
6.1.3 ECDF with loss of samples ... 19
6.2 Considered metrics ... 22
6.2.1 General ... 22
6.2.2 Accuracy ... 22
6.2.3 Integrity ... 24
6.2.4 Availability and continuity ... 28
6.3 Other metrics ... 30
6.3.1 Time To Fist Fix (TTFF) ... 31
6.3.2 Excluded metrics ... 31
6.4 Robustness concept: a summary metric ... 32
7 Test approach ... 32
7.1 SDR concept ... 33
7.2 Interference hardware impact ... 33
7.2.1 General ... 33
7.2.2 Antenna-LNA ... 34
7.2.3 AGC ... 34
7.2.4 ADC ... 34
7.2.5 Digital post-correlation processing ... 35
7.3 Record and replay choice ... 37
7.4 Jamming testing architecture ... 38
7.5 Spoofing testing architecture ... 40
7.6 File size and scenario length ... 42
7.7 Hybridization issue ... 43
8 Test scenarios ... 43
8.1 Relevant realistic scenarios ... 44
8.1.1 Nominal scenarios ... 44
8.1.2 Clear sky scenario as a special case ... 44

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

8.1.3 Scenario VS Data set VS Datafile 45
8.1.4 Scenario-management authority 45
8.2 Interference scenarios selection 45
8.2.1 Jamming proposed scenarios 46
8.2.2 Spoofing proposed scenarios 47
8.2.3 Meaconing assessment 49
8.2.4 Meaconing proposed scenarios 49

9 Test facilities specification 50
9.1 Data set record testbed 50
9.1.1 General 50
9.1.2 Jamming data generation 50
9.1.3 Spoofing data recording 54
9.2 Replay testbed 55
9.2.1 RF transmitters calibration 55
9.2.2 Replay testbed schemes 57

10 End-to-end validation 58
10.1 Devices under test 58
10.2 Nominal scenario recording and validation 60
10.2.1 Nominal scenario recording 60
10.2.2 Analytical tools 63
10.2.3 Nominal scenario validation 65
10.3 Jamming test results 73
10.3.1 General 73
10.3.2 Jamming scenarios generation 73
10.3.3 Interferences on AsteRx3 HDC 75
10.3.4 Interferences on Ublox 8 92
10.4 Spoofing test results 106
10.4.1 Spoofing scenario recording 106
10.4.2 Spoofing on AsteRx-3 HDC 106
10.4.3 Spoofing on Ublox 8 110

Annex A (informative) AGC principles and impact 115

Annex B (informative) GNSS SDR Format standardization 118

Annex C (informative) Spoofing insights 120

C.1 General 120

C.2 Range error impact 121

C.3 Oscillator error impact 121

C.4 Propagation channel impact 122

Annex D (informative) Noise amplification 124

D.1 Theory of noise amplification 124

D.2 Experimental validation 128

Annex E (informative) Accuracy and continuity simulations 130

Bibliography 135

Documents
Document Sharing Hub

Full document details: PD CEN/TR 17475:2020

European foreword

This document (CEN/TR 17475:2020) has been prepared by Technical Committee CEN-CENELEC/TC 5 “Space”, the secretariat of which is held by DIN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

1 Scope

1.1 Purpose of the document

This document is the CEN Technical Report WP2-D2 of the GP-START project, regarding the test procedures for assessment of robustness to security attacks.

Starting from the definition of security attacks taxonomy and security metrics highlighted in CEN/TR 17464, this task aims to:

1. Specify test facilities to be used in the field tests. This comprises both hardware and software equipment.

2. Define relevant test scenarios applicable to security performances. Also, the field test needed for validation of scenarios will be properly described.

3. Define end-to-end test procedures comprising experimental validation of the whole test chain.

The results will serve as the operational basis for field testing of robustness against security attacks.

1.2 Overview of the document

The outline of the document is as follows:

- Clause 5 provides a review of security metrics, in line with the other deliverables of the project and in particular with CEN/TR 17465 and CEN/TR 17464.

- Clause 6 consolidates the test approach with respect to jamming and spoofing oriented scenarios.

- Clause 7 provides a definition of relevant test scenarios, applicable to security testing, starting from outcomes of CEN/TR 17464.

- Clause 8 provides an in-depth discussion regarding test facilities, focusing on both data recording and replay.

- Clause 9 concludes with a set of real-life tests, for a preliminary end-to-end validation of the procedures.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 16803-1:2016, *Space — Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) — Part 1: Definitions and system engineering procedures for the establishment and assessment of performances*

ETSI TS 103 246-3, *Satellite Earth stations and systems (SES) —GNSS-based location systems — Part 3: Performance requirements*

CEN/TR 17447, *Space — Use of GNSS-based positioning for road Intelligent Transport System (ITS) — Mathematical PVT error model*

CEN/TR 17448, *Space — Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) — Metrics and Performance levels detailed definition*

AVA Documents
Document Sharing Hub

Full document details: PD CEN/TR 17475:2020

CEN/TR 17464, *Space — Use of GNSS-based positioning for road Intelligent Transport System (ITS) — Security attacks modelling and definition of performance features and metrics related to security*

CEN/TR 17465, *Space — Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) — Field tests definition for basic performances*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 16803-1:2016, ETSI TS 103 246-3 and ISO/IEC 27001:2013 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at http://www.iso.org/obp
- IEC Electropedia: available at http://www.electropedia.org/

3.1
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

3.2
authentification
provision of assurance that the location-related data associated with a location target has been derived from real signals associated with the location target

3.3
availability
property of being accessible and usable upon demand by an authorized entity

3.4
continuity
likelihood that the navigation signal-in-space supports accuracy and integrity requirements for duration of intended operation

Note 1 to entry: Continuity aids a user to start an operation during a given exposure period without an interruption of this operation and assuming that the service was available at beginning of the operation. Related to the Continuity concept, a Loss of Continuity occurs when the user is forced to abort an operation during a specified time interval after it has begun (the system predicts service was available at start of operation).

3.5
continuity risk
probability of detected but unscheduled navigation interruption after initiation of an operation

3.6
data
collection of values assigned to base measures, derived measures and/or indicators

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

3.7
electromagnetic interference
any source of RF transmission that is within the frequency band used by a communication link, and that degrades the performance of this link

Note 1 to entry: Jamming is a particular case of electromagnetic interference.

3.8
integrity
general performance feature referring to the trust a user can have in the delivered value of a given Position or Velocity component

Note 1 to entry: In this document, this feature is expressed by 2 (two) quantities: the Protection level and the associated Integrity risk.

3.9
integrity risk
for Positioning terminals providing a Protection level as integrity indicator, refers to the probability that the actual error on a given Position or Velocity component exceeds the associated Protection level provided with this quantity

3.10
jamming
deliberate transmission of interference to disrupt processing of wanted signals (which in this case are GNSS or telecommunications signals)

3.11
level of risk
magnitude of a risk expressed in terms of the combination of consequences and their likelihood

3.12
likelihood
chance of something happening

3.13
localisation
process of determining the position or location of a location target

3.14
performance
measurable result, performance can relate either to quantitative or qualitative findings

3.15
performance class
for a given performance metric, designates a domain delimited by 2 (two) boundaries

3.16
performance feature
a given characteristic used to qualify and quantify the service provided by a system, for example horizontal accuracy for a Positioning system

AVA Documents
Document Sharing Hub

Full document details: PD CEN/TR 17475:2020

3.17
performance metric
precise definition of the means of measuring a given performance feature of a given output of a system

Note 1 to entry: An example of accuracy metric can be the median value of an error sample acquired during a given test following a given protocol.

3.18
protection level
estimation of an upper bound for the error made on a Position or Velocity component (e.g. the plane position) associated with a given probability called Integrity risk

Note 1 to entry: Like the actual error, this feature can be characterized by its distribution function. The protection level PL is upper bound to the position error such that: $P(\varepsilon > PL) < I_{risk}$, where I_{risk} is the integrity risk and ε is the actual position error.

3.19
Pseudo-Random Noise Code (PRN)
unique binary code (or sequence) transmitted by a GNSS satellite to allow a receiver to determine the travel time of the radio signal from satellite to receiver

3.20
reference GNSS receiver
in this document, refers to a widely used and off-the-shelf high sensitivity GNSS receiver offering a good availability and a high sensitivity to the multipath and NLOS phenomena) whose production can be guaranteed for a long period

3.21
reference trajectory
series of time-stamped positions (and possibly speeds) of a reference point on a mobile object (test vehicle), produced by a Reference trajectory measurement system

3.22
Reference Trajectory Measurement System (RTMeS)
term used in this document for a measurement means capable of accuracy performances better than at least one order of magnitude than those of the Positioning terminal being tested

3.23
requirement
need or expectation that is stated, generally implied or obligatory

3.24
robustness
the degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions

3.25
security
function of a location system that aims at ensuring that the location-related data is safeguarded against unapproved disclosure or usage inside or outside the location system, and that it is also provided in a secure and reliable manner that ensures it is neither lost nor corrupted

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

3.26
spoof/spoofing
transmission of signals intended to deceive location processing into reporting false location target data

3.27
threat
potential cause of an unwanted incident, which may result in harm to a system or organisation

3.28
time-to-alert
time from when an unsafe integrity condition occurs to when an alerting message reaches the user

3.29
trajectory
series of time-stamped positions (and possibly speeds) of a mobile object

3.30
vulnerability
weakness of an asset or control that can be exploited by one or more threats

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

4 List of acronyms

ADAS	Advanced Driver Assistance Systems
ADC	Analog to Digital Converter
AGC	Automatic Gain Control
CDF	Cumulative Distribution Function
CEN	Comité Européen de Normalization (European Committee for Standardization)
CENELEC	Comité Européen de Normalization Électrotechnique (European Committee for Electrotechnical Standardization)
COTS	Commercial On The Shelves
DOS	Denial Of Service
DUT	Device Under Test
ECEF	Earth Centred Earth Fixed
ETSI	European Telecommunications Standards Institute
GBPT	GNSS-Based Positioning Terminal
GDOP	Geometrical Diluition Of Precision
GNSS	Global Navigation Satellite Systems
HPL	Horizontal Protection Level
IID	Independent identically distributed
IMU	Inertial Measurement Unit
ITS	Intelligent Transport Systems
KOM	Kick-Off Meeting
OCXO	Oven-controlled crystal oscillator
PPK	Post Processed Kinematic
PPS	Pulse Per Second
PVT	Position Velocity and Time
RAIM	Receiver Autonomous Integrity Monitoring
RFCS	Radio Frequency Constellation Simulator
RMS	Root Mean Square
RTK	Real Time Kinematic
SBAS	Satellite Based Augmentation System
SDR	Software Defined Radio
SIS	Signal In Space
TCXO	Temperature-controlled crystal oscillator
TTFF	Time To First Fix
VPL	Vertical Protection Level
VST	Vector Signal Transceiver

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

5 GNSS Threats overview

5.1 General

In this clause, a description of the most relevant security scenarios is provided, based on what described in CEN/TR 17464. The analysis is focused on the intentional RF threats scenarios since they represent a worst case with respect to unintentional interference. Furthermore, intentional attacks encompass a wide variety of cases that allow a more flexible, representative and controllable analysis.

The possible attacks on GNSS can be divided in 2 (two) macro areas:

- Denial of service (DoS):
  - jamming;
- Deception of Service:
  - spoofing;
  - meaconing.

The jamming threats are in general based on the transmission of an interfering signal on the GNSS bands. The disturbance impairs the receiver performance, preventing it to perform PVT operation. The jamming is not only intentional, but it can be generated by RF equipment employed in other applications as well. The equipment may emit signals that interfere with the GNSS band, causing unintentional jamming. DVB harmonics CEN/TR 17464 are examples of this kind of interference.

Deception of service attacks are instead focused on making a receiver computing a false PVT solution (position, velocity and time). This effect is achieved through the transmission of false signal generated from fake GNSS constellation or through the re-transmission of the received Signal in Space (SIS).

5.2 Denial of service: jamming

Jamming signals are disturbing signals purposely developed to prevent the correct operation of a receiver. In this context a number of different jammers exist. The current subclause provides a brief overview of the jamming taxonomy.

Different kinds of jammers are designed to attack and disrupt different stage of a GNSS receiver. In particular, jamming impacts the receiver front-end, that is the interface between the physical RF signal and the digital baseband domain.

In literature many works analysed and compared commercial available jammers. Even if these jammers are low-cost jammers, it can be assumed that the basic principles also apply in the design of more complex and expensive ones.Recalling the results reported in *Software-defined radio based roadside jammer detector: Architecture and results, Position, Location and Navigation Symposium* (ref. Bibliography [1]), commercial jammers can be categorized in:

1. Continuous wave (CW) signal (Class I).
2. Chirp signal with 1 (one) saw-tooth function (Class II).
3. Chirp signal with multi saw-tooth functions (Class III).
4. Chirp jammer with frequency bursts (Class IV).

AVA Documents Document Sharing Hub

Full document details: PD CEN/TR 17475:2020

The chirp signal is essentially a pure tone whose carrier frequency follows a saw-tooth like behaviour, sweeping from a minimum frequency to a maximum frequency in a linear fashion in a well-defined period.

The bandwidth of chirp jammer signals varies in a range from 10 MHz to 30 MHz. If the chirp bandwidth exceeds the bandwidth of the front-end it appears within the receiver as a pulsed chirp signal with a duty cycle of $DT = \frac{B_{front\ end}}{B_{chirp}}$.

Chirp jammers, with pulsed capability, could represent all the major categories. Frequency Burst (wideband component) can be modelled as wideband noise.

Chirp signals can be modelled (as normalized complex baseband equivalent) as:

$$y_i(t) = e^{j2\pi \int_{-\infty}^{t} f(\tau) d\tau} \tag{1}$$

Where $f(t)$ accounts for frequency modulation. The equation for modulating signal is (basic of analog FM)

$$f(t) = f_c + \Delta_f \cdot K(t, f_m) \tag{2}$$

The main parameters are hereinafter described:

- Central carrier set the central operating frequency of the jammer f_c [Hz];
- Sweep Band, i.e. span of the carrier during time, is set to Δ_f [Hz];
- Sweep Rate, i.e. the frequency of repetition of the basic waveform (in frequency) f_m [Hz/s];
- shape of the modulating signal can be ($K(\cdot)$):
  - SAWTOOTH (LINEAR CHIRP),
  - SQUARE (DUAL HOP),
  - SIN (CLASSICAL ANALOG FM).

Figure 1 reports a pictorial representation of a linear chirp, highlighting both time and frequency features. The picture reports a time plot, where the change in frequency is clearly visible, the spectrum plot, where the spectrum occupation is visible, and the spectrogram view, where time-frequency dynamics are reported.

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

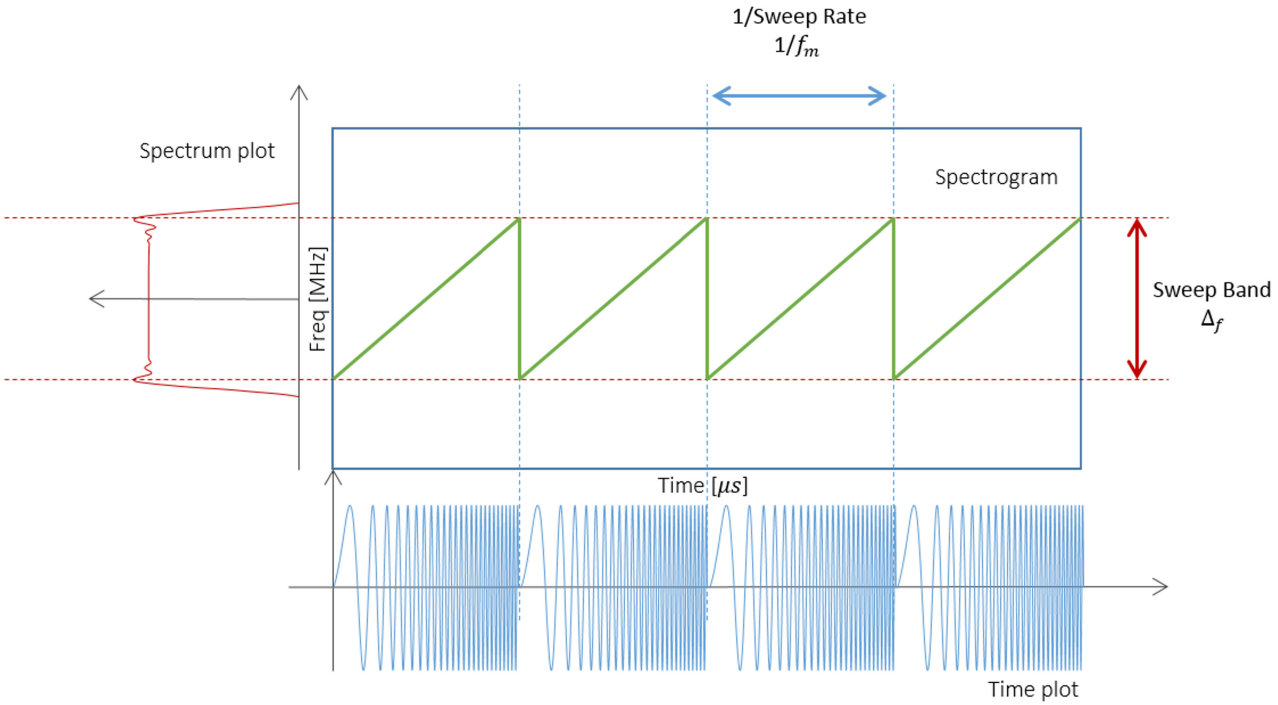


Figure 1 — Chirp signal (not to scale)

Several types of jamming signals that can be generated following an SDR approach are described in 9.1.2.

5.3 Deception of service: spoofing and meaconing

Instead, about deception of service, an additional division on top of spoofing and meaconing can be applied. Figure 2 shows the taxonomy about deception of service attacks.

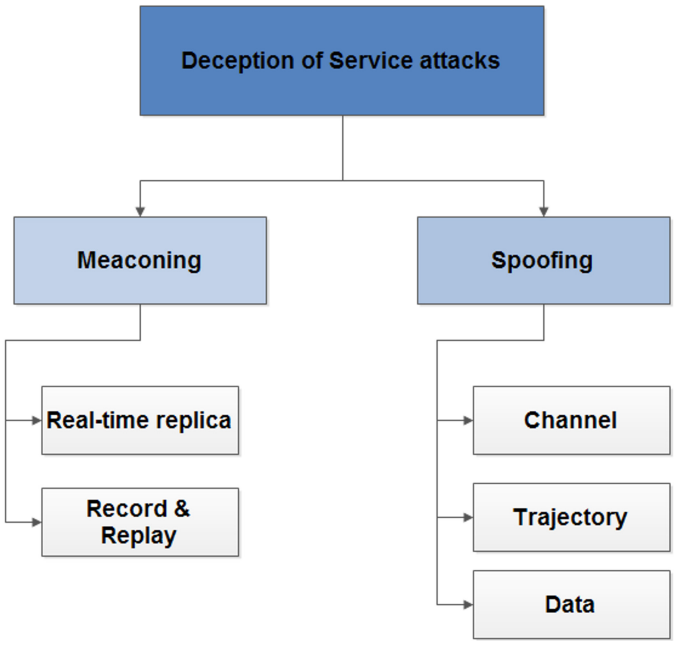


Figure 2 — Deception of Service taxonomy

Documents
Document Sharing Hub

Full document details: PD CEN/TR 17475:2020

Several types of attacks to GNSS can be grouped under the spoofing label, aimed at impacting different aspects of the GNSS system such as data or signals:

- **Channel spoofing**: this type of attack changes the dynamics of a GNSS channel introducing a Doppler or Pseudo-range offset with respect to the authentic signal; this type of attack hardly impairs the PVT computation because the use of RAIM (Receiver Autonomous Integrity Monitoring) can easily exclude the channel under attack. However, a continuous sweeping of the relative spoofing code phase could be introduced, leading to a denial of service on a specific channel limiting the probability of detection compared to a standard jamming attack. Additionally, a channel spoofing attack on many GNSS channels can force the receiver to bad PVT solutions, since it cannot recognize authentic and non-authentic signal.

- **Trajectory spoofing**: this type of attack is a generalization of the channel spoofing, but aimed to the falsification of the whole constellation. Specifically, the attacker generates the overall constellation corresponding to the fake position and transmits to the receiver the spoofing signal. In summary, this attack coordinates coherently several channels, so that they lead to compute a false PVT solution.

- **Data level spoofing**: the attacker does not apply modifications to the authentic signal dynamics, but it changes the navigation data transmitted, for impairing the PVT solution. This kind of attack can be very effective with SBAS signals.

All spoofing attacks are not straightforward to carry out, because the attacker shall be able to estimate the user receiver position for compensating the attacker-attacked dynamics. Consequently, the attacker shall generate the signals with the correct dynamics. Moreover, the attacks, depending on the capability of the attacker of aligning with the signal phase and delay at the receiver, can be synchronous or asynchronous. The synchronous attacks are very difficult to perform in a realistic scenario, because the attacker shall able to estimate the correct carrier phase and delay for each GNSS channel at the receiver side and generate the signal in accordance. Figure 3 shows an example of a spoofing ACF getting the lock from the authentic signal, in both synchronous and asynchronous case. Specifically, the spoofer ACF shall slowly transit over the authentic one and get the receiver lock, transmitting with slightly higher power.

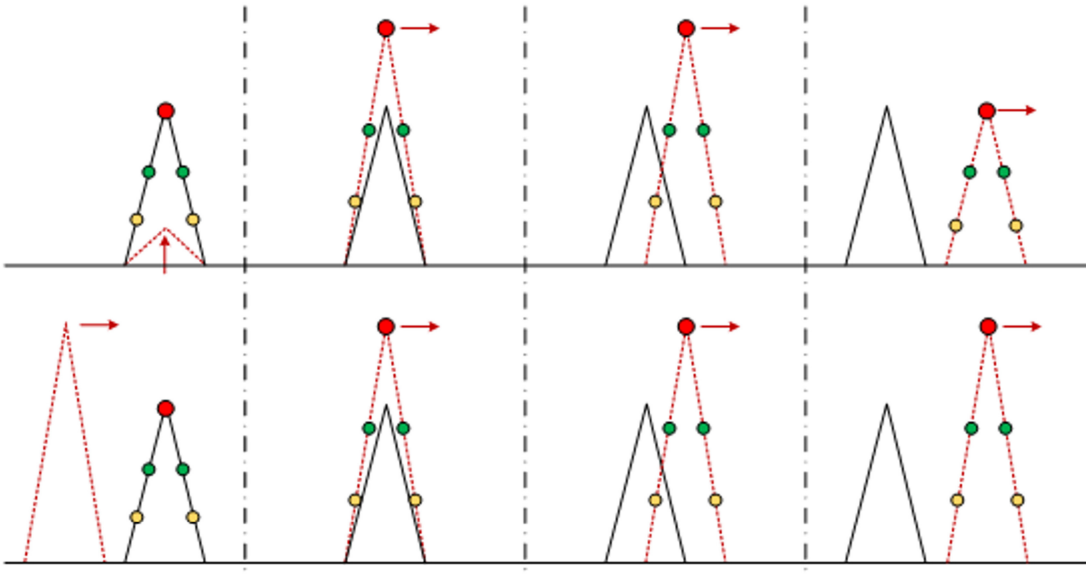


Figure 3 — Synchronous (top) and asynchronous (bottom) spoofing attacks

In the described scenario a good alignment between the authentic signal and spoofing is essential for the success of the attack. Mainly three phases can be identified during a spoofing attack:

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

- **Trusted Phase**: no spoofing signal is transmitted over the authentic; this phase is purely theoretical, because it is not verifiable in real environment, only in controlled scenarios such as constellation simulators;

- **Attack phase**: the spoofing ACF overlaps to the reference one, its amplitude should be comparable with the authentic in order to avoid unexpected power changes;

- **Spoofed phase**: the last phase of the attacks that can be considered starting from the moment when the spoofing ACF is outside the correlation window of the authentic, with delay higher than one chip. The receiver can then assume three states:

    - Spoofed: the attack is successful and the receiver is tracking the spoofing signal;

    - Normal operation: the attack was not effective and the receiver keeps tracking the authentic signal;

    - Loss of Lock: the attack was not effective, but it disturbed the tracking operation, therefore the receiver losses the lock on the authentic signal; the spoofer acts as a jammer.

Figure 4 shows a general scheme of the three phases of the spoofing attack.

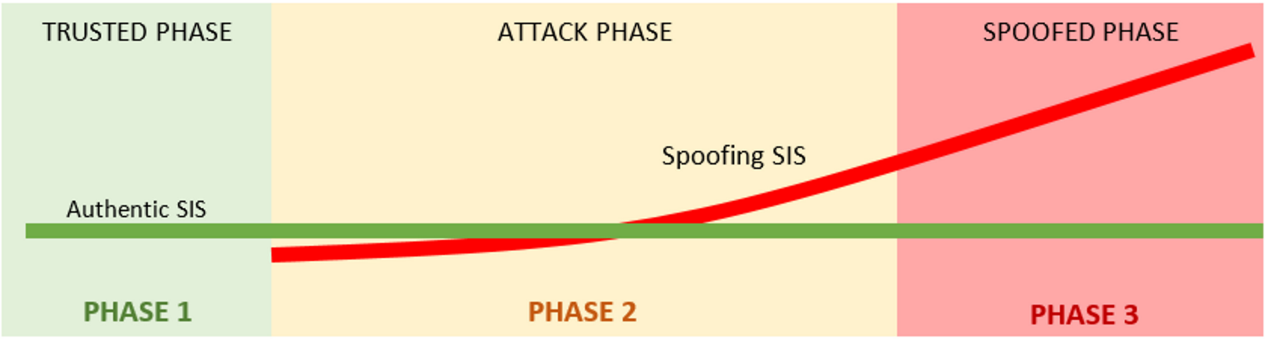


Figure 4 — Phase of spoofing attack

A much more straightforward approach is combining jamming and spoofing. Specifically, the attacker transmits a jamming signal with significant power to force the receiver to a loss of lock. Afterwards, it generates the false signal with slightly higher power with respect to the GNSS authentic signal. This attacking approach is very straightforward and works well for basic receivers. However, it is really easy to detect, because the spoofing procedure starts right after a receiver loss of lock. Typically, the focus of an attacker is spoofing the GPS system, because it usually has the highest priority in the GNSS receiving system. The complexity of acting also on the Galileo system is within the spoofer implementation, specifically more lines of code that simulate Galileo system as well. Concerning GLONASS instead, many commercial simulators that generate the Russian system are available, therefore it could be spoofed as well, even though it requests additional bandwidth, so higher quality radio peripherals. However, since it is transmitted over a different centre frequency the attacker's approach could be jamming it and spoofing GPS and Galileo systems, in order to not raise inconsistencies within the spoofed receiver.

Meaconing (Masking Beacon) identifies the repetition of a received GNSS signal in real-time or in post-processing. The attacker receives the GNSS signal and retransmits all the batch to the receiver. If the receiver locks on the delay signal, it experiences degradation on the time solution, because all the GNSS signals arrives in delay with respect to the reference. Moreover, since the attacker's position is different with respect to the receiver, also the position procedure is impaired. 2(two) types of meaconing attacks can be identified:

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

- Real-time Meaconing: it foresees the retransmission of the received GNSS signal in real-time, with a slight delay with respect the real signal. The delay can be roughly estimated in a range below 1 ms;

- Record and Replay Meaconing: it foresees the record of a GNSS batch and the retransmission after some time: in this case the delay is in principle arbitrary, from seconds to days).

This type of attack, especially the real-time meaconing, is potentially able to overcome the Spreading Code Encryption (SCE) protection, because the attacker repeats all the SIS, including the encrypted signals. The attacker could start to replay the signal with low delay, in order to make the receiver lock on the fake signal, and afterwards trying to delay it more and more, in order to have a considerable impact on the clock bias and therefore on the time estimation.

6 Security metrics

6.1 General approach

6.1.1 Introduction

Security metrics are necessary to assess the robustness of the receiver against jamming and spoofing threats. The behaviour of the DUT under intentional and non-intentional interference shall be evaluated in a quantitative manner, to state whether the receiver fulfils the standards for jamming/spoofing resilience. The general approach is to analyse the degradation of the metrics taken into account in the basic performance case, well described in CEN/TR 17448 and CEN/TR 17465.

Jamming attacks are brute force attacks intended for Denial of Service (DoS), being it a loss of accuracy below a certain threshold or a complete loss of lock and, consequently, loss of PVT estimation. These kind of attacks therefore can impair accuracy, and if strong enough, they can disrupt availability and continuity. A typical jammer performs little or none concealment countermeasure at all to avoid detection by the receiver. The transmission of high power signals can likely cause the disruption of service and it is necessary to assess how the receiver reacts to these threats.

Instead, spoofing attacks target mainly the accuracy and integrity of the service. In fact, the deception of service threat pursues the non-detection objective, therefore the continuity and availability of the GNSS service is in principle not impaired if the attack is carried out properly.

In summary, jamming and spoofing attacks impact the accuracy, availability, integrity and continuity of the GNSS service. These attacks can also impact Time to First Fix.

The degradation analysis is based on comparison of statistical estimates under attack with respect to the ones estimated in basic scenarios.

The most meaningful information requested for the degradation analysis are:

- reference trajectory for the whole recording time;

- reference velocity for the whole recording time;

- performance assessment in the basic case.

As above introduced, the mathematical assessment for comparison of different statistical estimates are reported in CEN/TR 17447. One of the most used statistical estimator is the Empirical Cumulative Density Function (ECDF). 6.1.2 and 6.1.3 provide some insights on the correct calculation of the ECDF, especially when considerable losses of data are experienced, as during jamming/spoofing attacks.

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

6.1.2 Notes on empirical CDF

One of the most widely used statistical estimator used to assess performance, as per EN 16803-1:2016, is the empirical Cumulative Density Function (ECDF).

In this paragraph, some important theoretical derivations are reported, together with an assessment on the minimum number of samples needed to estimate the CDF with a given error bound. This assessment could help choosing the minimum number of samples to be collected in a given scenario, and hence provide guidelines on the minimum length of each test scenario.

Suppose to have $X_1,\ldots, X_N \sim F$ independent identically distributed (IID) samples, where $F(x)=P[X_i \le x]$ is the distribution function. The Empirical Cumulative Density Function (ECDF) is calculated as follows:

$$\hat{F}(x)=\frac{1}{N}\cdot\sum_{i=1}^{N} I(X_i \le x) \quad . \tag{3}$$

Where $I(\cdot)$ is the indicator function, i.e. $I(X_i \le x)=1$ with probability $P(X_i \le x)=F(x)$ and $I(X_i \le x)=0$ with probability $P(X_i > x)=1-F(x)$. This implies that $I(X_i \le x)$ is a Bernoulli random variable with "success" probability $F(x)$. Provided that X_i are independent, $Y_N=\sum_{i=1}^{N} I(X_i \le x) \sim Bin(x, F(x))$ and hence the ECDF is distributed as:

$$\hat{F}(x) \sim \frac{1}{N} Bin(N, F(x)) \tag{4}$$

$$E[\hat{F}(x)]=F(x)$$

$$Var[\hat{F}(x)]=F(x)\cdot(1-F(x)) \tag{5}$$

Ung the normal approximation of the Binomial, i.e. $Bin(N,p) \to \mathcal{N}(Np, Np(1-p))$, that is valid in case N is great (with CDF estimation, $N>100$ tipically):

$$\hat{F}(x) \sim \mathcal{N}(F(x), F(x)\cdot(1-F(x))) \tag{6}$$

The plot of Figure 5 reports a simulation, with empirical percentiles and approximated bounds (cyan and green) calculated using normal approximation. Normal approximation could fail near 0 and 1, hence a saturation should be considered, since the following limits and bounds shall always hold:

$$0 \le \hat{F}(x) \le 1$$

$$\lim_{x \to +\infty} \hat{F}(x)=1$$

$$\lim_{x \to -\infty} \hat{F}(x)=0 \tag{7}$$

Another important theorem is the Dvoretzky-Kiefer-Wolfowitz inequality, that states, for any $\epsilon > 0$:

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

$$P\left(\sup_x \left|\hat{F}(x) - F(x)\right| > \epsilon\right) \leq 2e^{-2N\epsilon^2} \tag{8}$$

This theorem can be used to build a non-parametric confidence bound for $F(x)$.

In fact, given $L(x) = \max\left\{\hat{F}_N(x) - \epsilon_N, 0\right\}$ and $H(x) = \min\left\{\hat{F}_N(x) + \epsilon_N, 1\right\}$ the lower and higher bound respectively, where $\epsilon_N = \sqrt{\frac{1}{2N}\ln\left(\frac{2}{\alpha}\right)}$, then, for all F and N:

$$P\left(L(x) \leq F(x) \leq H(x) \forall x\right) \geq 1 - \alpha \tag{9}$$

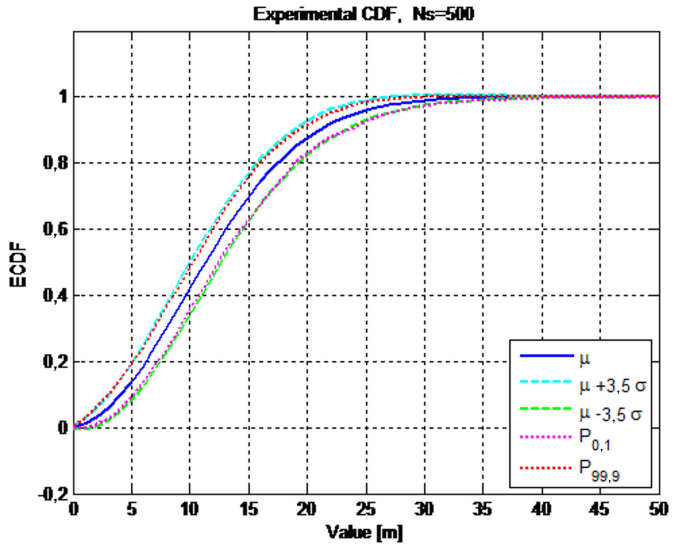


Figure 5 — Empirical CDF statistics

Combining Formula (8) and (9), it is possible to estimate a safe lower bound for CDF estimation, choosing a confidence bound $1 - \alpha$, and maximum allowed error ϵ. In Figure 6 and Table 1, some relevant results are summarized.

$$N_m \geq \left(\frac{1}{2\epsilon^2}\right)\ln\left(\frac{2}{\alpha}\right) \tag{10}$$

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

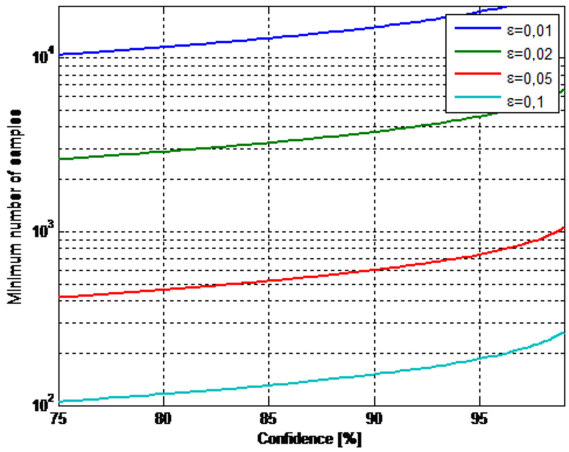


Figure 6 — Minimum number of samples for ECDF

Table 1 — Minimum number of samples, 95 % confidence

Eps	Nmin
0,01	18445
0,02	4612
0,05	738
0,1	185

6.1.3 ECDF with loss of samples

In case of security performance testing, but also in particular cases of basic performance testing in challenging environments or GNSS denied environments, the PVT sample set may experience some losses. This could cause a relevant impact on CDF estimation, as already pointed out in CEN/TR 17448. Assuming that the total number of provided samples is, with N_v valid and N_n not valid (measurements holes). Two (two) approaches can be used for CDF estimation:

- approach 1: discard holes and compute CDF on the rest, using N_v samples;
- approach 2: assign to holes dummy value and use all samples N.

In the following paragraphs a detailed overview of the two approaches is reported, with some simulation data. The consortium is proceeding toward approach 1, even if it has some important drawbacks.

Some simulation results are obtained, drawn using Matlab and considering the absolute value of an Additive White Gaussian Noise 2-D process (Horizontal absolute error). The titles of the figures report the number of samples and availability percentage.

In Figure 7 and Figure 8 the effect of number of available points for estimation on CDF is reported, for approach 1. The CDF estimated is very step-wise and rough, when only 5 % of the samples are available. The approach 1 discard holes and compute CDF on the rest, using $\frac{N_v}{N}$ samples. In this case it is always needed to stem a companion metric regarding availability of samples. It is hence needed to define a minimum availability threshold, according to Formula (10). A brief comparison of pros and cons is here reported:

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

- PROs:
  - CDF always reach the right value 1, resembling a real CDF in any case;
  - no need to decide a dummy value for data holes.
- CONs:
  - when few samples are available in the data set, it can be difficult to estimate properly the CDF, as seen in Figure 7;
  - the CDF is somehow not reflecting at all the effect of loss of samples. It is important to stress that loss of PVT is the worst degradation that can happen, since the measurement is not available at all;
  - it can happen that, with a pulsed interference for example, only few samples are lost, while the other show near-nominal behaviour, see Figure 11;
  - each metric shall be coupled with an availability metric, so the "degradation of performance" is less intuitive, since also the availability shall be considered, not only the CDF of the metric itself.

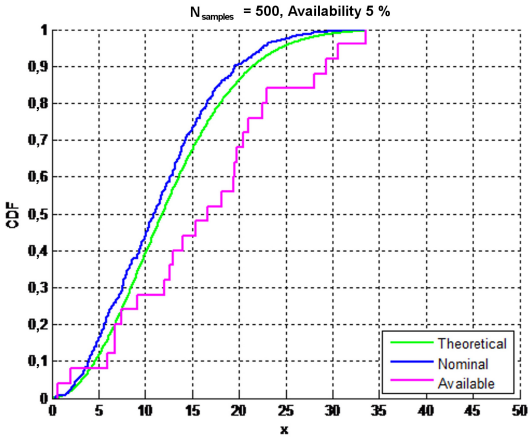


Figure 7 — CDF with available samples, low availability

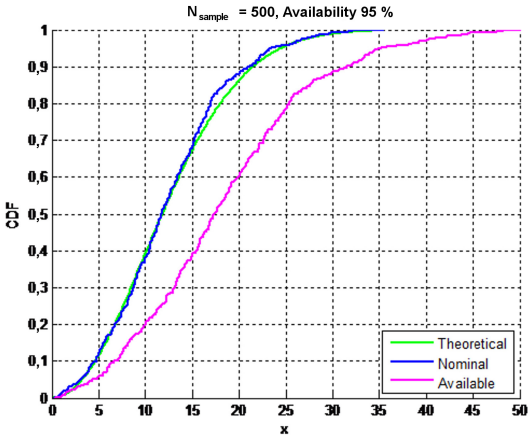


Figure 8 — CDF with available samples, high availability

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

The approach 2 uses all the samples, assigning to “holes” a dummy value (typically a value much higher than the maximum value among the available samples). In this manner it is always possible to compute the CDF with the standard approach, but it is also suggested to define a minimum availability threshold, according to Formula (10).

The choice of the dummy value is important, since the expected CDF shape with dummy value is reported in Formula (11). If the dummy value is properly selected, as in Figure 9, the CDF bends toward the right, reflecting the worsening of performance, and allowing to downgrade the performance class to a lower one. In case of wrong dummy value, as in Figure 10, the performance class is wrongly estimated, being also better than in the non-impaired case. A brief comparison of pros and cons is here reported:

- PROs:
  - no need for a companion availability metric;
  - same CDF estimation approach used in the basic performance estimation case;
  - dummy insertion, if properly chosen, reflects the fact that loss of measurements is equivalent to an extreme worsening of performance;
- CONs:
  - when few samples are available in the data set, the CDF can be extremely distorted around the dummy value, losing any resemblance of the nominal CDF.
  - dummy value choice have a significant impact on the performance estimation. It is not easy to “standardise” a dummy value.

$$\hat{F}_{dummy}(x) = \frac{N_v}{N} \cdot \hat{F}(x) + \frac{N - N_v}{N} \cdot H\left(x \geq x_{dummy}\right) \tag{11}$$

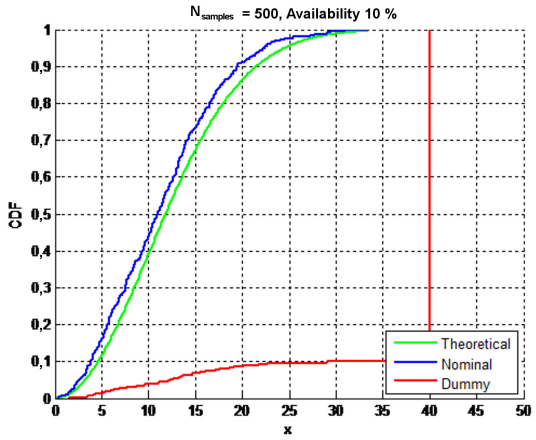


Figure 9 — CDF with proper dummy value

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

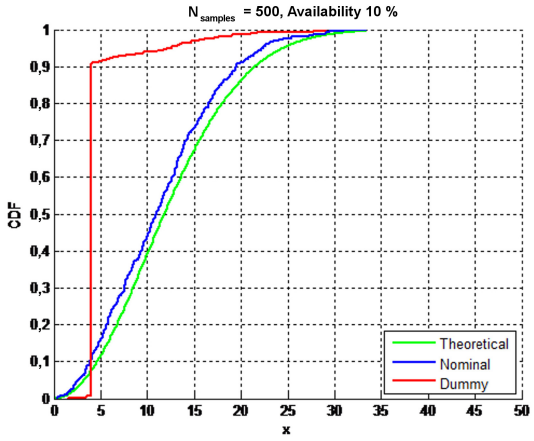


Figure 10 — CDF with underestimated dummy value

6.2 Considered metrics

6.2.1 General

The metrics considered for the security aspects are compliant with the ones defined in CEN/TR 17448 and EN 16803-1:2016. Specifically, the performance degradation is assessed in specific nominal scenarios defined for basic performance testing, where an interference or spoofing phenomenon is superimposed. The approach of considering the degradation of the same metrics defined for the basic performance testing simplifies the performance evaluation process, providing highly comparable results.

6.2.2 Accuracy

Accuracy metric, as defined in CEN/TR 17448, is the baseline metric for assessing security performance, and identifies the receiver capabilities of estimating correctly the position and velocity. The accuracy is evaluated through CDF computation, hence all the rationale described in 6.1 is applicable.

According to strategy 1 reported in 6.1.3 and CEN/TR 17465, let us assume that the metric is computed processing the data points where the GNSS PVT is available at the receiver. This approach avoids the introduction of dummy data in the performance computation, which could bias the degradation calculus.

A jamming threat can heavily impact the CDF:

- **Medium Jamming**: jamming can be seen as an error source, spreading the CDF toward higher values.
- **Intense Jamming**: in case of intense jamming, the PVT is lost at all, and if the number of remaining points is too low, no CDF can be computed at all.

A special case of jamming, that could be particularly tricky regarding performance evaluation, is related with pulsed interference. Considering the following scenario:

- open sky environment that allows good PVT performance;
- very intense jamming, with a pulsed behaviour of low period (consider for instance 8 s of jamming every 10 s):
  - when the jamming is on, PVT is lost,
  - when jamming is off, the receiver is able to recover the lock,
  - assuming a 1 Hz PVT generation, it can be assumed that 2-3 samples are lost every 10;

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

- the simulation continues for 5 minutes.

In this case, the service availability is less than 20 %, which represents bad test results indeed. However, the test would return excellent results in terms of accuracy, which is technically true, but it would return an outcome with good performance, even though the test results are not sufficient.

Figure 11 shows an example (Matlab simulation, AWGN noise, as described in 6.1.3) about the degradation over the accuracy CDF in case of high power pulsed jamming. As previously specified, the disturbance makes the receiver loose the lock on the GNSS signal, therefore the accuracy metric is computed only when the jammer is turned off. The approach leads to an accuracy comparable with the nominal case. Figure 12 shows instead the case of a low power jammer focused on degrading the operations and avoid detection. In this case, the error CDF presents a slight performance degradation.

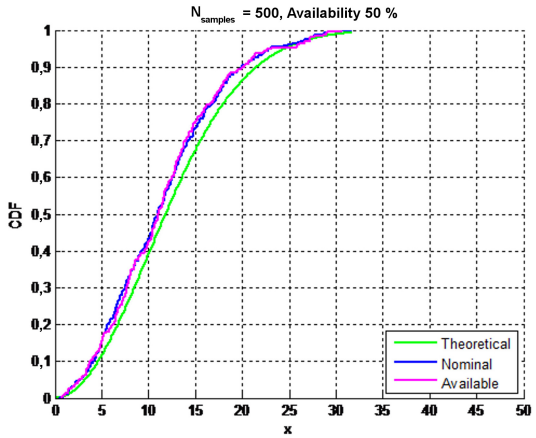


Figure 11 — CDF with available samples, pulsed high power interference

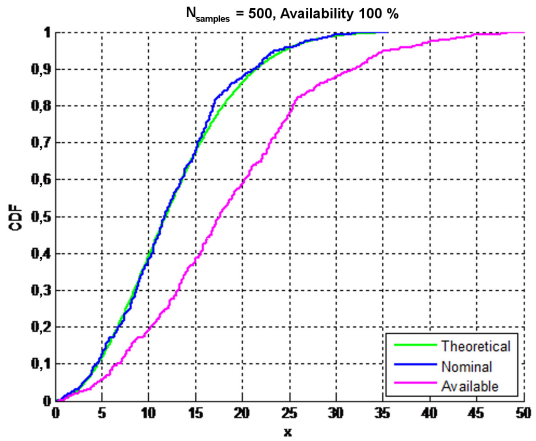


Figure 12 — CDF with available samples, low power interference

In case of spoofing attack, 2 (two) cases can happen (this is a simplified categorization):

- **Spoofing attack failed**: in this case only few samples are impacted, showing accuracy worsening or loss of lock, and the CDF may be almost identical to the nominal case without threat.

- **Spoofing attack successful**: the accuracy metric is highly impacted. Apart from some PVT losses due to a jamming phase or during alignment with the authentic signal, once that the spoofer has deceived the receiver, the calculated PVT may wander arbitrarily according to the spoofing signal. In fact, the

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

receiver computes a false position with respect to the nominal case, therefore the accuracy degradation can be extremely high. Especially in good channel conditions, where the nominal case accuracy is good.

Figure 13 shows an example of accuracy degradation in case of successful trajectory spoofing attack. The performance degradation is dramatic since, if the receiver gets the lock on the spoofing signal, the DUT computes a totally incorrect position.

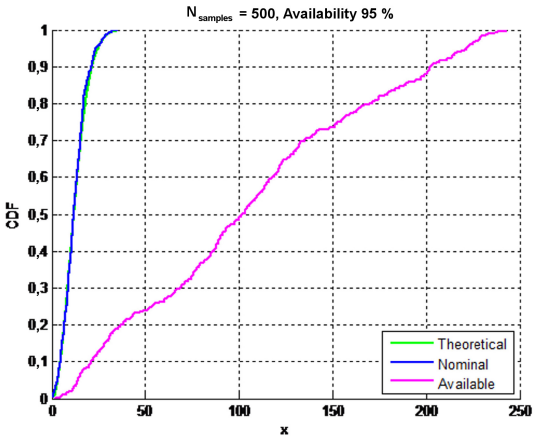


Figure 13 — CDF with available samples, spoofing attack

As a general rule, during security assessment:

- the accuracy shall be computed only during period of attack. In case of fast pulsed- jamming (period of the pulse up to 10s), the on-off pattern is to be intended as an intrinsic feature of the jamming signal, hence the CDF shall consider the entire duration of the test. In case only a portion of the test is affected by the threat, that portion only shall be considered;

- in any case, the CDF shall be computed only if a minimum number of points is available (namely 100 points).

6.2.3 Integrity

6.2.3.1 Integrity from aviation domain

Integrity measures the reliability of the information returned by the navigation system. This metric has been defined in the aviation domain and is currently highly exploited to ensure the airworthiness safety. The degradation of these metrics depends on the reaction to jamming and spoofing of the protection level computation unit. Figure 14 shows the Stanford diagram that illustrates all the integrity failures concepts displayed on Navipedia [1)](ref. Bibliography [5]). The same concept sketched here for position (horizontal or vertical) can be applied to velocity.

1) Integrity on http://www.navipedia.net.

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

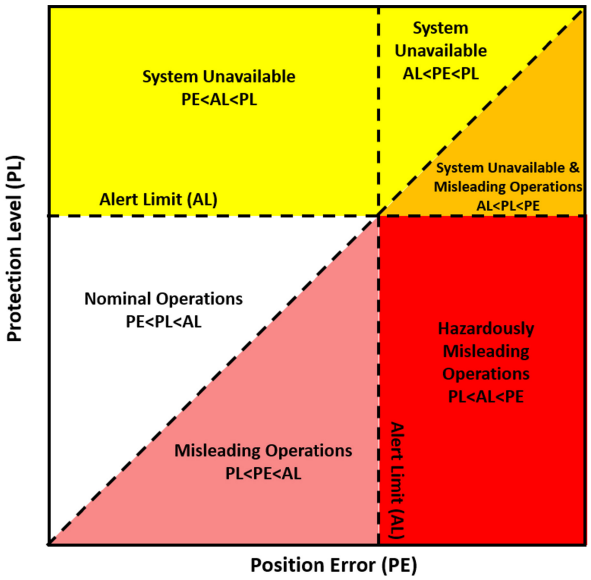


Figure 14 — Stanford diagram

The parameters related to integrity are the following:

- **Alert limit (AL)**: it is the maximum error that shall not be exceeded without an alert;
- **Position Error (PE)**: the position error of the receiver;
- **Protection Level (PL)**: it is a statistical bound over the position error that characterizes the risk that the PE is higher than the AL, since the PE is not available at the receiver. If the PL surpasses the AL an alert is triggered by the receiver.
- **Integrity Risk (IR)**: Probability that, at any moment, the position error exceeds the Protection Level, i.e. $P(PE > PL) < IR$. Graphically, this is the percentage of points laying below the line PL = PE.

The simplest algorithm for protection level calculation accounts for the following 3 (three) factors:

$$PL = k_{IR} \cdot \sigma_{UERE} \cdot GDOP \tag{12}$$

Where k_{IR} is a factor accounting for integrity risk requirements, σ_{UERE} is a term accounting for the overall user equivalent ranging errors, i.e. the noise on receiver measurements, and GDOP is the geometric dilution of precision, a factor accounting for geometry of the satellites.

The above described formula is valid in "ideal" conditions, where only random Gaussian noise is present. Other more sophisticated algorithms exist (ref. Bibliography [5]) that consider also other impairments due to the environment. In many cases the PL calculation is highly refined by using external aiding provided by Satellite Based Augmentation System (SBAS) signals. The integrity events, as in Figure 14, can be divided in 5 (five) categories:

- **Nominal Operations (white)**: the position error is below the estimated protection, that is below the alarm limit;
- **System Unavailable (yellow)**: the protection level is above the alarm limit and hence an integrity alarm is properly triggered;

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

- **System Unavailable and Misleading Information (orange)**: the protection error is above the protection level, which is above the alarm limit. In this case the system is flagged as unavailable, but the protection level is not over-bounding the position error;
- **Misleading Information (MI: pink)**: the position error surpasses the protection level but not the alert limit;
- **Hazardously Misleading Information (HMI: red)**: the position error exceeds the alert limit, but the system is declared available. This is the most dangerous case, since the system is not able to detect and alert the user about a risk condition.

6.2.3.2 Integrity in ITS

Intelligent Transport System sector have defined a simplified version of Integrity, and in particular the concept of Alarm Limit is not used. For the sake of simplicity, the Stanford plot above described can still be used to represent graphically the relation among Protection Level and Position Error (and the same is for velocity plots), since many software analysis tools are capable of deriving such plots by default. In the analysis presented in Clause 10, the alarm limit is present and is set to a conventional value. Nonetheless, the classical Stanford plot can still be used, by considering only the two regions above and below the line $PL = PE$ in the plot, as visible in Figure 15.

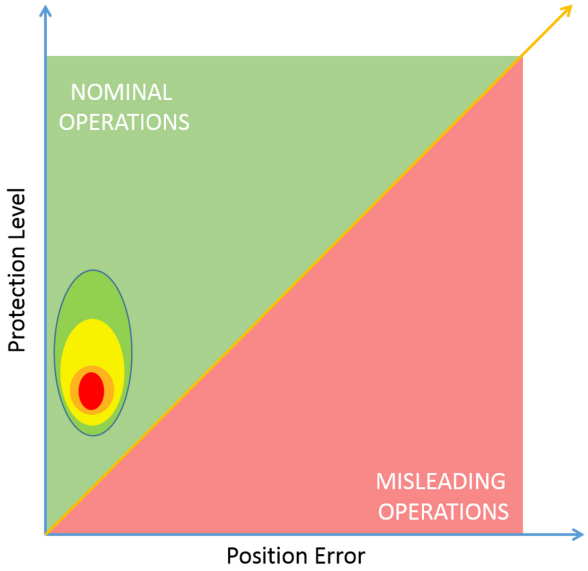


Figure 15 — Integrity plot in ITS

The interference threats can affect the Stanford diagram in many different ways. Specifically, a jamming attack that degrades, but does not deny completely, the GNSS service could have 2 (two) main impacts (see Figure 16):

- strongly increasing the PL due to the poor receiving conditions while the PE increases as well (see Formula (12)), as in Figure 16;
- if the PL is not efficiently computed there could be risk is ending in HMI zone, which would mean very poor receiver integrity performance in presence of jamming.

Conversely, in case of successful spoofing attack, the effects can be the following (see Figure 17):

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

- PL remains almost constant, since the receiver does not detect an increase in the noise contribution and the satellite geometry remain good, but PE strongly increase due to the PVT deception. The system is in the Misleading Operation zone.

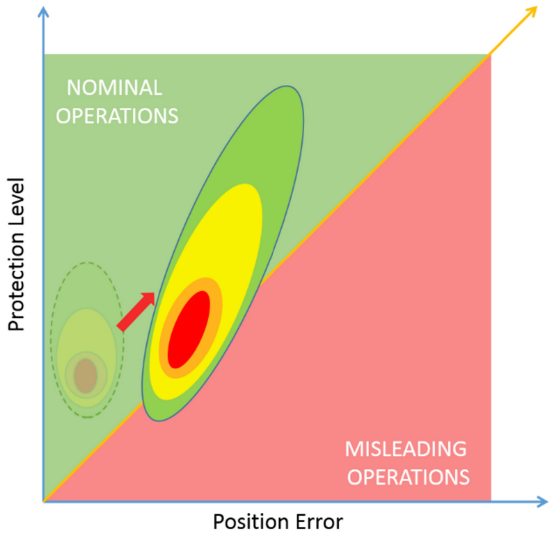


Figure 16 — Stanford diagram in jamming case

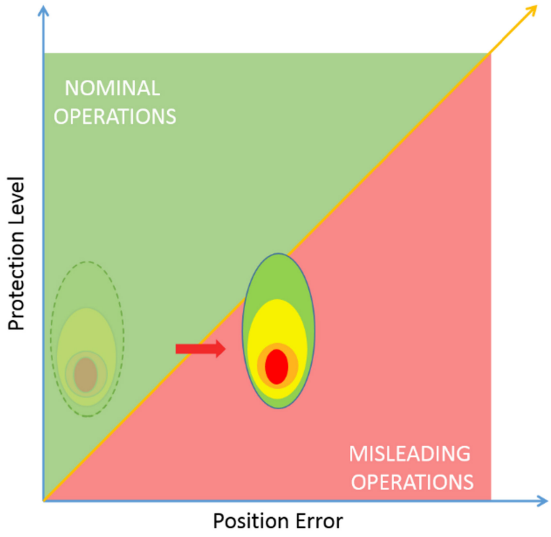


Figure 17 — Stanford diagram in spoofing case

This integrity behaviour states that the receiver is vulnerable against spoofing threats. However, receivers that implement anti-spoofing techniques may avoid to lock on the false signal maintaining a low PE, keeping the system on the Nominal Operations zone.

In CEN/TR 17448 and CEN/TR 17465, it is clearly stated that a method to assess integrity performances is to derive CDF for protection levels and estimate integrity risk.

As visible in Figure 16 and Figure 17, it is expected that:

- jamming will lead to a spread of the CDF. Some specific cases, as strong pulsed jammer, may elude this effect. Also the Integrity risk could be affected (but not mandatory, depends on the algorithm used for PL computation);

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

- spoofing will lead to a slight CDF modification, but probably will trigger Misleading Operation zone, i.e. the PL will remain the same, but the integrity risk will increase.

Any non-available sample could be:

- discarded, leaving less points for plot;
- accounted in the "nominal operations", assigning a dummy value with coordinate $\left(0, \max\left(PL\right)\right)$. A lost sample is by definition not violating integrity, since the system knows that for that point the system is non-operational (would be accounted as "system unavailable" in the classical Stanford diagram).

6.2.4 Availability and continuity

The availability is a simple dimensionless quantity, i.e. (according to 2 (two) possible definitions):

1. The ratio of the number of samples with valid PVT over the total number of samples.
2. In CEN/TR 17448 a slightly more complex definition is provided *"Position Availability (T) is the percentage of operating time intervals of length T during which the positioning terminal provides at least one position output"*. In this case also the observation period is considered, but the 2 (two) definition are equivalent if the time interval is taken equal to the length of the PVT period, i.e. 1 (one) second in the worst case.

The availability represents the percentage of time when the GNSS service is usable.

- In case of DOS Jamming this metric is highly degraded, since the disturbance is addressed to make the receiver losing the lock.
- Instead, in case of spoofing attack, the availability is degraded only when a jamming signal is transmitted for inducing a loss of lock in the receiver. Otherwise, when the deceiving signal "steals" the receiver tracking loop from the authentic one, the availability impact is little or nothing at all.

As stated in 6.1.2, a proper threshold on availability shall be decided, since the loss of data are the worst phenomenon that can happen to a GBPT, together with falsified position. If availability is too low, any CDF estimation is meaningless.

The tolerable availability loss depends on the specific application, but it is sometimes even more important to consider the length of the "holes "in signal availability. In this reasoning continuity come into play, since it is the companion metric of availability.

In ITS applications, where speed can reach 50 m/s, the tolerable loss of sample is very low, namely 10 samples. So at least one sample every 10 shall be present. As a preliminary assessment it is suggested to use as a very lower bound of 10 % on availability, according to definition 1).

In CEN/TR 17448 and CEN/TR 17465, continuity (T) is defined as *"the percentage of time intervals of length T during which the positioning terminal provides valid outputs at the expected rate and without interruptions"*.

A possible procedure for continuity estimation, according to this definition is the following:

- Start from the sample validity, i.e. for each valid sample assign a value 1 and assign instead a value 0 to each invalid (or not present) PVT sample.
- Fix a time interval of length T (i.e. window of T contiguous samples). An example is provided in Figure 18 (a), where the window is 3 (three) samples-wide.

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

- Perform a sliding window on the data, summing at each instant the number of valid samples in the window. The outcome spans from 0 to T. In Figure 18 (b) the signal is reported, together with 2 (two) thresholds, one for availability set to 1, and one for continuity set to T. In practice the continuity signal is set to 1 if at least one sample in the window is equal to 1, while the continuity signal is set to 1 only if all samples in the window are equal to 1.

- Apply the thresholds, obtaining run-length estimates for availability and continuity (respectively Figure 18 (c) and Figure 18 (d)).

- Evaluate availability and continuity as the ratio of the number of 1 obtained over the total number of sliding-window samples.

Some interesting simulations showing the impact of size T are reported in Annex E.

Documents
Document Sharing Hub

Full document details: PD CEN/TR 17475:2020

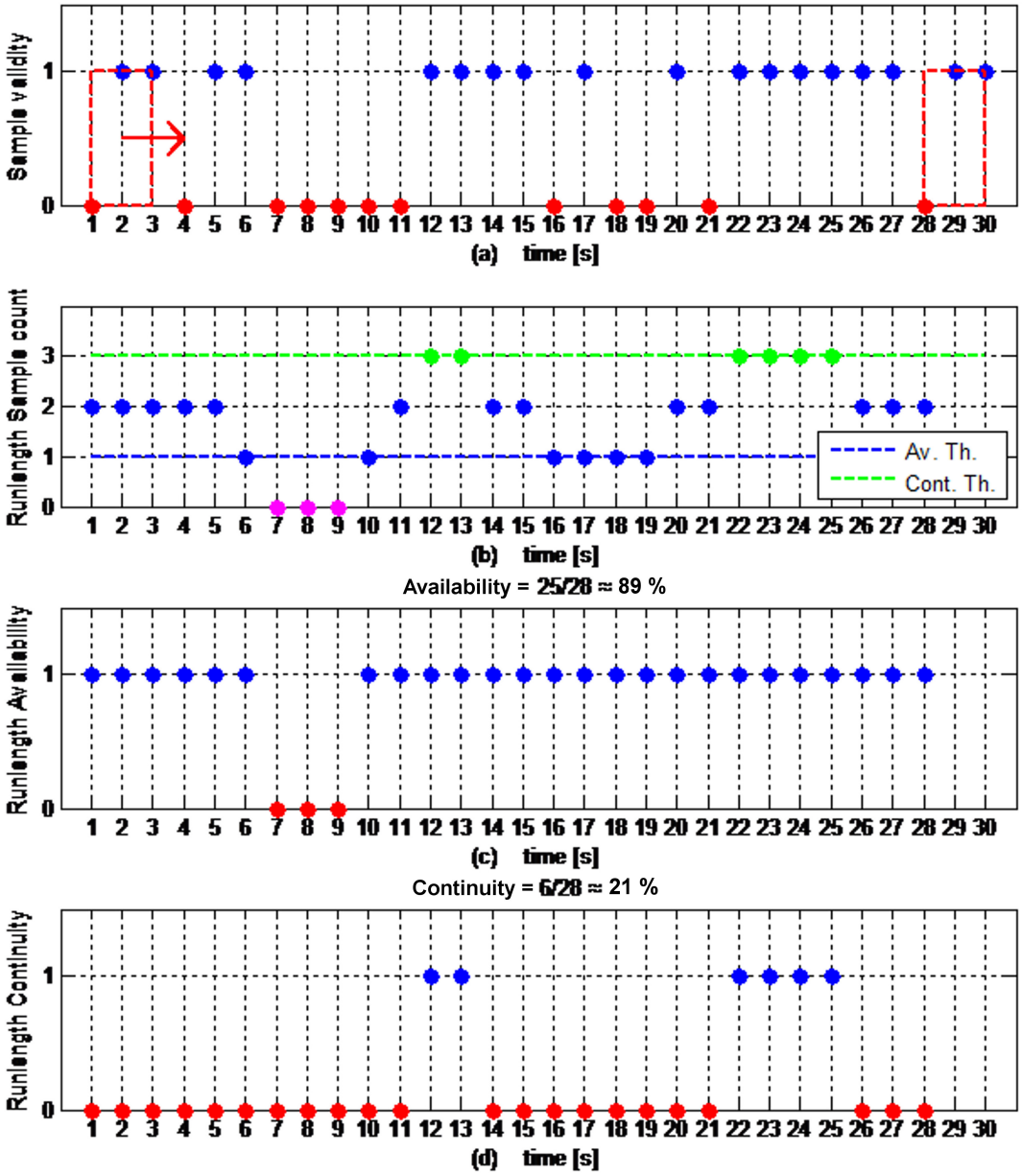


Figure 18 — Availability and continuity calculation: (a) raw samples validity, (b) Run-length sliding window sample count, (c) Run-length availability, (d) Run-length continuity

6.3 Other metrics

NOTE The ETSI TS 103 246–3 and CEN/TR 17464 considered specific metrics for security assessment. In the following list they are briefly analysed, and a rationale behind their inclusion or exclusion is provided.

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

6.3.1 Time To Fist Fix (TTFF)

Time to First Fix: TTFF measures the time of first fix, so for each run 1 (one) sample is collected. It is very time consuming to build a CDF. It is hence suggested to evaluate TTFF as an average, not a CDF, averaging 10 to 30 test runs. In CEN/TR 17465, specific test scenarios are proposed for TTFF evaluation. It seems better to reuse the same scenarios considered for the other security metrics, for the sake of homogeneity of the testing procedure. In particular, it is not clear why TTFF needs field tests. It seems also TTFF can be assessed, as the other metrics, i.e. with a Record (or Generation) and Replay of specific scenarios with jamming and spoofing superimposed to authentic GNSS signal.

The consortium agreed, for basic performance testing, not to address specific states of the receiver, as cold, warm or hot start, since it is not always possible to force the receiver in such states from the external.

Instead, it is proposed to test the DUT after a well-defined OFF period, so that aiding information becomes degraded or even useless, if too old.

This approach is in line also with security performance testing. Provided that for each test run 1 (one) sample of TTFF is derived, it is possible to repeat N times the same test scenario, stopping it as soon as the first Fix is reached. This approach is absolutely fine if it is assumed that all processes involved are ergodic and hence time averages are equivalent to statistical one. Also, in case of jamming this can apply. Each test run would experience:

- slightly misalignment of the replay starting point, due to semi-automatic replay procedure. This could for instance lead to different jamming phase at each run;
- different thermal noise contribution;
- different oscillators phase.

In particular for spoofing, where the attack has very complex dynamics and the scenario is highly non-stationary from a statistical perspective, it is suggested to reuse a recorded scenario N times by shifting the offset of the data set according to a well-defined pattern, to properly grab different relevant event in the scenario recording that may impact TTFF.

6.3.2 Excluded metrics

- **Detection flag/authenticity flag/time-to-alarm/probability of detection/false alarm**: these metrics are connected to threat detection capabilities of the GBPT. These metrics are also connected to time-to-alarm, i.e. the minimum time elapsed between threat condition is on and the first detection instant. After an internal consortium discussion these metrics have been excluded, at least as an initial assessment, mainly for 3 (three) main reasons:
  - many receivers are not able to provide them,
  - the proper evaluation of probability of detection and/or authentication or false alarm need a lot of samples (>30000 for a 10^{-4} value to be properly estimated), probably not in line with typical scenario length,
  - black box approach is preferred, where only degradation of baseline metrics is considered, and the end user would probably not use such new metrics;
- Resolution metrics: timestamp resolution or other resolution metrics are not reflecting any statistical behaviour. It is only a datasheet information. Maybe, as stated in CEN/TR 17448, position resolution can be provided, but timestamp resolution should be removed.

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

6.4 Robustness concept: a summary metric

All the metrics above described are somehow isolated one from the other. Assuming that a receiver manufacturer or ITS system integrator wants to assess the performance of "robustness" or "rejection factor" ρ of a receiver, assigning to the receiver a single number score. This could be a concise metric summarizing all the security assessment as a whole.

In this proposal, the robustness is clearly dependent on the type and number of scenarios, but it is clearly a way to weight different outcomes in a consistent way. It is dependent on distance function chosen and saturation values chosen, but once standardized, can be used to fairly and consistently compare different DUT.

Let us assume to have N_{sc} scenarios and each scenario i has $N_d(i)$ data files to be tested. In total we have N data file to be tested.

Let us assume to have K metrics to be tested $m_1,\cdots,m_K$. For each metric k to be tested, and each test run n, a distance estimator from basic-performance metrics shall be chosen $d_{n,k}$. The distance estimator is in line with CDF comparison distances reported in CEN/TR 17447: PVT error model report. The proper distance shall be created: for instance comparing CDF is different from comparing availability or continuity, but the following constraints shall hold:

- Non negativity: $d_{n,k} \geq 0$
- Identity: $d_{n,k} = 0$ if the outcome is equal to the basic-performance condition (equal CDF for instance)
- Normalization: $d_{n,k} = 1$ in case of result very distant (a threshold shall be selected). For the ease of distance calculation, it is suggested to use the dummy insertion approach to account for missing data, as described in 6.1.3.

It can be hence possible to calculate the mean distance, which is a convex combination of values in [0,1], and hence is confined to [0,1]:

$$\bar{d} = \frac{1}{M \cdot K} \sum_{k=1}^{K} \sum_{n=1}^{N} d_{n,k}$$

$$\rho = 1 - \bar{d} \tag{13}$$

Using this approach, it is easy to combine distances and obtain the robustness indicator that has the following bounds:

- $\rho = 1$ in case of all distance are 0, i.e. every test outcome has comparable performances with respect to basic-performance condition.
- $\rho = 0$ in case of all distance are 1, i.e. every test outcome has reached the saturation value and hence is very distant from the basic-performance condition, especially in case of heavy loss of data samples.

7 Test approach

NOTE This clause describes at high level the test approach suggested for security metrics assessment. In particular, leading-edge Software-Defined-Radio (SDR) equipment is proposed for the sake of flexibility and cost

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

reduction. Some insights on the effect of interference (being it jamming or spoofing) on the hardware of a GNSS receiver or data recording equipment are provided. After that, testing architectures are reported. The clause concludes with concepts regarding scenario files management and hybridization issues.

7.1 SDR concept

SDR (Software Defined Radio) identifies a communication system where all the components are software based. Specifically, a generic RF hardware can be connected at the end of the signal generation chain and it transmits all the samples that are generated, regardless what is their nature or standard. Within this project, the SDR architecture is very helpful, because it allows the operator to replay several kinds of recorded signal samples with the same radio peripheral. This approach leads to costs reduction and higher flexibility, since every test can be accomplished with no hardware modifications. This concept can be applied to the reception process as well. Essentially, with an SDR architecture it is possible to acquire signal samples with a general-purpose RF frontend and afterwards process and decode it in software mode. Figure 19 shows a very high-level RF chain, which highlights the software configuration of both the transmitting and receiving sides.

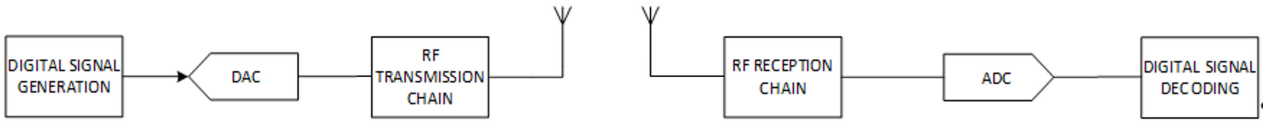


Figure 19 — SDR general scheme

7.2 Interference hardware impact

7.2.1 General

This subclause describes a brief overview of the jamming/spoofing effects on target receiver stages.

As depicted in Figure 20, a SDR front-end and is constituted of the following blocks:

- Antenna + Low Noise Amplifier (LNA).
- Variable Gain Amplifier (VGA) and Automatic Gain Control (AGC).
- Analog to digital Converter (ADC).
- Digital Processing.

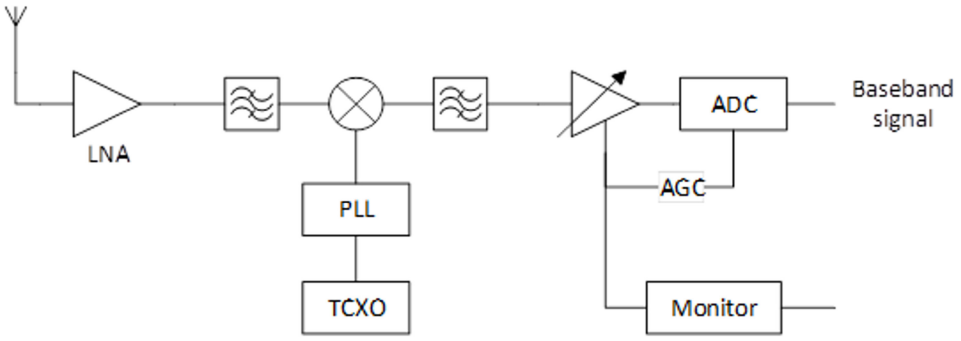


Figure 20 — Generic receiver front-end blocks

For each receiver block, specific jamming features could be designed to maximize the probability of failure.

Documents
Document Sharing Hub

Full document details: PD CEN/TR 17475:2020

7.2.2 Antenna-LNA

For power levels above a certain threshold, antenna and LNA may be damaged mainly for electric discharge (electric overstress EOS) or thermic phenomena. Typically, the maximum RF input for commercial receivers is about 20 dBm, therefore only a very powerful jammer of about 60 dBm-1 KW (considering at least 40 dB attenuation for space loss in the first meter) would be able to disrupt the frontend of a receiver.

7.2.3 AGC

If the AGC is available, and the jammer dynamic are slower than the AGC recovery time (i.e. the time window used to estimate the signal power in the AGC circuitry), a high jammer pulse can trigger the modification of the AGC gain. Therefore, in case of jamming superimposed to SIS signal, the AGC level is lower than the one experienced during SIS-only operations. An in-depth analysis of AGC can be found in Annex A. Typically spoofing can have little or no impact on AGC, since the AGC is locked to power level of thermal noise, which is 20 dB above authentic (or spoofing) GNSS signal.

For a good jamming signal characterization, 16 bits-resolution ADC is desirable (many commercial SDR product are already capable of this resolution). Moreover, the objective is to well characterize the jamming power, amplitude, pulsing and spectrum. A fast reacting AGC approach is not suitable for the recording purposes, since it can distort the signal. The target is fixing an amplitude scale and keeping it constant, for well defining in the signal samples file the amplitude variations of the jamming signal.

Specifically, the following guidelines, applicable to both jamming recording, shall be followed:

- Amplitude dynamic Range Estimation (preliminary phase):
    - start with low gain values, so that the jammer is fully contained in the ADC dynamic range, avoiding saturation,
    - set the AGC estimation window 10/100 times the period of the jamming signal, to properly capture the statistical evolution of the histogram of the jammer,
    - increase gain so that the 99,9 percentile of the signal is fully contained in the dynamic range of the ADC
- Signal recording:
    - use the above estimated gain for the whole recording session.

Following this approach, the jamming signal characteristics such as amplitude and power variations are well characterized.

The approach is very similar if the jammer is digitally generated. In this case, the samples are typically double precision floating point numbers that shall be properly rounded and stored on disk. The scaling shall be performed as above described. In this case the gain is a software scaling, but the concept still holds.

7.2.4 ADC

ADC and quantized signal samples are heavily affected by the presence of a jammer. The behaviour changes depending on AGC availability:

- Fast AGC: the AGC is able to adapt to the highest power level. A weak signal, e.g. GNSS one, buried below the noise, could be considerably attenuated or cancelled at all, depending on how many bits are used. High resolution 8-16 bits ADC suffer less this effect.

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

- AGC not present or slow AGC present: the ADC is tuned to the expected noise floor (in case of GNSS signal) or to the average signal amplitude, so a higher signal would lead to saturation of the ADC.

As for the AGC, spoofing has little or no impact on ADC, since its power should be far below the noise floor.

7.2.5 Digital post-correlation processing

Jamming has a quite important effect also if its power is comparable with the noise floor. In this case jamming affects both the acquisition and the tracking stage of a GNSS receiver, causing C/N0 degradation and PVT error. The digital processing part can be heavily impaired by a spoofing signal, since the power level and signal structure of spoofing signals are comparable to the ones of an authentic signal.

Interference impacts GNSS Receiver performance as follow:

- **Degradation of C/N0** that could provoke loss of tracking and lower availability of observables (Pseudo range, Carrier Phase…).
- Higher Noise on Code and Phase Observables leading a degradation of PVT Estimation.
- **Longer Acquisition Time** causing longer time to first fix.

The C/N0 is accurately described as the signal power to noise power density ratio. The C/N0 gives a good measure for the quality of a received signal as long as the noise has a flat spectrum over the entire frequency band (white noise) and can indeed be described by a scalar value (the noise power density). When there is also RFI the effective C/N0 should be used instead. This value uses a white noise power density that is equivalent to the actual noise plus interference.

$$\frac{C}{N_{0,eff}} = \frac{1}{\frac{1}{C/N_0} + \frac{J/S}{QR_c}} \tag{14}$$

Or equivalently:

$$\frac{C}{N_{0,eff}} = \frac{C}{N_0 + \frac{CQJ/S}{R_c}} \tag{15}$$

Where:

- C/N_0 is the unjammed signal to noise ratio.
- J/S is the jammer-to-signal ratio.
- R_c is the spreading code rate of the signal.
- Q is the dimensionless jamming resistance quality factor.

$$Q = \frac{1}{R_c \int_{-B_r/2}^{-B_r/2} G_s(f) G_i(f)} \tag{16}$$

Where

Documents
Document Sharing Hub

Full document details: PD CEN/TR 17475:2020

- B_r is the receiver bandwidth.
- $G_s(f)$ is the power spectral density of the signal normalized over the entire spectrum.
- $G_i(f)$ is the power spectral density of the interference normalized over the entire spectrum.

The above equation can be generalized for Pulsed Interference as follow for a receiver with Pulse Blanking mitigation:

$$\frac{C}{N_{0,eff}} = \frac{C(1-\sum_{k,(C\frac{J}{S}>TH)} pdc_k)}{N_0 + \frac{CQJ/S}{R_c}(\sum_{k,(C\frac{J}{S}<TH)} pdc_k)} \quad (17)$$

Where:

- pdc_k is the pulse duty cycle of the interferer.
- TH is the blanking threshold of the receiver.

Figure 21 and Figure 22 resume the effects in terms of C/N_0 degradation vs the J/S.

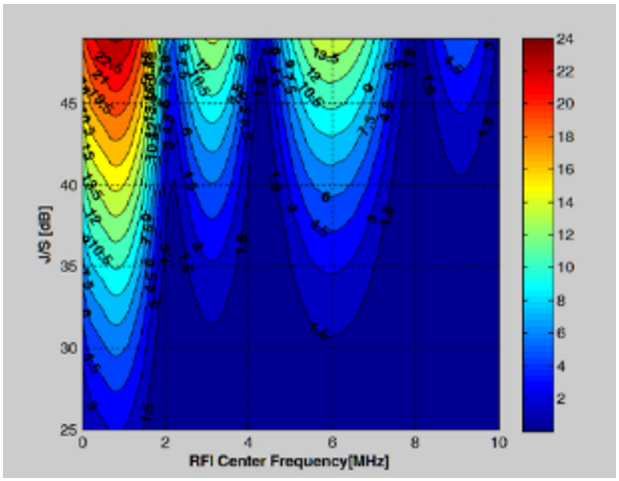


Figure 21 — C/N_0 Degradation for Galileo E1BC using a CHIRP Jamming

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

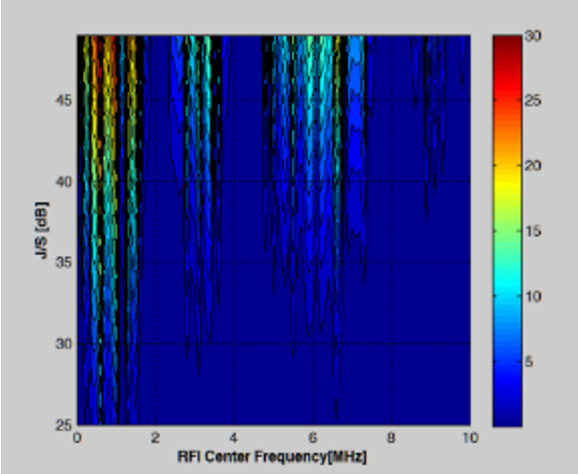


Figure 22 — C/N_0 Degradation for Galileo E1BC using a CW Jamming

7.3 Record and replay choice

Record and replay approach is the counterpart of the simulation option. In GNSS testing the record and replay foresees the sampling gathering with an RF device of the satellites signals. As specified in CEN/TR 17465, along with the samples recorder, additional equipment shall be used in order to derive the reference data concerning trajectory. In principle, the reference trajectory is not known a priori, therefore the recording means shall be able to perform precise positioning for having coherent test comparison. Instead, simulation option foresees the use of a RF constellation simulator that returns a precise reference position (it is set in the settings), but emulates a less realistic environment.

Both options are valid, because they coherently represent the received GNSS signal. They present some pros and cons. specifically, the record and replay choice shows many pros:

- very realistic scenarios, because it uses real signal samples;
- repeatable tests, the test foresees the replay of always the same batch;
- no need of buying a RFCS (Radio Frequency Constellation Simulator) for the test operator, a general purpose radio peripheral is required;
- the scenarios are generic and not linked to a specific RFCS, therefore a scenario library can be created and every receiver can be standardized referring to that library.

On the other hand, record and replay approach presents some cons, especially in the logistic:

- the data gathering process has huge impact on the test process;
- the computation of the reference data for the test comparison shall be very accurate for having a good base for the tests; this is not straightforward in all the environment;
- an overall SNR degradation is introduced in the recording process; more details are described in Annex D;
- calibration procedure on the transmitting RF device shall be accomplished and attenuators shall be included in the testbed, in order to reproduce the correct power levels.

Table 2 summarizes all the pros and cons just described.

Documents
Document Sharing Hub

Full document details: PD CEN/TR 17475:2020

Table 2 — Pros and Cons of record and replay approach

Pros	Cons
Extremely realistic scenarios	Data gathering process high impact
Repeatable tests	Hard computation of reference data
No need to buy RFCS	SNR degradation
Scenario library creation	Power calibration procedure necessary

Record and replay procedure is in principle the most accurate approach for testing, because it perfectly reproduces the real-world conditions. However, the process introduces additional noise with respect to the simulated case, because two frontends are involved. Although the record and replay tests are for sure still valid, an analysis of this effect should be carried out and is introduced in Annex D.

To summarize, since a loss in SNR is always present due to the noise amplification process, the following recommendations shall be adopted for record and replay approach:

- use at least a 16-bit capable record tool, to minimize quantization error;
- use an amplification level that fully exploits the dynamic range of the ADC;
- use low noise figure amplifier, that have the higher impact on overall noise figure;
- choose an acquisition bandwidth that is in line with the one of DUT (much bigger bandwidth is a waste of disk space).

7.4 Jamming testing architecture

This subclause is aimed at analysing the applicable jamming test architectures and performing a choice among them. There are mainly 2 (two) possible architectures for jamming testing, which are:

- Record SIS (Signal In Space) and jamming separately;
- Record SIS + jamming together.

The first approach allows the tester to add the jamming at runtime and easily combine the scenarios, namely the jamming can be applied to all the nominal recordings. On the other hand, the second type of architecture foresees a simpler replay setup, because it includes a unique batch.

Given the higher flexibility and reusability of the signal samples, the first option is preferred. The separated recording procedure is applicable because there is no need for synchronisation with the SIS. Jamming is a generic signal interference that does not require specific precision, unlike spoofing that has to be perfectly synchronised with the SIS. The main advantage is identified by the applicability of the recorded jamming signals to all the nominal scenarios, for performance assessment over all the environments. Within this test approach, the jamming signal samples can be generated in 2 (two) different manners:

- real jammer signal recording;
- SDR jamming signal generator.

The real jammer option foresees the record of a real jamming equipment. Many options can be found in the market, such as Privacy Protection Devices (PPDs). Different solutions are described in *Software-defined radio based roadside jammer detector: Architecture and results, Position, Location and Navigation Symposium* (ref. Bibliography [1])

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

This approach allows to generate a realistic jamming signal and provides test flexibility because the disturbance is recorded separately with respect to the SIS. However, the SDR generation option gives even more flexibility and possibilities to the user. Specifically, a wide variety of signals can be generated with a software defined approach without buying specific equipment for every different jamming type. The SDR jamming generation would dramatically dwindle the samples construction costs and increasing the signal quality, since it foresees less recording steps, reducing the overall noise. An SDR allows to create jamming signals that go beyond the usual CW and Chirp in commerce, such as:

- nonlinear chirp (i.e. Sine Frequency Modulation);
- slow and Fast Frequency Hopping;
- radar-like jamming signals.

In light of these considerations, the SDR option is the most promising testing architecture. Figure 24 shows the high-level architecture of the jamming testbed.

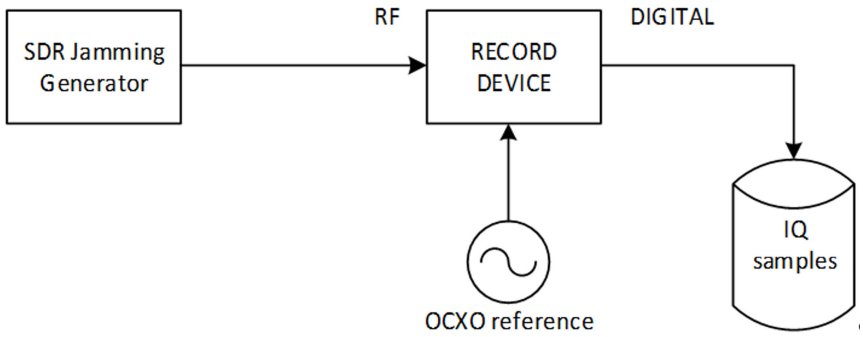


Figure 23 — Jamming recording architecture including SDR Jamming Generator

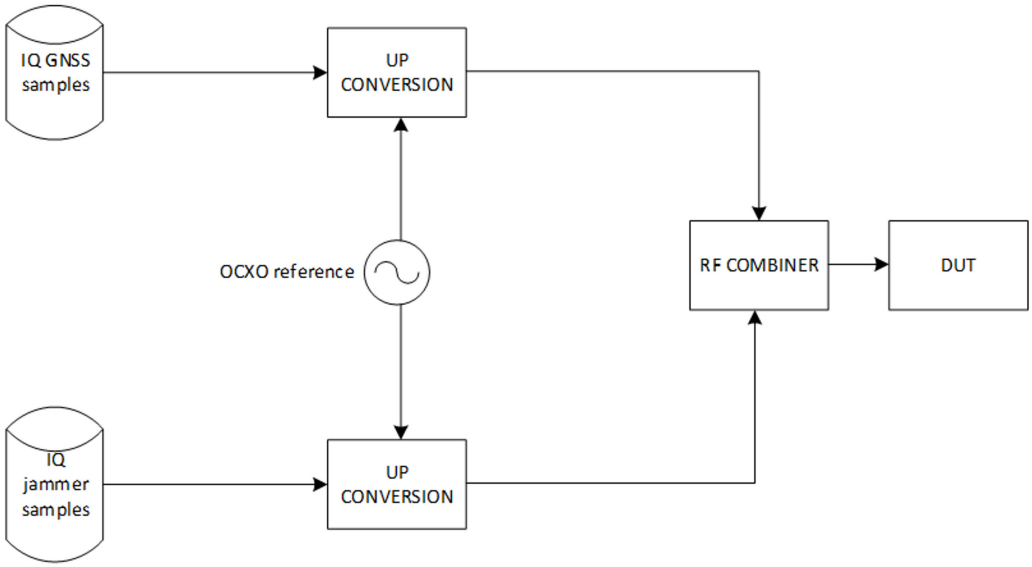


Figure 24 — Jamming testing high-level architecture

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020

The RF connections shall include attenuators to set the output power to levels compliant with the GNSS standard. Moreover, the RF signal generators output power shall be well known to the operator, in order to perform realistic tests.

7.5 Spoofing testing architecture

Spoofing scenario recording requires more attention to the synchronisation with the SIS with respect to the jamming one. Therefore, the recording option stated for the jamming scenarios is not preferable anymore. Spoofing signals need fine synchronisation for being effective, so the recording shall be achieved in a unique sample file, along with the reference GNSS signal.

In this configuration 2 (two) paths can be followed:

- equipping the recording vehicle with a constellation simulator that, getting the ephemeris, observables and PPS (Pulse Per Second) from a receiver locked into the SIS, generates a spoofing signal that is combined with the real SIS before the frontend;
- generating the whole signal with RFCS and record the output.

Figure 25 shows a high-level scheme of the first approach, instead Figure 26 describes the second configuration. Even though the first approach would be more realistic, the second seems to be much more straightforward and linear. Performing spoofing on the live signal that includes multipath and several additional impairments can be very complicated. Moreover, the second approach isolates the performance of the DUT under spoofing with respect to the environment impairments.

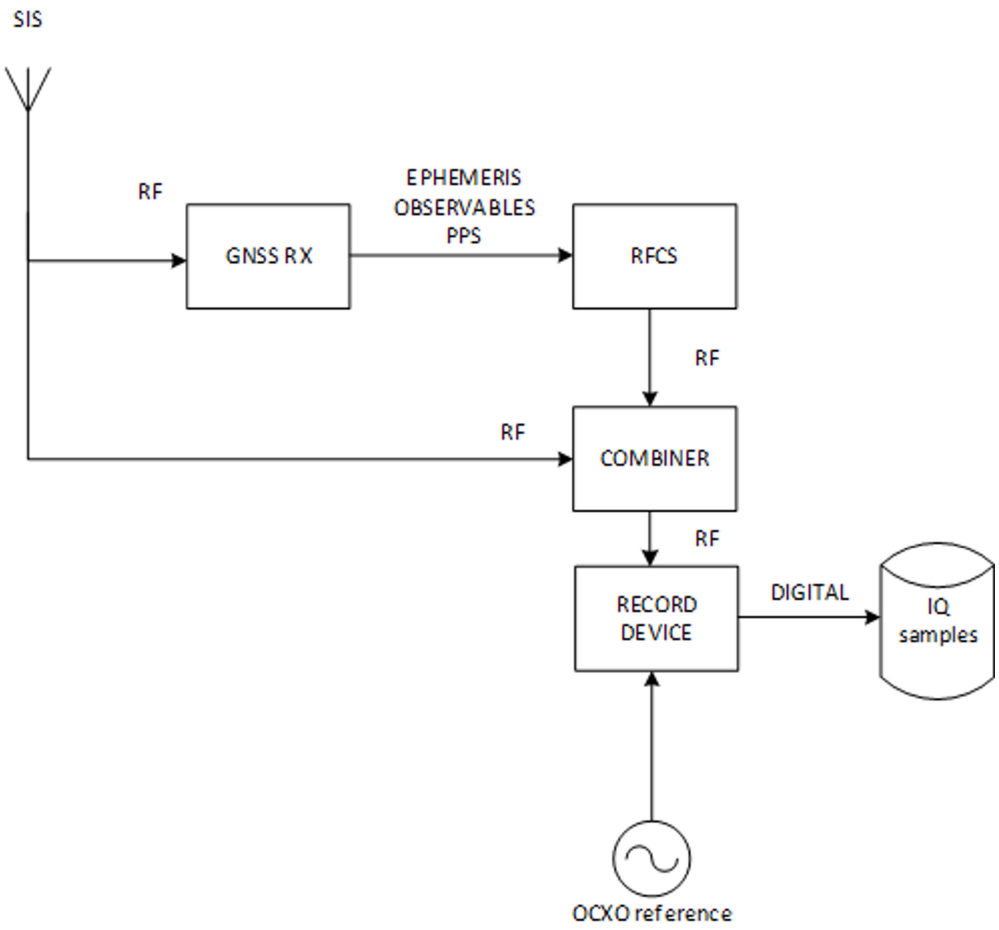


Figure 25 — Spoofing recording architecture performing live spoofing

Documents
Document Sharing Hub
Full document details: PD CEN/TR 17475:2020