

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 Testscenarien, 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

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 First 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

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

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.

This document is a preview generated by EVS

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*

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

authentication

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