

**SLOVENSKI STANDARD**  
**oSIST prEN 16803-3:2019**  
**01-april-2019**

---

**Vesolje - Uporaba sistemov globalne satelitske navigacije (GNSS) za ugotavljanje položaja pri inteligentnih transportnih sistemih (ITS) v cestnem prometu - 3. del: Ocenjevanje varnostnih tehničnih lastnosti terminalske opreme za določanje položaja, ki uporablja GNSS**

Space - Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) - Part 3: Assessment of security performances of GNSS-based positioning terminals

Raumfahrt - Anwendung von GNSS-basierter Ortung für Intelligente Transportsysteme (ITS) im Straßenverkehr - Teil 3: Überprüfung der sicheren Leistungen von GNSS-basierten Ortungsendgeräten [SIST EN 16803-3:2020](https://standards.iteh.ai/catalog/standards/sist/814ad11f-80a1-4b8e-aa47-92bce571a245/sist-en-16803-3-2020)

Espace - Utilisation du positionnement GNSS pour les systèmes de transport routier intelligents (ITS) - Partie 3 : Evaluation des performances de sécurité des terminaux de positionnement GNSS

**Ta slovenski standard je istoveten z: prEN 16803-3**

---

**ICS:**

|           |  |  |
|-----------|--|--|
| 03.220.20 | Cestni transport   | Road transport   |
| 33.060.30 | Radiorelejni in fiksni satelitski komunikacijski sistemi | Radio relay and fixed satellite communications systems |
| 35.240.60 | Uporabniške rešitve IT v prometu                         | IT applications in transport                           |

**oSIST prEN 16803-3:2019**

**en,fr,de**



EUROPEAN STANDARD  
NORME EUROPÉENNE  
EUROPÄISCHE NORM

**DRAFT**  
**prEN 16803-3**

February 2019

ICS 03.220.20; 33.060.30; 35.240.60

English version

## Space - Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) - Part 3: Assessment of security performances of GNSS-based positioning terminals

Espace - Utilisation du positionnement GNSS pour les systèmes de transport routier intelligents (ITS) - Partie 3 : Evaluation des performances de sécurité des terminaux de positionnement GNSS

Raumfahrt - Anwendung von GNSS-basierter Ortung für Intelligente Transportsysteme (ITS) im Straßenverkehr - Teil 3: Überprüfung der sicheren Leistungen von GNSS-basierten Ortungsendgeräten

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/CLC/JTC 5.

If this draft becomes a European Standard, CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN and CENELEC in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation. Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

**Warning** : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.



| <b>Contents</b>   | <b>Page</b> |
|---|-------------|
| European foreword.....  | 5           |
| Introduction .....  | 6           |
| <b>1 Scope.....</b>   | <b>8</b>    |
| <b>2 Normative references.....</b>  | <b>8</b>    |
| <b>3 Terms and definitions .....</b>  | <b>8</b>    |
| <b>3.1 Definitions .....</b>  | <b>8</b>    |
| <b>3.2 Acronyms .....</b>   | <b>10</b>   |
| <b>4 Description of the general logic of the security tests.....</b>                      | <b>12</b>   |
| <b>4.1 Record and Replay principle.....</b>   | <b>12</b>   |
| <b>4.2 Specificity of security tests based upon the R&amp;R approach.....</b>             | <b>12</b>   |
| <b>4.3 Jamming testing Architecture.....</b>  | <b>13</b>   |
| <b>4.4 Spoofing/meaconing testing architecture .....</b>                                  | <b>14</b>   |
| <b>5 Definition of the metrics with respect to security performances.....</b>             | <b>16</b>   |
| <b>5.1 General.....</b>   | <b>16</b>   |
| <b>5.2 Accuracy metrics.....</b>  | <b>16</b>   |
| <b>5.3 Availability and continuity metrics .....</b>                                      | <b>18</b>   |
| <b>5.4 Integrity metrics.....</b>   | <b>18</b>   |
| <b>5.4.1 Protection Level performance metrics .....</b>                                   | <b>18</b>   |
| <b>5.4.2 Misleading Information metrics .....</b>   | <b>19</b>   |
| <b>5.5 Timing metrics .....</b>   | <b>19</b>   |
| <b>5.5.1 Timestamp resolution .....</b>   | <b>19</b>   |
| <b>5.5.2 Nominal output latency.....</b>  | <b>19</b>   |
| <b>5.5.3 Nominal output rate.....</b>   | <b>19</b>   |
| <b>5.5.4 Output latency stability.....</b>  | <b>20</b>   |
| <b>5.5.5 Output rate stability.....</b>   | <b>20</b>   |
| <b>5.5.6 Time to first fix.....</b>   | <b>20</b>   |
| <b>6 Description of the test procedures and the test equipment.....</b>                   | <b>21</b>   |
| <b>6.1 Scope .....</b>  | <b>21</b>   |
| <b>6.2 Setting-up of the replay test-bench.....</b>                                       | <b>22</b>   |
| <b>6.2.1 Replay device calibration.....</b>   | <b>22</b>   |
| <b>6.2.2 Replay testbed architecture .....</b>  | <b>24</b>   |
| <b>6.3 Validation of the data processing HW and SW by the RF test laboratory .....</b>    | <b>25</b>   |
| <b>6.4 Replaying of the data .....</b>  | <b>26</b>   |
| <b>6.4.1 General.....</b>   | <b>26</b>   |
| <b>6.4.2 Jamming scenarios.....</b>   | <b>26</b>   |
| <b>6.4.3 Spoofing &amp; meaconing scenarios.....</b>                                      | <b>26</b>   |
| <b>6.5 Computation of metrics degradation .....</b>                                       | <b>27</b>   |
| <b>6.5.1 General.....</b>   | <b>27</b>   |
| <b>6.5.2 Jamming scenarios.....</b>   | <b>27</b>   |
| <b>6.5.3 Spoofing &amp; meaconing scenarios.....</b>                                      | <b>28</b>   |
| <b>6.6 Establishment of the final test report.....</b>                                    | <b>28</b>   |
| <b>7 Validation procedure.....</b>  | <b>28</b>   |
| <b>8 Definition of the synthesis report: how to report the results of the tests .....</b> | <b>28</b>   |

|  |           |
|--|-----------|
| <b>Annex A (informative) Analysis of the GNSS attacks taxonomy</b> .....   | <b>35</b> |
| <b>A.1 General</b> .....   | <b>35</b> |
| <b>A.2 Categorisation of GNSS attacks</b> .....  | <b>35</b> |
| <b>A.3 GNSS attack models</b> .....  | <b>36</b> |
| <b>A.3.1 General</b> .....   | <b>36</b> |
| <b>A.3.2 Interference and jamming attacks</b> .....  | <b>36</b> |
| <b>A.3.3 Meaconing attacks</b> .....   | <b>37</b> |
| <b>A.3.4 Spoofing attacks</b> .....  | <b>37</b> |
| <b>Annex B (informative) Security-specific metrics (authentication capabilities, spoofing and jamming detection flags, etc.)</b> ..... | <b>39</b> |
| <b>Annex C (informative) Scenarios proposition</b> .....   | <b>41</b> |
| <b>C.1 General</b> .....   | <b>41</b> |
| <b>C.2 Jamming/interference proposed scenarios</b> .....   | <b>41</b> |
| <b>C.3 Spoofing proposed scenarios</b> .....   | <b>42</b> |
| <b>C.4 Meaconing proposed scenarios</b> .....  | <b>45</b> |
| <b>Annex D (informative) Spoofing insights</b> .....   | <b>47</b> |
| <b>D.1 General</b> .....   | <b>47</b> |
| <b>D.2 Range error impact</b> .....  | <b>48</b> |
| <b>D.3 Oscillator error impact</b> .....   | <b>48</b> |
| <b>D.4 Propagation channel impact</b> .....  | <b>49</b> |
| <b>Annex E (informative) Dataset record testbed</b> .....  | <b>51</b> |
| <b>E.1 General</b> .....   | <b>51</b> |
| <b>E.2 Jamming data generation</b> .....   | <b>51</b> |
| <b>E.3 Spoofing data recording</b> .....   | <b>55</b> |
| <b>Bibliography</b> .....  | <b>56</b> |

## List of Figures

|  |           |
|--|-----------|
| <b>Figure 1 — Generic functional architecture of a Positioning-based road ITS system</b> ..... | <b>6</b>  |
| <b>Figure 2 — Jamming recording architecture including SDR jamming generator</b> .....         | <b>14</b> |
| <b>Figure 3 — Jamming testing high-level architecture</b> .....                                | <b>14</b> |
| <b>Figure 4 — Spoofing recording architecture performing live spoofing</b> .....               | <b>15</b> |
| <b>Figure 5 — Spoofing recording architecture including RFCS</b> .....                         | <b>15</b> |
| <b>Figure 6 — Spoofing testing high-level architecture</b> .....                               | <b>16</b> |
| <b>Figure 7 — Accuracy degradation metrics</b> .....   | <b>17</b> |
| <b>Figure 8 — Scheme of gain contribution for calibration</b> .....                            | <b>23</b> |

|   |           |
|---|-----------|
| <b>Figure 9 — Calibration table construction high-level architecture, to estimate the DEVICE GAIN .....</b> | <b>23</b> |
| <b>Figure 10 — Spoofing/Nominal replay testbed architecture .....</b>                                       | <b>25</b> |
| <b>Figure 11 — Jamming replay testbed architecture .....</b>  | <b>25</b> |
| <b>Figure 12 — NDS and ADS position in the jamming testing architecture .....</b>                           | <b>26</b> |
| <b>Figure 13 — NDS position in the spoofing testing architecture .....</b>                                  | <b>27</b> |
| <b>Figure 14 — ADS position in the spoofing testing architecture.....</b>                                   | <b>27</b> |
| <b>Figure A.1 — GNSS attacks taxonomy.....</b>  | <b>35</b> |
| <b>Figure C.1 — CW typical jamming scenario .....</b>   | <b>42</b> |
| <b>Figure C.2 — Chirp typical jamming scenario .....</b>  | <b>42</b> |
| <b>Figure C.3 — Spoofing relative position/velocity dynamics.....</b>                                       | <b>43</b> |
| <b>Figure C.4 — Spoofing relative power profile .....</b>   | <b>44</b> |
| <b>Figure D.1 — Propagation in Free Space and Hata Channel models.....</b>                                  | <b>50</b> |
| <b>Figure E.1 — CW jammer .....</b>   | <b>52</b> |
| <b>Figure E.2 — LFM chirp jammer.....</b>   | <b>52</b> |
| <b>Figure E.3 — NLFM chirp jammer.....</b>  | <b>52</b> |
| <b>Figure E.4 — Radar jammer.....</b>   | <b>53</b> |
| <b>Figure E.5 — Frequency hopping fast jammer.....</b>  | <b>53</b> |
| <b>Figure E.6 — Frequency hopping slow jammer.....</b>  | <b>53</b> |
| <b>Figure E.7 — Noise Narrowband jammer .....</b>   | <b>54</b> |
| <b>Figure E.8 — Noise broadband jammer.....</b>   | <b>54</b> |
| <b>Figure E.9 — Jamming recording architecture .....</b>  | <b>55</b> |
| <b>Figure E.10 — Spoofing recording architecture.....</b>   | <b>55</b> |

#### List of Tables

|   |           |
|---|-----------|
| <b>Table C.1 — Four types of jamming scenarios .....</b>              | <b>41</b> |
| <b>Table C.2 — Spoofing scenarios.....</b>                            | <b>44</b> |
| <b>Table C.3 — Meaconing scenarios .....</b>                          | <b>45</b> |
| <b>Table D.1 — Attacker Technology to estimate User Distance.....</b> | <b>48</b> |
| <b>Table D.2 — Range Estimation Error .....</b>                       | <b>48</b> |
| <b>Table D.3 — Oscillator summary .....</b>                           | <b>49</b> |
| <b>Table D.4 — Power Estimation Error due to the environment.....</b> | <b>50</b> |

## European foreword

This document (prEN 16803-3:2019) has been prepared by Technical Committee CEN-CENELEC/TC 5 “SPACE”, the secretariat of which is held by DIN.

This document is currently submitted to the CEN Enquiry.

This document has been prepared under a mandate given to CEN and CENELEC by the European Commission and the European Free Trade Association.

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

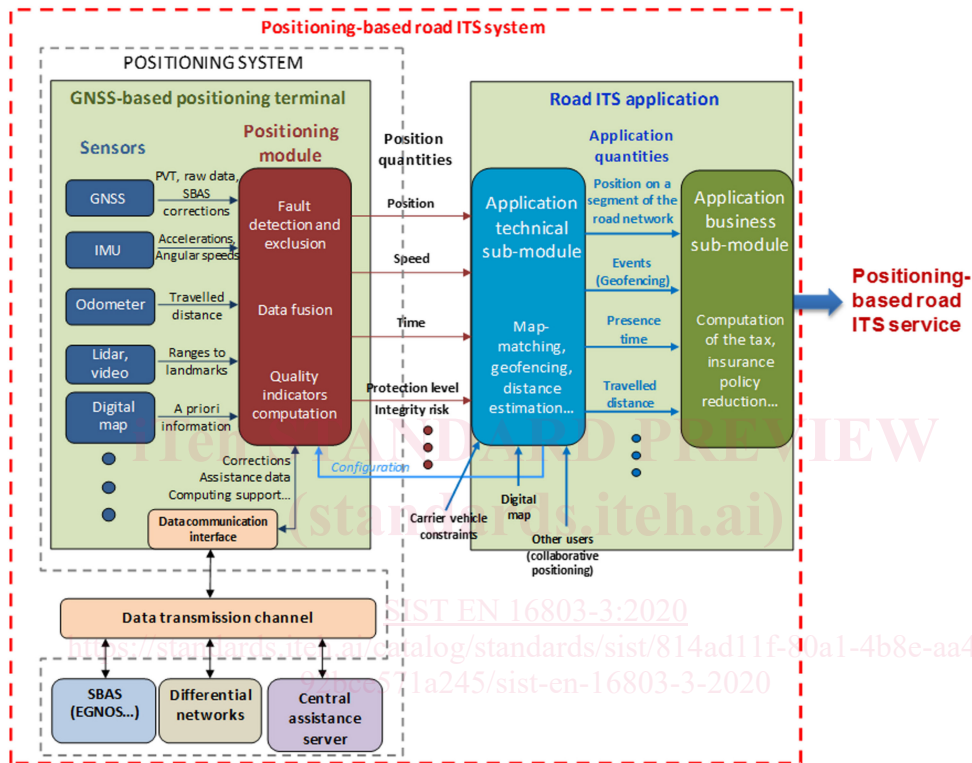
SIST EN 16803-3:2020

<https://standards.iteh.ai/catalog/standards/sist/814ad11f-80a1-4b8e-aa47-92bce571a245/sist-en-16803-3-2020>

## Introduction

The EN 16803 series of CEN-CENELEC standards deals with the use of GNSS technology in the intelligent transport domain and addresses more particularly the issue of performance assessment.

As recalled in the generic functional architecture of a road ITS system based on GNSS, two main sub-systems can be considered: the positioning system (GNSS-based positioning terminal (GBPT) + external sources of data) and the road ITS application processing the position quantities output by the terminal to deliver the final service to the user.



**Figure 1 — Generic functional architecture of a Positioning-based road ITS system**

This EN is the third one of the EN 16803 series.

EN 16803-1 standard proposes a method called “Sensitivity analysis” to assess the adequacy of the GBPT’s performances to the end-to-end performance of the road ITS system. In addition, this first EN defines the generic architecture, the generic terms and the basic performance metrics for the Positioning quantities.

EN 16803-2 proposes a test methodology based on the replay in the lab of real data sets recorded during field tests, assuming no security attack during the test.

This standard, EN 16803-3, proposes a complement to this **Record & Replay (R&R)** test methodology to assess the performance degradation when the GNSS signal-in-space (SIS) is affected by intentional or unintentional radio-frequency (RF) perturbations. Next sections below stress the importance of this assessment in the context of the security threats.

The number of applications in road *Intelligent Transport Systems (ITS)* relying on *Global Navigation Satellite System (GNSS)* technologies has shown an impressive growth in recent years. At the same time, as many of those applications can be considered safety-critical or liability-critical, the need to increase the robustness and the security of the *GNSS-Based Positioning Terminal (GBPT)* is becoming a critical



point. Civil GNSS signals and receivers are known to be vulnerable not only to natural impairments (e.g. atmospheric effects, presence of multipath and obstacles) or unintentional interference, but also to attacks of intentional nature. For instance, in the case of road ITS, it is widely discussed how users hoping to perpetrate fraud on road tolling applications might attack an on-board GNSS receiver in order to elude a payment. In this scenario, the malicious user can try to disrupt the receiver functionalities (typically through **jamming**), making it either unable to compute a *Position, Velocity, and Time* (PVT) information, or even forcing it to output counterfeit PVT data (e.g. through **spoofing** attacks). While in past years these types of GNSS attacks were considered as feasible but requiring significant technical means, it is not the case today considering that illegal jammers are available on the market for just a few euros and basic spoofing attacks can be carried out at relatively low cost.

GNSS positioning threats have intensely interested the research community and the industry over the last decade, motivating the increasing awareness on the GNSS vulnerabilities and the development of suitable countermeasures. For instance, the reader can refer to the following recent publications, see Bibliography [5] [6] [7] [8] [9] [10].

In this context, device manufacturers have started to implement new technologies to make their positioning modules robust against GNSS attacks. In addition, major advances have been done in the GNSS security aspects in Europe, especially those related to the development of new GNSS capabilities for the Galileo system (i.e. civil authentication services provided by means of cryptographically protected signals, see Bibliography [12] [13] [14] [15]).

These trends motivate a standardization effort in order to identify, harmonize, and properly define GNSS attack scenarios and test procedures. In this sense, a first important step is to define a **common categorization of relevant GNSS attacks**.

For this reason, Annex A of this standard aims to provide a high-level categorization of GNSS attacks (A.1) and a brief description of possible attack models in each category (A.2). It is important to read carefully Annex A to understand correctly the meaning of this document. It is informative in the sense that it provides informative material related to the attack scenarios that shall be used in a R&R process for security tests, compatible with the quality required for high-level standards. In fact, a wide number of possible attacks have been proposed in past years and new threats continue to emerge, not just based on controlled simulations done by GNSS security experts and researchers in their laboratories, but also with an impressive number of reported real world accidents (e.g., see Bibliography [16] and [17]).

## 1 Scope

This document shall be considered as a complementary standard to EN 16803-2 that is intended to assessment of the performances of a GBPT placed in real-life or simulated road environments. This document is instead specifically targeting security attacks such as interferences, jamming, meaconing or spoofing. This document cannot be applied independently from EN 16803-2 that describes in details the general methodology of the assessment procedure.

This document provides normative information necessary to replay in the lab standardized scenarios specifically dedicated to security tests applied to GNSS.

Depending on the case (jamming or spoofing), these scenarios are composed of data sets combining either real life recorded SIS and jamming signals or simulated SIS and spoofing signals. The reason for that will be explained in Clause 6.

Although a high-level categorization of GNSS attacks is given in Annex A, a comprehensive and detailed categorization of possible GNSS attacks is out of the scope of this document.

It is not the aim of this EN to standardize the record procedure neither to define the specific requirements for the generation of the attack scenarios. The record procedure itself and its quality framework for accredited GNSS-specialized laboratories (Lab-A), with the detailed definition of standardized attack scenarios, will be totally and precisely described in EN 16803-4 (under preparation). The list of attack scenarios will have to be regularly updated considering the evolution of GNSS technologies, emerging threats, and countermeasures.

## 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, *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*

prEN 16803-2:2018, *Space — Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) — Part 2: Assessment field tests for basic performances of GNSS-based positioning terminals*

## 3 Terms and definitions

### 3.1 Definitions

For the purposes of this document, the following terms and definitions apply.

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

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

Relevant definitions, extracted from ETSI TS 103 246-3, ISO/IEC 27001 and on ISO online browsing platform (<https://www.iso.org/obp/ui/#search>).

#### 3.1.1

##### **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

[SOURCE: ETSI TS 103 246-3]

**3.1.2****jamming**

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

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

[SOURCE: ETSI TS 103 246-3]

**3.1.3****spooof/spoofing**

transmission of signals intended to deceive location processing into reporting false location target data

[SOURCE: ETSI TS 103 246-3]

**3.1.4****threat**

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

[SOURCE: ISO/IEC 27001]

**3.1.5****vulnerability**

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

[SOURCE: ISO/IEC 27001]

**3.1.6****GBPT**

GNSS Based Positioning Terminal. Term used to define the component that basically outputs PVT

**3.1.7****DUT****Device Under Test**

term used to defined a device that is assessed

Note 1 to entry: In the context of EN 16803-2, DUT refers to GPBT.

**3.1.8****Test Scenario**

a Test Scenario is composed of GNSS SIS data and potential sensor data resulting from field tests, complemented by a metadata description file; a test scenario is a non-empty combination of UTS that allows to assess a GBPT in the desired environments

Note 1 to entry: Data inside a Test Scenario are raw data, either RF signals from GNSS satellites, or raw data from other embedded sensors.

Note 2 to entry: A Test Scenario is the whole package that a GNSS-specialized test laboratory delivers to a Generalist RF test laboratory in charge of performance assessment tests according to the EN 16803 series.

Note 3 to entry: Considering the 6 (six) different environments as defined in EN 16803-1, there's a combination of  $2^6 - 1 = 63$  possible test scenarios; from let's say "Rural only" test scenario up to "All environment" test scenario that covers the 6 (six) different environments.

**prEN 16803-3:2019 (E)****3.1.9****Unitary Test Scenario (UTS)**

a Unitary Test Scenario is an elementary brick of a Test Scenario, resulting from a specific field test; in other words, a Test Scenario is composed of a concatenation of several Unitary Test Scenarios

**3.1.10****Uniform Environment Data Set (UEDS)**

Uniform Environment Data Set is the output of the DUT collected after a replay in laboratory sorted by environment; it is a concatenation of the output of the DUT for all UTS restricted to a unique environment

Note 1 to entry: Considering the 6 different environments as defined in EN 16803-1, there is the same number of UEDS ; i.e. 6(six).

Note 2 to entry: Data composing a Uniform Environment Data Set are PVT data, as they are output by a GBPT.

Note 3 to entry: Uniform Environment Data Sets are the data sets to which the metrics shall be applied to assess the performances of the device under test.

**3.1.11****GNSS-specialized test laboratory**

laboratory in charge of producing Test Scenarios for generalist RF test laboratories

**3.1.12****Generalist RF test laboratory**

laboratory in charge of assessing the performances of GBPTs thanks to Test Scenario

**3.1.13****Benchmark Unitary Test Scenario (B-UTS)**

dedicated UTS used specifically for the validation procedure as defined in Clause 7

**3.1.14****Benchmark Uniform Environment Data Set (B-UEDS)**

each of the UEDS obtained with the benchmark receiver at the GNSS specialised lab (used by the generalist lab to validate their test platform and procedures)

**3.2 Acronyms**

For the purposes of this document, the following acronyms apply.

| Acronym | Description   |
|---------|---|
| ACAI    | Availability, Continuity, Accuracy, Integrity   |
| ADC     | Analog to Digital Converter   |
| ADS     | Attacked Data Set   |
| AGC     | Automatic Gain Control  |
| CEN     | <i>Comité Européen de Normalisation</i> (European Committee for Standardization)                                      |
| CENELEC | <i>Comité Européen de Normalisation Électrotechnique</i><br>(European Committee for Electrotechnical Standardization) |
| CSAC    | Chip Scale Atomic clock   |
| CW      | Continuous Waves  |

| Acronym | Description  |
|---------|--|
| DAC     | Digital to Analog Converter  |
| DUT     | Device Under Test  |
| ETSI    | European Telecommunications Standards Institute  |
| GBPT    | GNSS-Based Positioning Terminal  |
| GNSS    | Global Navigation Satellite Systems  |
| I/Q     | In-phase and Quadrature – I/Q format is an efficient way to store RF signals so that it is possible to reproduce RF signals in laboratory after modulation. I/Q format is the format used to store GNSS UTS. |
| IMU     | Inertial Measurement Unit  |
| ITS     | Intelligent Transport Systems  |
| J/S     | Jamming to Signal ratio  |
| LNA     | Low Noise Amplifier  |
| Lab-A   | GNSS-specialized test laboratory   |
| Lab-B   | Generalist RF test laboratory  |
| MIR     | Misleading Information Rate  |
| NDS     | Nominal Data Set   |
| OCXO    | Oven-controlled crystal oscillator   |
| PA      | Power Amplifier  |
| PPS     | Pulse Per Second   |
| PVT     | Position Velocity and Time   |
| RAIM    | Receiver Autonomous Integrity Monitoring   |
| RF      | Radio Frequency  |
| RFCS    | Radio Frequency Constellation Simulator  |
| RMS     | Root Mean Square   |
| R&R     | Record & Replay  |
| SBAS    | Satellite Based Augmentation System  |
| SDR     | Software Defined Radio   |
| SIS     | Signal In Space  |
| SNR     | Signal to Noise Ratio  |
| TCXO    | Temperature-controlled crystal oscillator  |
| TIR     | Target Integrity Risk  |
| TTF     | Time To First Fix  |
| UTS     | Unitary Test Scenario  |
| UEDS    | Uniform Environment Data Set   |

## 4 Description of the general logic of the security tests

### 4.1 Record and Replay principle

Security tests in EN 16803-3 are based on the same methodology as the tests described in EN 16803-2, designed for assessing the basic performance features **Availability**, **Continuity**, **Accuracy**, **Integrity** (ACAI) and **Time-To-First-Fix** (TTFF) of the PVT information.

This methodology is called **Record & Replay** (R&R). The rationale for this choice and the advantages of this methodology are explained in details in prEN 16803-2:2018, 4.1.1 and 4.1.2.

Different test approaches exist. To be effective and widely accepted, test procedures shall be:

- representative;
- repeatable;
- rapid;
- affordable.

R&R approach consists in replaying in a laboratory GNSS Signal-In-Space (SIS) data, and potentially additional sensor data or assistance/correction data, recorded in specific operational conditions thanks to a specific test vehicle. The dataset comprising GNSS SIS data and potential sensor or assistance/correction data resulting from these field tests, together with the corresponding metadata description file, is called a “**test scenario**”.

This approach is:

- **representative** of the reality, when the proper set of scenarios is identified. The representativeness is for sure much higher than fully simulated environment;
- **repeatable**: it is very easy to replay even complex scenarios with low-complexity testbed. Apart from thermal noise, very few variables change. The degrees of freedom of the testbed lower dramatically with respect to live testing, improving the repeatability;
- **rapid**: once received the scenario datasets, the testbed setup is “trivial”, or at least showing a complexity that can be afforded by a non-GNSS-expert test engineer;
- **affordable**: since replaying equipment is much cheaper than full-featured GNSS simulators. It also allows measures in pre-compliance in company laboratories, at very reasonable cost if entry level equipment is used.

For what concerns nominal scenarios, EN 16803-2 proposes an optimized merge of:

- use cases (type of trips);
- road topologies;
- GNSS environments as per (EN 16803-1).

### 4.2 Specificity of security tests based upon the R&R approach

The difference between the two categories of assessment tests (standard tests and security tests) is the following:

- in EN 16803-2, the SIS data files recorded in the scenario are assumed to be free of interferences and jamming/spoofing/meaconing attacks;

- in EN 16803-3, specific jamming, or spoofing, or meaconing signals are added to the SIS data files for the replay phase in the laboratory (Lab-B).

Nevertheless, given the differences between the two categories of attacks (jamming versus spoofing/meaconing), two different approaches for adding the interfering signals leading to two different test architectures shall be applied. These architectures are defined in the next two sections.

### 4.3 Jamming testing Architecture

There are mainly two possible architectures for jamming testing, which are:

- record SIS and jamming signal separately;
- record SIS + jamming signal 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 signal stream to be replayed.

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 two different manners:

- real jammer signal recording;
- software design radio (SDR) jamming signal generator.

The real jammer option foresees the record of real jamming equipment. Many options can be found in the market, such as Privacy Protection Devices (PPDs). Different solutions are described in [18]. This option allows generating 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 decrease the samples construction costs and increase the signal quality, since it foresees less recording steps, reducing the overall noise. An SDR allows creating jamming signals that go beyond the usual CW and Chirp in commerce, such as:

- non-linear 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 and is the one proposed in this standard. It is important to underline that SDR jamming generators might generate directly digital samples, without the need of recording device and hence minimizing the noise contribution, mainly due to the recording device.

Figure 2 shows the jamming recording architecture and Figure 3 the high-level architecture of the jamming testbed for the replaying phase.

The jamming signal is added to the reconstructed SIS by Lab-B in charge of the DUT testing.