BS EN 16803-3:2020

BSI Standards Publication

Space — Use of GNSS-based positioning for road Intelligent Transport Systems (ITS)

Part 3: Assessment of security performances of GNSS-based positioning terminals

bsi.

National foreword

This British Standard is the UK implementation of EN 16803-3:2020.

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 committee manager.

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 01836 3

ICS 33.060.30; 03.220.20; 35.240.60

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2020.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16803-3

September 2020

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 : Évaluation 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 European Standard was approved by CEN on 15 June 2020.

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. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists 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, 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.

Contents

Page

European foreword

This document (EN 16803-3:2020) has been prepared by Technical Committee CEN-CENELEC/TC 5 “Space”, the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by March 2021, and conflicting national standards shall be withdrawn at the latest by March 2021.

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

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: 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 the United Kingdom.

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.

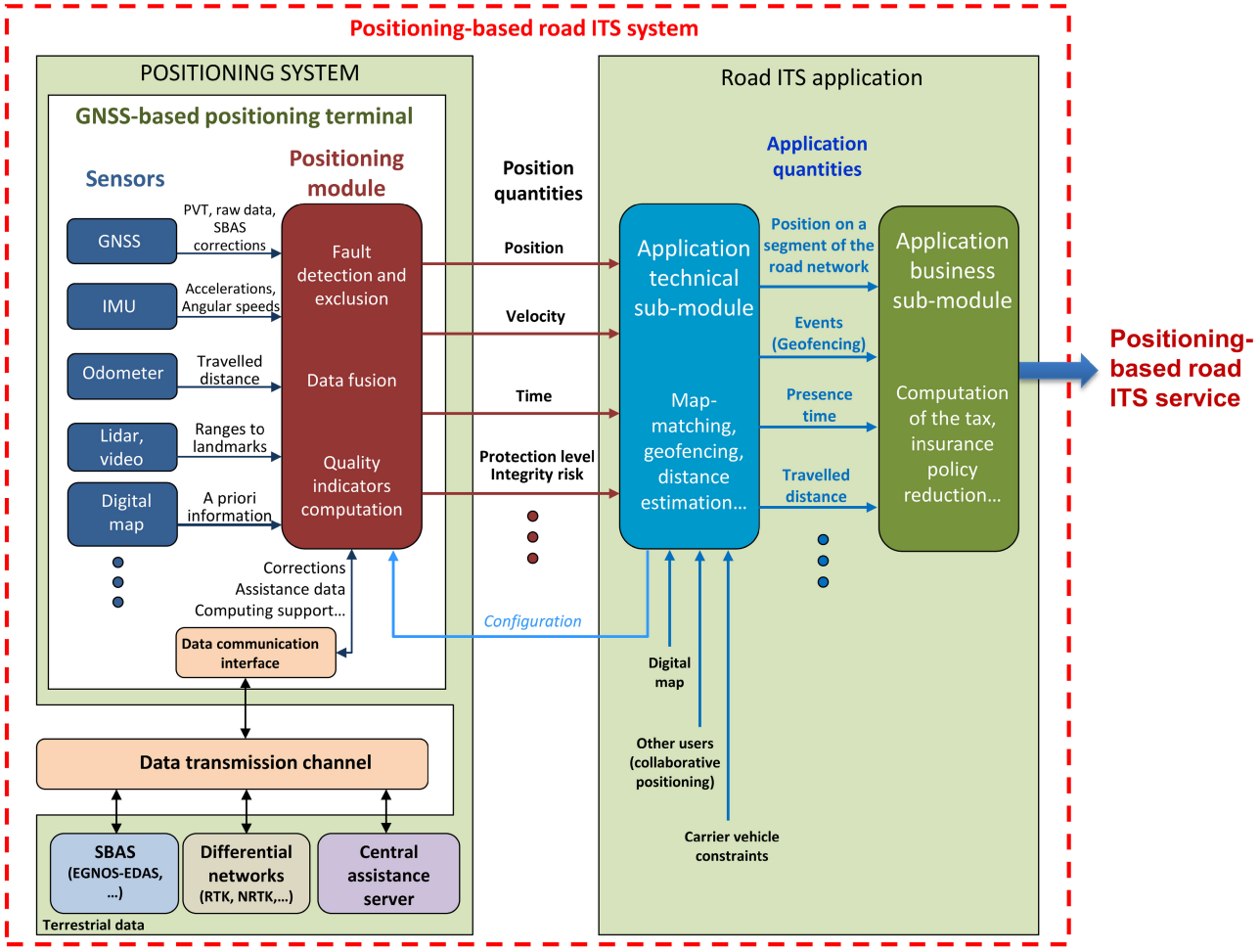

Figure 1 — Generic functional architecture of a Positioning-based road ITS system

This document 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 document, 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 is 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 detail 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 document 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*

EN 16803-2:2020, *Space — Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) — Part 2: Assessment of basic performances of GNSS-based positioning terminals*