

E DIN EN 16803-3:2019-03 (D/E)

Erscheinungsdatum: 2019-02-15

Raumfahrt - Anwendung von GNSS-basierter Ortung für Intelligente Transportsysteme (ITS) im Straßenverkehr - Teil 3: Überprüfung der sicheren Leistungen von GNSS-basierten Ortungsendgeräten; Deutsche und Englische Fassung prEN 16803-3:2019

Space - Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) - Part 3: Assessment of security performances of GNSS-based positioning terminals; German and English version prEN 16803-3:2019

Inhalt	Seite
Europäisches Vorwort.....	5
Einleitung	6
1 Anwendungsbereich.....	8
2 Normative Verweisungen	8
3 Begriffe	8
3.1 Definitionen	8
3.2 Abkürzungen	11
4 Beschreibung der allgemeinen Logik der Sicherheitsprüfungen	12
4.1 Prinzip von Aufzeichnung und Wiedergabe	12
4.2 Beschreibung von Sicherheitsprüfungen, die auf dem R&R-Ansatz beruhen	13
4.3 Prüfarchitektur für Störsendungen	13
4.4 Prüfarchitektur zur Prüfung von Spoofing/Meaconing.....	15
5 Definition der Metriken bezogen auf die Sicherheitsleistungsdaten	17
5.1 Allgemeines.....	17
5.2 Genauigkeitsmetriken	17
5.3 Verfügbarkeits- und Stetigkeitsmetriken	18
5.4 Integritätsmetriken	19
5.4.1 Leistungsmetriken der Protection Levels	19
5.4.2 Metrik der irreführenden Informationen	19
5.5 Zeitsteuerungsmetriken	20
5.5.1 Zeitstempelauflösung	20
5.5.2 Nominelle Ausgabelatenz	20
5.5.3 Nominelle Ausgabegeschwindigkeit	20
5.5.4 Stabilität der Ausgabelatenz.....	20
5.5.5 Stabilität der Ausgabegeschwindigkeit.....	21
5.5.6 Time To First Fix.....	21
6 Beschreibung der Prüfverfahren und der Prüfeinrichtung.....	22
6.1 Anwendungsbereich.....	22
6.2 Aufstellung des Wiedergabeprüfstandes.....	22
6.2.1 Kalibrieren des Wiedergabegeräts.....	22
6.2.2 Architektur des Wiedergabe-Prüfstandes	25
6.3 Validierung der zur Datenverarbeitung verwendeten Hard- und Software durch das HF-Prüflaboratorium	26
6.4 Wiedergabe der Daten	27
6.4.1 Allgemeines.....	27
6.4.2 Störsendungsszenario	27
6.4.3 Spoofing- und Meaconing-Szenarien.....	27

6.5	Berechnung der Minderung von Metriken.....	28
6.5.1	Allgemeines.....	28
6.5.2	Störsendungsszenarien.....	28
6.5.3	Spoofing- und Meaconing-Szenarien.....	29
6.6	Erstellung des Abschlussberichts zur Prüfung.....	29
7	Validierungsverfahren	29
8	Definition des Syntheseberichts: Wie die Ergebnisse der Prüfungen im Bericht anzugeben sind	29
Anhang A (informativ) Systematik der Analyse der GNSS-Angriffe.....		37
A.1	Allgemeines.....	37
A.2	Einteilung von GNSS-Angriffen in Kategorien.....	37
A.3	GNSS-Angriffsmodelle.....	38
A.3.1	Allgemeines.....	38
A.3.2	Angriffe durch Störbeeinflussung und Störsendung	38
A.3.3	Meaconing-Angriffe	39
A.3.4	Spoofing-Angriffe	39
Anhang B (informativ) Sicherheitsspezifische Metriken (Authentifizierungsfunktionen, Erkennungs-Flags für Spoofing und Störsendung usw.).....		41
Anhang C (informativ) Empfohlene Szenarien.....		43
C.1	Allgemeines.....	43
C.2	Empfohlene Störsendungs-/Störbeeinflussungsszenarien.....	43
C.3	Empfohlene Spoofing-Szenarien	44
C.4	Empfohlene Meaconing-Szenarien	47
Anhang D (informativ) Spoofing-Erkenntnisse		49
D.1	Allgemeines.....	49
D.2	Auswirkung von Bereichsfehlern	50
D.3	Auswirkung von Oszillatorfehlern	50
D.4	Einfluss des Ausbreitungskanal.....	51
Anhang E (informativ) Prüfstand für die Aufzeichnung von Datensätzen		53
E.1	Allgemeines.....	53
E.2	Erzeugung von Störsendungsdaten.....	53
E.3	Aufzeichnung von Spoofing-Daten.....	57
Literaturhinweise		58

Bilder

Bild 1	— Generische Funktionsarchitektur eines ortungsbasierten ITS für den Straßenverkehr	6
Bild 2	— Architektur der Aufzeichnung der Störsendung mit SDR-Störgenerator	15
Bild 3	— Übergeordnete Architektur der Prüfung mit Störsendung	15
Bild 4	— Architektur der Spoofing-Aufzeichnung zur Durchführung von Live-Spoofing.....	16
Bild 5	— Architektur der Spoofing-Aufzeichnung mit RFCS	16
Bild 6	— Übergeordnete Architektur der Spoofing-Prüfung	16
Bild 7	— Minderung der Genauigkeitsmetrik	18
Bild 8	— Schema der Verstärkungsbeiträge für die Kalibrierung	23
Bild 9	— Übergeordnete Architektur für den Aufbau des Kalibrierschemas zur Ermittlung der GERÄTEVERSTÄRKUNG	24
Bild 10	— Architektur des Wiedergabe-Prüfstandes mit Spoofing-/nominellen Signalen	25
Bild 11	— Architektur des Wiedergabe-Prüfstandes mit Störsendung	26
Bild 12	— Position von NDS und ADS in der Architektur der Prüfung mit Störsendung	27
Bild 13	— Position des NDS in der Architektur mit Spoofing	28
Bild 14	— Position des ADS in der Architektur mit Spoofing	28
Bild A.1	— Systematik der GNSS-Angriffe	37

Bild C.1 — Typisches CW-Störsendungsszenario	44
Bild C.2 — Typisches Chirp-Störsendungsszenario	44
Bild C.3 — Relative Spoofing-Dynamik von Position/Geschwindigkeit	45
Bild C.4 — Relatives Spoofing-Leistungsprofil	46
Bild D.1 — Ausbreitung im Kanalmodell des freien Raumes und im Hata-Kanalmodell	52
Bild E.1 — CW-Störsender	54
Bild E.2 — LFM-Chirp-Störsender	54
Bild E.3 — NLFM-Chirp-Störsender	54
Bild E.4 — Radar-Störsender.....	55
Bild E.5 — Störsender mit schnellem Frequenzwechsel	55
Bild E.6 — Störsender mit langsamem Frequenzwechsel.....	55
Bild E.7 — Störsender mit Schmalbandrauschen	56
Bild E.8 — Störsender mit Breitbandrauschen	56
Bild E.9 — Aufzeichnungsarchitektur für eine Störsendung	57
Bild E.10 — Spoofing-Aufzeichnungsarchitektur	57

Tabellen

Tabelle C.1 — Vier Arten von Störsendungsszenarien	43
Tabelle C.2 — Spoofing-Szenarien.....	47
Tabelle C.3 — Meaconing-Szenarien.....	48
Tabelle D.1 — Angreifertechnologie zur Abschätzung der Abstands zum Anwender.....	50
Tabelle D.2 — Abschätzung des Bereichsfehlers.....	50
Tabelle D.3 — Zusammenfassung der Oszillatoren	51
Tabelle D.4 — Fehler der Leistungsabschätzung durch die Umgebung.....	52