

# DIN EN 16803-3:2021-07 (D)

## Raumfahrt - Anwendung von GNSS-basierter Ortung für Intelligente Transportsysteme (ITS) im Straßenverkehr - Teil 3: Überprüfung der sicheren Leistungen von GNSS-basierten Ortungsendgeräten; Deutsche Fassung EN 16803-3:2020

---

Inhalt	Seite
Europäisches Vorwort.....	4
Einleitung .....	5
1 Anwendungsbereich.....	7
2 Normative Verweisungen .....	7
3 Begriffe und Abkürzungen .....	7
3.1 Begriffe .....	7
3.2 Abkürzungen .....	10
4 Beschreibung der allgemeinen Logik der Sicherheitsprüfungen .....	11
4.1 Prinzip von Aufzeichnung und Wiedergabe .....	11
4.2 Beschreibung von Sicherheitsprüfungen, die auf dem R&R-Ansatz beruhen .....	12
4.3 Prüfarchitektur für Störsendungen .....	12
4.4 Prüfarchitektur zur Prüfung von Spoofing/Meaconing.....	14
5 Definition der Metriken bezogen auf die Sicherheitsleistungsdaten .....	16
5.1 Allgemeines.....	16
5.2 Genauigkeitsmetriken .....	16
5.3 Verfügbarkeits- und Stetigkeitsmetriken .....	17
5.4 Integritätsmetriken .....	18
5.5 Zeitsteuerungsmetriken .....	19
6 Beschreibung der Prüfverfahren und der Prüfeinrichtung.....	21
6.1 Anwendungsbereich.....	21
6.2 Aufstellung des Wiedergabeprüfstandes.....	21
6.3 Validierung der zur Datenverarbeitung verwendeten Hard- und Software durch das HF-Prüflaboratorium .....	25
6.4 Wiedergabe der Daten .....	26
6.5 Berechnung der Minderung von Metriken.....	28
6.6 Erstellung des Abschlussberichts zur Prüfung .....	28
7 Validierungsverfahren .....	28
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
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 Empfohlenes Spoofing-Szenario .....	45

<b>C.4</b>	<b>Empfohlene Meaconing-Szenarien .....</b>	<b>47</b>
	<b>Anhang D (informativ) Spoofing-Erkenntnisse.....</b>	<b>48</b>
<b>D.1</b>	<b>Allgemeines.....</b>	<b>48</b>
<b>D.2</b>	<b>Auswirkung von Bereichsfehlern .....</b>	<b>49</b>
<b>D.3</b>	<b>Auswirkung von Oszillatorfehlern .....</b>	<b>50</b>
<b>D.4</b>	<b>Ausbreitungskanal.....</b>	<b>51</b>
	<b>Anhang E (informativ) Prüfstand für die Aufzeichnung von Datensätzen .....</b>	<b>52</b>
<b>E.1</b>	<b>Allgemeines.....</b>	<b>52</b>
<b>E.2</b>	<b>Erzeugung von Störsendungsdaten.....</b>	<b>52</b>
<b>E.3</b>	<b>Aufzeichnung von Spoofing-Daten.....</b>	<b>56</b>
	<b>Literaturhinweise .....</b>	<b>57</b>