

DIN EN 16803-3

ICS 03.220.20; 33.060.30; 35.240.60

**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**

Space –
Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) –
Part 3: Assessment of security performances of GNSS-based positioning terminals;
German version EN 16803-3:2020

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;
Version allemande EN 16803-3:2020

Gesamtumfang 60 Seiten

DIN-Normenausschuss Luft- und Raumfahrt (NL)

Nationales Vorwort

Dieses Dokument (EN 16803-3:2020) wurde vom Technischen Komitee CEN/CLC/JTC 5 „Raumfahrt“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Gremium ist der Arbeitsausschuss NA 131-06-02 AA „Interoperabilität von Informations-, Kommunikations- und Navigationssystemen“ im DIN-Normenausschuss Luft- und Raumfahrt (NL).

DIN EN 16803 besteht unter dem allgemeinen Titel *Raumfahrt — Anwendung von GNSS-basierter Ortung für Intelligente Transportsysteme (ITS) im Straßenverkehr* aus den folgenden Teilen:

- Teil 1: Definitionen und Systemtechnikverfahren für die Festlegung und Überprüfung von Leistungsdaten
- Teil 2: Bestimmung der grundlegenden Leistungen von GNSS-basierten Ortungsendgeräten
- Teil 3: Überprüfung der sicheren Leistungen von GNSS-basierten Ortungsendgeräten.

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 9001	siehe	DIN EN ISO 9001
ISO/IEC 17025	siehe	DIN EN ISO/IEC 17025
ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

DIN EN ISO/IEC 17025, *Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien*

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen*

Deutsche Fassung

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

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

Diese Europäische Norm wurde vom CEN am 15. Juni 2020 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

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
C.4 Empfohlene Meaconing-Szenarien	47
Anhang D (informativ) Spoofing-Erkenntnisse	48
D.1 Allgemeines	48

D.2 Auswirkung von Bereichsfehlern..... 49

D.3 Auswirkung von Oszillatorfehlern..... 50

D.4 Ausbreitungskanal..... 51

Anhang E (informativ) Prüfstand für die Aufzeichnung von Datensätzen 52

E.1 Allgemeines 52

E.2 Erzeugung von Störsendungsdaten 52

E.3 Aufzeichnung von Spoofing-Daten 56

Literaturhinweise..... 57

Europäisches Vorwort

Dieses Dokument (EN 16803-3:2020) wurde vom Technischen Komitee CEN-CENELEC/TC 5 „Raumfahrt“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis März 2021, und etwaige entgegenstehende nationale Normen müssen bis März 2021 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument wurde im Rahmen eines Mandats erarbeitet, das die Europäische Kommission und die Europäische Freihandelsassoziation CEN und CENELEC erteilt haben.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Einleitung

Die CEN-CENELEC-Normenreihe EN 16803 befasst sich mit der Nutzung der GNSS-Technologie im Bereich des intelligenten Transports und besonders mit dem Aspekt der Leistungsüberprüfung.

Wie in der generischen Funktionsarchitektur eines GNSS-basierten ITS für den Straßenverkehr dargelegt, können zwei Haupt-Subsysteme betrachtet werden: das Ortungssystem (GNSS-basiertes Ortungsendgerät [GBPT] + externe Datenquellen) und die ITS-Anwendung für den Straßenverkehr, die die vom Endgerät ausgegebenen Positionsgrößen verarbeitet, um dem Anwender den Enddienst zur Verfügung zu stellen.

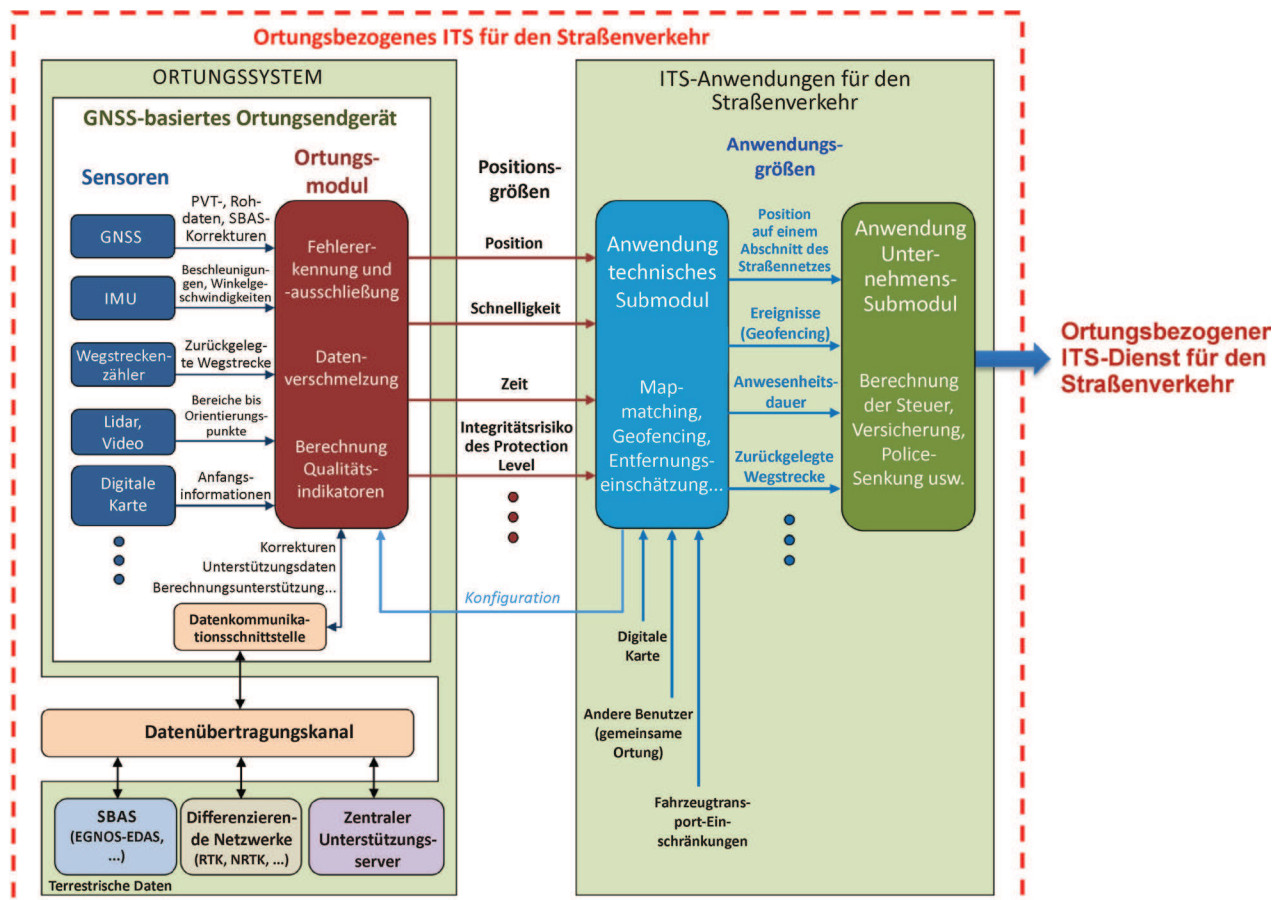


Bild 1 — Generische Funktionsarchitektur eines ortungsbasierten ITS für den Straßenverkehr

Dieses Dokument ist Teil 3 der Normenreihe EN 16803.

Die Norm EN 16803-1 schlägt ein als „Sensitivitätsanalyse“ bezeichnetes Verfahren für die Beurteilung der Angemessenheit der Leistungsdaten des GBPT für die Ende-zu-Ende-Leistung des ITS für den Straßenverkehr vor. Darüber hinaus legt diese erste Europäische Norm die generische Architektur, die generischen Begriffe und die grundlegenden Leistungsmetriken für die Ortungsgrößen fest.

EN 16803-2 schlägt eine Prüfmethodik vor, die auf der Wiedergabe von echten in Einsatzprüfungen aufgezeichneten Datensätzen im Labor basiert – unter der Annahme, dass während der Prüfung kein Sicherheitsangriff erfolgt ist.

Dieses Dokument EN 16803-3 schlägt eine Ergänzung zu dieser **Aufzeichnung/Wiedergabe**-Prüfmethodik (R&R-Prüfung) vor, die dazu dient, die Leistungsminderung bei Beeinträchtigung des GNSS-Signal-in-Space (SIS) durch vorsätzlich oder unabsichtlich erzeugte Hochfrequenz(HF)-Störungen zu überprüfen. In den nachfolgenden Abschnitten wird die Bedeutung dieser Überprüfung im Zusammenhang mit Sicherheitsrisiken hervorgehoben.

Die Zahl von Anwendungen in *intelligenten Transportsystemen* (ITS) für den Straßenverkehr, die auf der Technik der *globalen Navigationssatellitensysteme* (GNSS) beruhen, hat in den letzten Jahren stark zugenommen. In dem gleichen Maß, wie viele dieser Anwendungen als sicherheitskritisch oder kritisch bezüglich der Haftung angesehen werden können, wird die Notwendigkeit der Verbesserung der Stabilität und der Sicherheit des *GNSS-basierten Ortungsendgeräts* (GBPT) ein entscheidender Punkt. Es ist bekannt, dass zivile GNSS-Signale und -Empfänger nicht nur natürlichen Beeinträchtigungen (z. B. atmosphärische Wirkungen, Mehrwegausbreitung und vorhandene Hindernisse) oder unerwünschten Störbeeinflussungen, sondern auch vorsätzlichen Angriffen ausgesetzt sind. Bei ITS für den Straßenverkehr wird z. B. häufig diskutiert, wie Anwender, die einen Gebührenbetrug an Mautanwendungen begehen möchten, einen fahrzeugseitigen GNSS-Empfänger angreifen können, um sich der Zahlung zu entziehen. Bei diesem Szenario kann der böswillige Anwender versuchen, die Empfängerfunktionen zu stören (gewöhnlich durch **Störsendungen**), indem er entweder die Berechnung einer *Positions-, Geschwindigkeits- und Zeitinformation* (PVT-Information) unmöglich macht oder sogar die Ausgabe gefälschter PVT-Daten erzwingt (z. B. durch **Spoofing**-Angriffe). Während diese Arten von GNSS-Angriffen in den vergangenen Jahren als durchführbar angesehen wurden, allerdings verbunden mit einem erheblichen technischen Aufwand, ist das heutzutage nicht mehr der Fall, wenn die Tatsache berücksichtigt wird, dass illegale Störsender für nur wenige Euro auf dem Markt verfügbar und Spoofing-Angriffe mit relativ geringen Kosten möglich sind.

Die Forschungsgemeinschaft und die Industrie haben sich im letzten Jahrzehnt intensiv mit Bedrohungen der GNSS-basierten Ortung beschäftigt, was das zunehmende Bewusstsein für die Schwachstellen des GNSS und die Entwicklung geeigneter Gegenmaßnahmen angeregt hat. Der Leser kann z. B. auf die folgenden neuesten Veröffentlichungen aus den Literaturhinweisen zurückgreifen [5] [6] [7] [8] [9] [10].

In diesem Zusammenhang haben Gerätehersteller begonnen, neue Technologien einzuführen, um ihre Ortungsmodule sicherer gegen GNSS-Angriffe zu machen. Darüber hinaus wurden in Europa große Fortschritte bei den GNSS-Sicherheitsaspekten gemacht, besonders in Bezug auf die Entwicklung neuer GNSS-Funktionen für das Galileo-System (z. B. zivile Authentifizierungsdienste durch kryptografisch geschützte Signale, siehe Literaturhinweise [12] [13] [14] [15]).

Diese Entwicklungen fördern Normungsbestrebungen zur Beschreibung, Harmonisierung und genauen Definition von GNSS-Angriffsszenarien und Prüfverfahren. In diesem Sinne ist ein erster wichtiger Schritt die Festlegung einer **allgemeinen Einteilung von einschlägigen GNSS-Angriffen in Kategorien**.

Dafür enthält Anhang A der vorliegenden Norm eine Einteilung von GNSS-Angriffen in übergeordnete Kategorien (A.1) und eine kurze Beschreibung möglicher Angriffsmodelle in jeder Kategorie (A.2). Für das richtige Verständnis des vorliegenden Dokuments ist es wichtig, Anhang A sorgfältig zu lesen. Er ist insofern informativ, als er Informationsmaterial für die Angriffsszenarien bereitstellt, die in einem R&R-Prozess für Sicherheitsprüfungen, die mit der für High-level-Standards erforderlichen Qualität kompatibel sind, verwendet werden müssen. Tatsächlich wurde in den letzten Jahren eine große Anzahl möglicher Angriffe vorgeschlagen und es ergeben sich ständig neue Bedrohungen, und das nicht nur durch von GNSS-Sicherheitsfachleuten und Forschern in ihren Laboren gesteuerte Simulationen sondern mit einer beachtlichen Zahl auch als gemeldete reale Vorfälle (z. B. siehe Literaturhinweise [16] und [17]).

1 Anwendungsbereich

Das vorliegende Dokument ist eine ergänzende Norm zu EN 16803-2, die für die Überprüfung der Leistungsdaten eines GBPT in realen oder simulierten Straßenumgebungen vorgesehen ist. Dieses Dokument behandelt stattdessen speziell ausgerichtete Sicherheitsangriffe wie Störbeeinflussungen, Störsendungen, Meaconing oder Spoofing. Es kann nicht unabhängig von EN 16803-2 angewendet werden, die die allgemeine Methodik für das Überprüfungsverfahren eingehend beschreibt.

Dieses Dokument enthält normative Informationen, die notwendig sind, um im Labor genormte Szenarien, die speziell für auf GNSS zutreffende Sicherheitsprüfungen vorgesehen sind, wiederzugeben.

In Abhängigkeit vom Störfall (Störsendung oder Spoofing) setzen sich diese Szenarien aus Datensätzen zusammen, die entweder echte aufgenommene SIS und Signale von Störsendern oder simulierte SIS und Spoofing-Signale miteinander kombinieren. Die Gründe für diesen Ansatz werden in Abschnitt 6 erläutert.

Auch wenn Anhang A eine Einteilung von GNSS-Angriffen in übergeordnete Kategorien enthält, gehört eine umfassende und genaue Einteilung möglicher GNSS-Angriffe nicht zum Anwendungsbereich des vorliegenden Dokuments.

Ziel dieses Dokuments ist weder die Normung des Aufzeichnungsverfahrens noch die Festlegung spezifischer Anforderungen für die Aufstellung der Angriffsszenarien. Das Aufzeichnungsverfahren selbst und sein Qualitätsrahmen für bevollmächtigte auf GNSS spezialisierte Labore (Lab-A) mit der genauen Definition der genormten Angriffsszenarien werden vollständig und eingehend in EN 16803-4 (in Vorbereitung) beschrieben. Die Liste der Angriffsszenarien muss unter Berücksichtigung der Weiterentwicklung der GNSS-Technologie, auftretender Bedrohungen und Gegenmaßnahmen regelmäßig aktualisiert werden.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

EN 16803-1, *Raumfahrt — Anwendung von GNSS-basierter Ortung für Intelligente Transportsysteme (ITS) im Straßenverkehr — Teil 1: Definitionen und Systemtechnikverfahren für die Festlegung und Überprüfung von Leistungsdaten*

EN 16803-2:2020, *Raumfahrt — Anwendung von GNSS-basierter Ortung für Intelligente Transportsysteme (ITS) im Straßenverkehr — Teil 2: Bestimmung der grundlegenden Leistungen von GNSS-basierten Ortungsendgeräten*

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

3.1.1

elektromagnetische Störung

Quelle einer HF-Übertragung innerhalb des von einer Kommunikationsverbindung verwendeten Frequenzbandes, die die Leistung dieser Verbindung beeinträchtigt

[QUELLE: ETSI TS 103 246-3]

3.1.2

Störsendung

vorsätzliche Übertragung einer Störgröße mit dem Ziel der Störung der Verarbeitung von Nutzsignalen (die in diesem Fall GNSS-Signale oder Telekommunikationssignale sind)

Anmerkung 1 zum Begriff: Die Störsendung ist ein besonderer Fall der elektromagnetischen Störung.

[QUELLE: ETSI TS 103 246-3]

3.1.3

Spoof/Spoofing

Übertragung von Signalen mit dem Ziel der Verarbeitung von vorgetäuschten Ortsdaten für die Meldung falscher Zieldaten für den Ort

[QUELLE: ETSI TS 103 246-3]

3.1.4

Bedrohung

mögliche Ursache eines unerwünschten Vorfalls, der einem System oder einer Organisation einen Schaden zufügen kann

[QUELLE: ISO/IEC 27001]

3.1.5

Sicherheitslücke

Schwäche eines Wertes oder einer Maßnahme, die durch eine oder mehrere Bedrohungen ausgenutzt werden kann

[QUELLE: ISO/IEC 27001]

3.1.6

GBPT, en: GNSS based positioning terminal

GNSS-basiertes Ortungsendgerät

Benennung der Komponente, die im Wesentlichen PVT ausgibt

3.1.7

DUT, en: device under test

Prüfling

Benennung eines Geräts, das gegenwärtig überprüft wird

Anmerkung 1 zum Begriff: Im Kontext von EN 16803-2 ist DUT gleichbedeutend mit GPBT.

3.1.8

Prüfszenario

setzt sich aus GNSS-SIS-Daten und gegebenenfalls in Einsatzprüfungen erhobenen Sensordaten zusammen, ergänzt um eine Metadatenbeschreibungsdatei; ein Prüfszenario ist eine nicht leere Kombination von UTS, die es ermöglicht, ein GBPT in den gewünschten Umgebungen zu überprüfen

Anmerkung 1 zum Begriff: Daten innerhalb eines Prüfzenarios sind Rohdaten, entweder HF-Signale von GNSS-Satelliten oder Rohdaten von anderen eingebetteten Sensoren.

Anmerkung 2 zum Begriff: Bei einem Prüfzenario handelt es sich um das gesamte Paket, das einem universell aufgestellten HF-Prüflaboratorium, das für die Prüfungen zur Leistungsüberprüfung nach der Normenreihe EN 16803 zuständig ist, von einem auf GNSS spezialisierten Prüflaboratorium zur Verfügung gestellt wird.

Anmerkung 3 zum Begriff: Betrachtet man die 6 (sechs) verschiedenen in EN 16803-1 festgelegten Umgebungen, so ergibt sich eine Kombination von $2^6 - 1 = 63$ möglichen Prüfzenarien, die z.B. von einem „rein ländlichen“ Prüfzenario bis zu einem Prüfzenario „sämtliche Umgebungen“, das die 6 (sechs) verschiedenen Umgebungen abdeckt, reichen.

3.1.9

unitäres Prüfzenario

UTS, en: unitary test scenario

elementarer Baustein eines Prüfzenarios, der sich aus einer bestimmten Einsatzprüfung ergibt; mit anderen Worten: Ein Prüfzenario stellt eine Verknüpfung verschiedener unitärer Prüfzenarien dar

3.1.10

einheitlicher Umgebungsdatensatz

UEDS, en: uniform environment data set

Ausgaben des DUT, die nach einer Wiedergabe im Labor erfasst und nach Umgebungen sortiert wurden; er ist eine Verknüpfung der Ausgaben des DUT für alle auf eine eindeutige Umgebung beschränkten UTS

Anmerkung 1 zum Begriff: Betrachtet man die 6 unterschiedlichen in EN 16803-1 definierten Umgebungen, so ergibt sich dieselbe Anzahl von UEDS, d. h. 6 (sechs).

Anmerkung 2 zum Begriff: Bei den Daten, aus denen sich ein einheitlicher Umgebungsdatensatz zusammensetzt, handelt es sich um PVT-Daten, wie sie von einem GBPT ausgegeben werden.

Anmerkung 3 zum Begriff: Einheitliche Umgebungsdatensätze sind die Datensätze, auf die die Metriken angewendet werden müssen, um die Leistungsdaten des Prüflings zu überprüfen.

3.1.11

auf GNSS spezialisiertes Prüflaboratorium

Laboratorium, das für die Erstellung von Prüfzenarien für universell aufgestellte HF-Prüflaboratorien zuständig ist

3.1.12

universell aufgestelltes HF-Prüflaboratorium

Laboratorium, das für die Überprüfung der Leistungsdaten von GBPT mit Hilfe eines Prüfzenarios zuständig ist

3.1.13

unitäres Bezugsgrößen-Prüfzenario (B-UTS)

dediziertes UTS, das speziell für das Validierungsverfahren herangezogen wird, wie in Abschnitt 7 festgelegt

3.1.14

einheitlicher Bezugsgrößen-Umgebungsdatensatz (B-UEDS)

jeder der mit dem Bezugsgrößenempfänger von dem auf GNSS spezialisierten Labor erhaltenen UEDS (der vom universell aufgestellten Labor zur Validierung seiner Prüfplattform und seiner Prüfverfahren genutzt wird)

3.2 Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Abkürzungen.

Abkürzung	Beschreibung
ACAI	Verfügbarkeit, Stetigkeit, Genauigkeit, Integrität (en: availability, continuity, accuracy, integrity)
ADC	Analog-Digital-Wandler (en: analog to digital converter)
ADS	angegriffener Datensatz (en: attacked data set)
AGC	automatische Verstärkungsregelung (en: automatic gain control)
CEN	Europäisches Komitee für Normung (en: European Committee for Standardization)
CENELEC	Europäisches Komitee für elektrotechnische Normung (en: European Committee for Electrotechnical Standardization)
CSAC	Atomuhr auf Chipbasis (en: chip scale atomic clock)
CW	Dauerstrich (en: continuous waves)
DAC	Digital-Analog-Wandler (en: digital to analog converter)
DUT	Prüfling (en: device under test)
ETSI	Europäisches Institut für Telekommunikationsnormen (en: European Telecommunications Standards Institute)
GBPT	GNSS-basiertes Ortungsendgerät (en: GNSS based positioning terminal)
GNSS	globale Navigationssatellitensysteme (en: global navigation satellite systems)
I/Q	In-Phase-&-Quadrature – das I/Q-Format ist eine effiziente Art der Speicherung von HF-Signalen, die es ermöglicht, HF-Signale im Labor nach der Modulation zu reproduzieren. Das I/Q-Format ist das zur Speicherung von GNSS-UTS verwendete Format.
IMU	inertiale Messeinheit (en: inertial measurement unit)
ITS	intelligente Transportsysteme (en: intelligent transport systems)
J/S	Störung-Signal-Verhältnis (en: jamming to signal ratio)
LNA	rauscharmer Verstärker (en: low noise amplifier)
Lab-A	auf GNSS spezialisiertes Prüflaboratorium (en: GNSS-specialized test laboratory)
Lab-B	universell aufgestelltes HF-Prüflaboratorium (en: generalist RF test laboratory)
MIR	Rate der irreführenden Informationen (en: misleading information rate)
NDS	nomineller Datensatz (en: nominal data set)
OCXO	beheizter Quarzoszillator (en: oven-controlled crystal oscillator)
PA	Leistungsverstärker (en: power amplifier)
PPS	Impulse je Sekunde (en: pulse per second)
PVT	Position, Geschwindigkeit und Zeit (en: position, velocity and time)
RAIM	empfängereigene Integritätsüberwachung (en: receiver autonomous integrity monitoring)
HF	Hochfrequenz (en: radio frequency [RF])
RFCS	Hochfrequenz-Konstellationssimulator (en: radio frequency constellation simulator)

Abkürzung	Beschreibung
RMS	Effektivwert (en: root mean square)
R&R	Aufzeichnung und Wiedergabe (en: Record and Replay)
SBAS	satellitengestütztes Erweiterungssystem (en: satellite based augmentation system)
SDR	softwaredefinierter Funk (en: software defined radio)
SIS	Signal-In-Space (de: Signal im Raum)
SNR	Signal-Rausch-Verhältnis (en: signal to noise ratio)
TCXO	temperaturstabilisierter Quarzoszillator (en: temperature-controlled crystal oscillator)
TIR	angestrebtes Integritätsrisiko (en: target integrity risk)
TTFF	Time To First Fix (Zeit für die erste Ortungsbestimmung)
UTS	unitäres Prüfzenario (en: unitary test scenario)
UEDS	einheitlicher Umgebungsdatensatz (en: uniform environment data set)

4 Beschreibung der allgemeinen Logik der Sicherheitsprüfungen

4.1 Prinzip von Aufzeichnung und Wiedergabe

Sicherheitsprüfungen nach EN 16803-3 beruhen auf der gleichen Methodik wie die in EN 16803-2 beschriebenen Prüfungen, die für die Überprüfung der grundlegenden Leistungsmerkmale Verfügbarkeit, Stetigkeit, Genauigkeit und Integrität (ACAI) und Time To First Fix (TTFF) der PVT-Information vorgesehen sind.

Diese Methodik wird als Aufzeichnung & Wiedergabe (R&R) bezeichnet. Die Gründe für diese Wahl und die Vorteile dieser Methodik werden in EN 16803-2:2020, 4.1.1 und 4.1.2, im Einzelnen erläutert.

Es gibt verschiedene Ansätze für die Prüfung. Leistungsfähige und weithin anerkannte Prüfverfahren müssen:

- repräsentativ;
- wiederholbar;
- schnell;
- finanziell tragbar sein.

Der R&R-Ansatz besteht in der Wiedergabe in einer Laborumgebung von GNSS-SIS-Daten und gegebenenfalls zusätzlichen Sensordaten oder Unterstützungs-/Korrekturdaten, die mit Hilfe eines speziellen Testfahrzeugs unter bestimmten Betriebsbedingungen aufgezeichnet wurden. Der die GNSS-SIS-Daten und gegebenenfalls Sensordaten oder Unterstützungs-/Korrekturdaten aus diesen Einsatzprüfungen enthaltende Datensatz wird in Verbindung mit der entsprechenden Metadatenbeschreibungsdatei als „**Prüfszenario**“ bezeichnet.

Dieser Ansatz ist:

- **repräsentativ** für die tatsächlichen Gegebenheiten, wenn die richtige Menge von Szenarien bestimmt wird. Der repräsentative Charakter ist mit Sicherheit größer als eine vollständig simulierte Umgebung.

- **wiederholbar:** Es ist sehr einfach, selbst komplexe Szenarien mit einem Prüfstand geringer Komplexität wiederzugeben. Abgesehen von thermischem Rauschen gibt es sehr wenige veränderliche Variablen. Die Freiheitsgrade des Prüfstandes sind gegenüber der Einsatzprüfung erheblich geringer bei einer verbesserten Wiederholpräzision.
- **schnell:** Sobald die Datensätze des Szenarios erhalten werden, ist die Einrichtung des Prüfstandes „trivial“ oder weist zumindest eine Komplexität auf, die von einem Prüfenieur, der kein GNSS-Fachmann ist, bewältigt werden kann.
- **finanziell tragbar:** da die Wiedergabeeinrichtung sehr viel kostengünstiger ist als voll ausgerüstete GNSS-Simulatoren. Außerdem sind entwicklungsbegleitende (en: pre-compliance) Messungen in Laboren durch Unternehmen mit akzeptablen Kosten möglich, wenn Einstiegsmodelle der Einrichtungen verwendet werden.

Was nominelle Szenarien betrifft, schlägt EN 16803-2 eine optimierte Mischung vor aus:

- Anwendungsfällen (Fahrtyp);
- Straßentopologien;
- GNSS-Umgebungen nach (EN 16803-1).

Da die R&R-Methodik nicht auf eine einzelne Konstellation oder auf eine einzelne Frequenz beschränkt ist, sind Sicherheitsprüfungen auch so zu verstehen, dass sie Ortungssysteme mit mehreren Konstellationen und mehreren Frequenzen abdecken.

4.2 Beschreibung von Sicherheitsprüfungen, die auf dem R&R-Ansatz beruhen

Der Unterschied zwischen den beiden Kategorien von Bewertungsprüfungen (Standardprüfungen und Sicherheitsprüfungen) ist folgender:

- in EN 16803-2 wird davon ausgegangen, dass die im Szenario aufgezeichneten SIS-Datendateien frei von Störbeeinflussungen und Angriffen durch Störsendung/Spoofing/Meaconing sind;
- in EN 16803-3 werden für die Wiedergabephase im Labor (Lab-B) zu den SIS-Datendateien spezifische Stör-, Spoofing- oder Meaconing-Signale hinzugefügt.

Unter Berücksichtigung der Unterschiede zwischen den beiden Angriffskategorien (Störsendung gegenüber Spoofing/Meaconing) müssen 2 (zwei) verschiedene Ansätze für das Hinzufügen der Störsignale angewendet werden, die zu 2 (zwei) verschiedenen Prüfarchitekturen führen. Diese Architekturen sind in den nächsten beiden Abschnitten beschrieben.

4.3 Prüfarchitektur für Störsendungen

Es gibt vorzugsweise 2 (zwei) mögliche Architekturen für die Prüfung mit Störsendungen:

- getrennte Aufzeichnung von SIS- und Störsendungssignal;
- gemeinsame Aufzeichnung von SIS- und Störsendungssignal.

Der erste Ansatz erlaubt es dem Prüfer, die Störsendung während der Durchlaufzeit hinzuzufügen und die Szenarien einfach zu kombinieren, so kann die Störsendung für alle nominellen Aufzeichnungen angewendet werden. Die zweite Art der Architektur sieht dagegen einen einfacheren Wiedergabeaufbau vor, weil er einen einzigen Signalstrom enthält, der wiederzugeben ist.

Unter der Voraussetzung einer höheren Flexibilität und Wiederverwendbarkeit der Signalproben ist die erste Option zu bevorzugen. Das getrennte Aufzeichnungsverfahren ist anwendbar, weil keine Synchronisation mit dem SIS notwendig ist. Die Störsendung ist eine generische Signalstörung, die keine besondere Genauigkeit erfordert, anders als Spoofing, welches genau mit dem SIS synchronisiert sein muss. Der größte Vorteil ergibt sich durch die Anwendbarkeit der aufgezeichneten Störsendungssignale auf alle nominellen Szenarien zur Leistungsüberprüfung in allen Umgebungen.

Bei diesem Prüfansatz können die Störsignalproben auf zwei verschiedene Arten erzeugt werden:

- Aufzeichnung eines echten Störsendungssignals;
- Signalgenerator für eine softwaredefinierte Funkstörung (SDR).

Die Option der echten Störsendung sieht eine Aufzeichnung mit einem echten Störsender vor. Dafür gibt es auf dem Markt viele Angebote wie Geräte zum Schutz der Privatsphäre (PPDs, en: privacy protection devices). Weitere Lösungen sind in [18] beschrieben. Diese Option ermöglicht das Erzeugen eines realistischen Störsendungssignals und bietet eine flexible Prüfung, weil die Störung getrennt vom SIS aufgezeichnet wird. Die Option der SDR-Erzeugung bietet dem Anwender jedoch noch mehr Flexibilität und Möglichkeiten. Vor allem kann mit einem softwaredefinierten Ansatz eine breite Auswahl von Signalen erzeugt werden, ohne für jeden bestimmten Typ der Störsendung eine spezifische Einrichtung anzuschaffen. Die SDR-Störungserzeugung würde die Kosten für die Bereitstellung der Signalproben erheblich senken und die Signalqualität verbessern, weil weniger Aufzeichnungsschritte vorgesehen sind, was das Gesamtrauschen vermindert. Eine SDR ermöglicht die Erzeugung von Störsendungssignalen, die über handelsübliche Dauerstrich- und Chirp-Sender hinausgehen, wie:

- nichtlinearer Chirp (d. h. Sinus-Frequenzmodulation);
- langsamer und schneller Frequenzwechsel (en: slow and fast frequency hopping);
- RADAR-ähnliche Störsendungssignale.

Angesichts dieser Betrachtungen ist die SDR-Option die vielversprechendste Prüfarchitektur und damit die diejenige, die in der vorliegenden Norm empfohlen wird. Dabei muss hervorgehoben werden, dass SDR-Störgeneratoren digitale Signalproben direkt erzeugen können, ohne dass Aufzeichnungsgeräte benötigt werden, und damit der hauptsächlich durch Aufzeichnungsgeräte entstehende Rauschbeitrag verringert wird.

Bild 2 zeigt die Architektur der Aufzeichnung der Störsendung und Bild 3 die übergeordnete Architektur des Störsendungs-Prüfstandes für die Wiedergabephase.

Das Störsendungssignal wird vom für die Prüfung verantwortlichen Lab-B zum rekonstruierten SIS hinzugefügt.

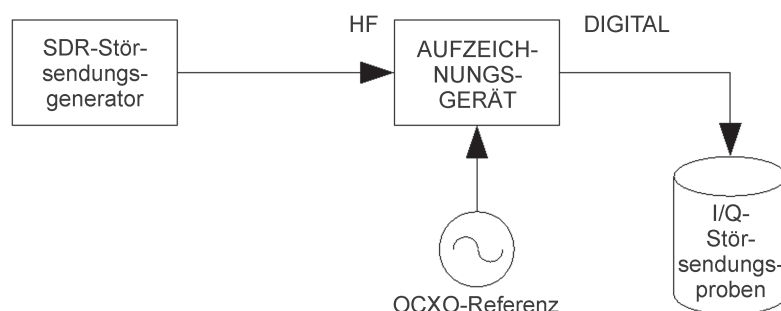


Bild 2 — Architektur der Aufzeichnung der Störsendung mit SDR-Störgenerator

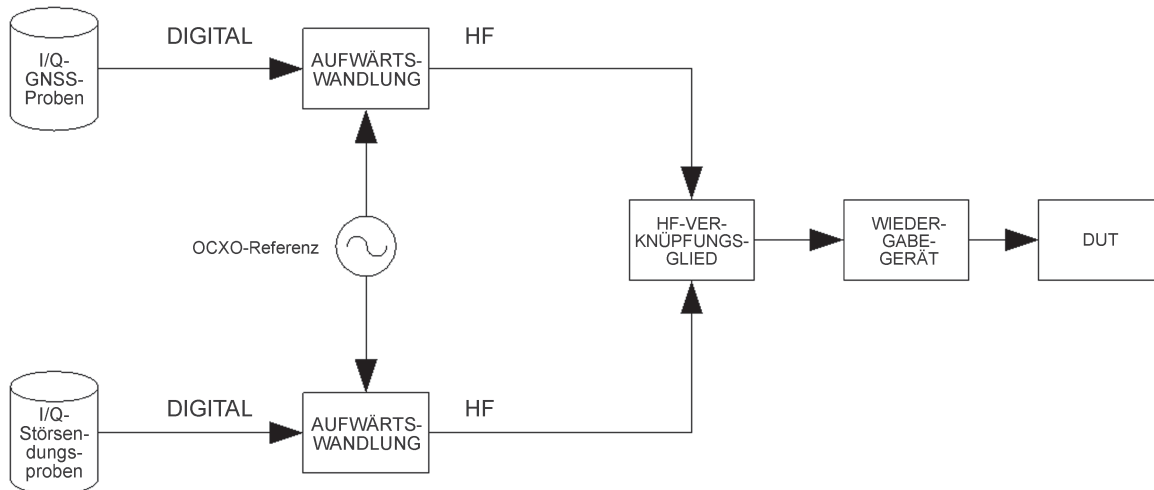


Bild 3 — Übergeordnete Architektur der Prüfung mit Störsendung

Die HF-Verbindungen müssen Dämpfungsglieder enthalten, um die Ausgangsleistung auf Pegel einzustellen, die dem GNSS-Standard entsprechen. Darüber hinaus muss dem Nutzer die Ausgangsleistung des HF-Signalgenerators bekannt sein, damit realistische Prüfungen durchgeführt werden können.

4.4 Prüfarchitektur zur Prüfung von Spoofing/Meaconing

Die Aufzeichnung des Spoofing-Szenarios erfordert im Gegensatz zur Störsendung die Beachtung der Synchronisation mit dem SIS. Aus diesem Grund wird die für das Störsendungsszenario angegebene Aufzeichnungsoption nicht mehr bevorzugt angewendet. Damit Spoofing-Signale wirksam werden, erfordern sie eine gute Synchronisation, sodass die Aufzeichnung in einer einzigen Datei der Signalprobe zusammen mit dem GNSS-Referenzsignal realisiert werden muss.

Bei diesem Aufbau können zwei Wege verfolgt werden:

- Ausrüstung des Aufzeichnungsfahrzeugs mit einem Hochfrequenz-Signalsimulator (RFCS), der unter Anwendung der empfangenen Ephemeriden, Observablen und Impulse je Sekunde (PPS) von einem mit dem SIS gleichlaufenden Empfänger ein Spoofing-Signal erzeugt, das mit dem echten SIS vor dem Front-End kombiniert wird;
- Erzeugung eines kombinierten Signals (SIS + Spoofing) mit einem RFCS und Aufzeichnung der Ausgabegröße.

Bild 4 zeigt ein übergeordnetes Schema des ersten Ansatzes, während Bild 5 den zweiten Aufbau beschreibt.

Bei beiden Ansätzen wird von dem auf GNSS spezialisierten Labor (Lab-A), das für die Erzeugung der Prüfscenarien verantwortlich ist, das Spoofing-Signal zum SIS (echt oder simuliert) vor der Digitalisierungs- und Wiedergabephase hinzugefügt und das für die Prüfung des DUT verantwortliche universell aufgestellte Labor (Lab-B) muss das aufgezeichnete Szenario nur wiedergeben, ohne einen RFCS zu verwenden.

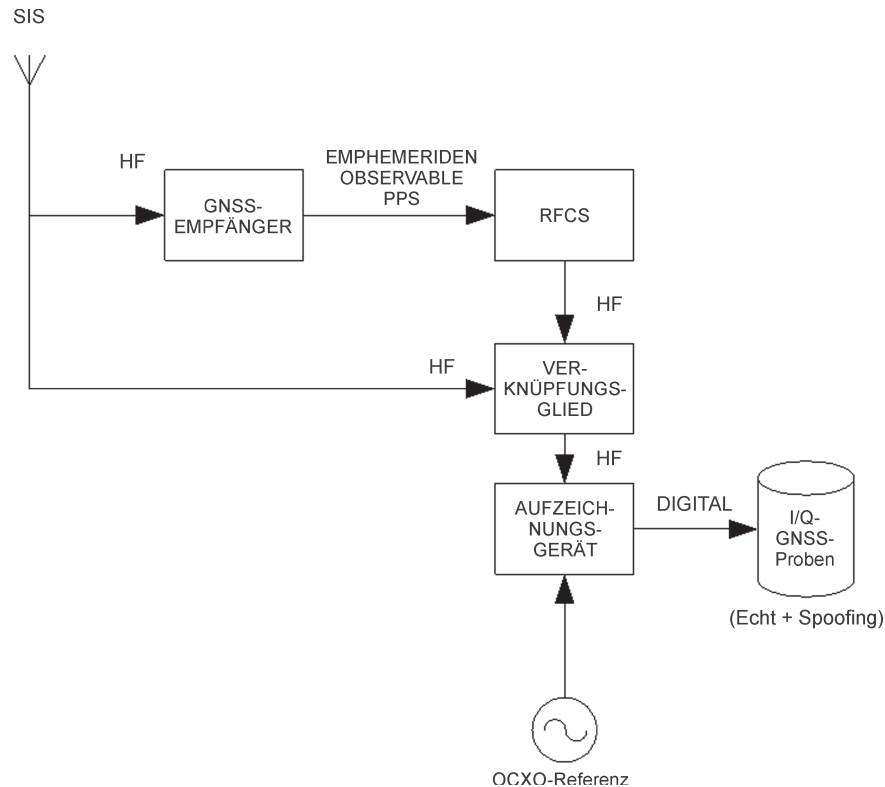


Bild 4 — Architektur der Spoofing-Aufzeichnung zur Durchführung von Live-Spoofing

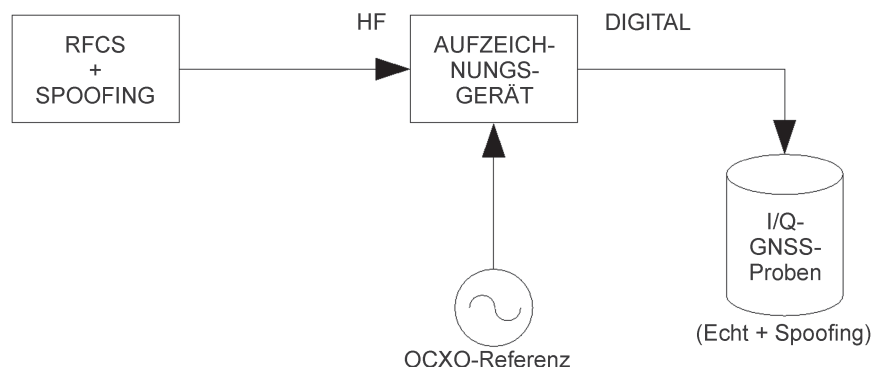


Bild 5 — Architektur der Spoofing-Aufzeichnung mit RFCS

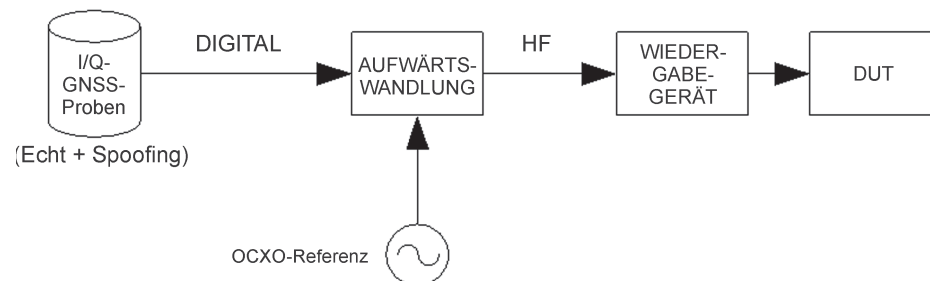


Bild 6 — Übergeordnete Architektur der Spoofing-Prüfung

Obwohl der erste Ansatz praxisnäher wäre, erscheint der zweite sehr viel unkomplizierter und geradliniger. Die Durchführung des Spoofing am Live-Signal mit Mehrwegausbreitung und einigen weiteren Beeinträchtigungen kann sehr kompliziert sein. Darüber hinaus trennt der zweite Ansatz die Leistungsfähigkeit des DUT, welcher dem Spoofing ausgesetzt ist, von den Beeinträchtigungen durch die Umwelt ab.

Aus diesen Gründen wird der in Bild 5 dargestellte zweite Ansatz bevorzugt und in dieser EN 16803-3 empfohlen.

5 Definition der Metriken bezogen auf die Sicherheitsleistungsdaten

5.1 Allgemeines

Die allgemeine Strategie für die Messung der GBPT-Leistungsdaten im Hinblick auf die Sicherheit besteht in der Bestimmung, wie sich die in EN 16803-1 festgelegten grundlegenden Leistungsmetriken verschlechtern, wenn das GBPT Sicherheitsangriffen ausgesetzt ist. In den folgenden Abschnitten wird beschrieben, wie diese Leistungsminderung zu messen ist, und es wird davon ausgegangen, dass die grundlegenden Leistungsmetriken aus zwei Datensätzen ermittelt wurden, von denen einer (nachfolgend als der nominelle Datensatz oder NDS bezeichnet) frei von Sicherheitsangriffen ist, während der andere (nachfolgend als der angegriffene Datensatz oder ADS bezeichnet) das Ergebnis der Überlagerung eines Angriffssignals mit dem ersteren ist. Die mathematische Formulierung und die allgemeinen Verfahren für die Ermittlung der grundlegenden Leistungsmetriken für den NDS sowie den ADS sind in EN 16803-2 angegeben.

5.2 Genauigkeitsmetriken

Mit X als PVT-Ausgabegröße (z. B. die horizontale Position), deren Genauigkeitsleistung zu messen ist, sei X_G die Menge der gültigen GBPT-Ausgabewerte von X für den NDS und X'_G sei die Menge der gültigen GBPT-Ausgabewerte von X für den ADS. T_G sei die Menge der Zeitmarken von X_G und T'_G sei die Menge der Zeitmarken von X'_G . Abgesehen von der Rundung sollten alle Zeitmarken in T'_G auch in T_G vorhanden sein (infolge des Angriffs sollte sich die Verfügbarkeit der GBPT-Ausgabegrößen nicht erhöhen). Ist das nicht der Fall, wird die Situation als anormal angesehen und muss untersucht und entweder korrigiert oder angemessen begründet werden.

$T_C = T'_G \cap T_G$ sei die Menge der allgemeinen Zeitmarken von X'_G und X_G (abgesehen von der Rundung, falls erforderlich, da sich die Zeitmarken für dieselbe Epoche von einer Menge zur anderen leicht unterscheiden dürfen). Wenn T_C eine leere Menge ist, kann die Minderung der Genauigkeit von X für die gegebenen Datensätze nicht gemessen werden. Ansonsten wird das Verfahren wie folgt fortgesetzt.

X_C und X'_C seien die Mengen der GBPT-Ausgabewerte von X für den NDS bzw. den ADS bei den Zeitmarken in T_C (d. h., es werden in jedem Datensatz nur Ausgabewerte von X betrachtet, für die im anderen Datensatz eine Entsprechung vorhanden ist).

δ_{50} , δ_{75} und δ_{95} bezeichnen das 50., 75. und 95. Fehler-Perzentil von X_C und δ'_{50} , δ'_{75} und δ'_{95} bezeichnen das 50., 75. und 95. Fehler-Perzentil von X'_C . Die Minderung der Genauigkeitsmetrik für X wird angegeben als das Triplet, das sich aus den 3 (drei) Minderungszahlen für das 50., 75. und 95. Fehler-Perzentil zusammensetzt, und zwar:

$$AccDeg_X = \left(100 \cdot \frac{\delta'_{50} - \delta_{50}}{\delta_{50}}, 100 \cdot \frac{\delta'_{75} - \delta_{75}}{\delta_{75}}, 100 \cdot \frac{\delta'_{95} - \delta_{95}}{\delta_{95}} \right)$$

Diese Definition erfordert, dass alle 3 (drei) nominellen Fehler-Perzentile δ_{50} , δ_{75} und δ_{95} verschieden von Null sind (und damit der Auslegung nach positiv, wie es EN 16803-2 entnommen werden kann). Dabei ist außerdem zu beachten, dass die Minderungswerte, die als Prozentsätze des Leistungsverlustes bezogen auf die Nennleistung angegeben werden, grundsätzlich alle positiv sein sollten, da jeder δ' -Wert schlechter sein sollte (also größer, da es sich um einen Fehlerwert handelt) als seine δ -Entsprechung. Es kann jedoch nicht