

DIN EN 16803-3



ICS 03.220.20; 33.060.30; 35.240.60

Einsprüche bis 2019-04-15

Entwurf

**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

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;
Version allemande et anglaise prEN 16803-3:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-02-15 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs
besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nl@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Luft- und Raumfahrt (NL), 10772 Berlin, Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 119 Seiten

DIN-Normenausschuss Luft- und Raumfahrt (NL)

Nationales Vorwort

Dieses Dokument (prEN 16803-3:2019) 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).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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

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

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

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: CEN-Umfrage
Dokument-Sprache: D

STD Version 2.9o

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 Wiedergabepfandes	22
6.2.1 Kalibrieren des Wiedergabegeräts	22
6.2.2 Architektur des Wiedergabe-Pfandes	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 Ausbreitungskanals	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

Europäisches Vorwort

Dieses Dokument (prEN 16803-3:2019) wurde vom Technischen Komitee CEN-CENELEC/TC 5 „Raumfahrt“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

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

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.

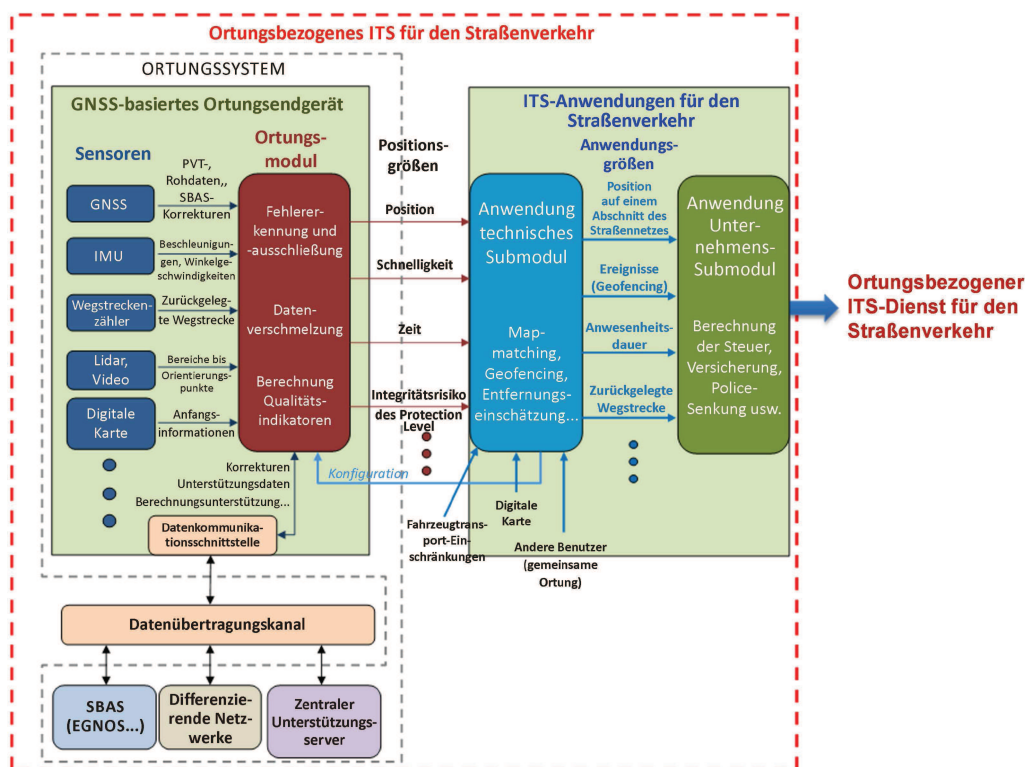


Bild 1 — Generische Funktionsarchitektur eines ortungsbasierten ITS für den Straßenverkehr

Diese Europäische Norm 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 End-zu-End-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.

Diese Norm 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 muss als ergänzende Norm zu EN 16803-2 angesehen werden, 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 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 dieser EN 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 eingehend in EN 16803-4 beschrieben (in Vorbereitung). 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*

prEN 16803-2:2018, *Raumfahrt — Anwendung von GNSS-basierter Ortung für Intelligente Transportsysteme (ITS) im Straßenverkehr — Teil 2: Bestimmung der grundlegenden Leistungen von GNSS-basierten Ortungsendgeräten*

3 Begriffe

3.1 Definitionen

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/>

Einschlägige Begriffe aus ETSI TS 103 246-3, ISO/IEC 27001 und der ISO Online Browsing Platform (<https://www.iso.org/obp/ui/#search>).

3.1.1

elektromagnetische Störung

jede 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

GNSS-basiertes Ortungsendgerät

GBPT

(en: GNSS based positioning terminal)

Benennung der Komponente, die im Wesentlichen PVT ausgibt

3.1.7

Prüfling

DUT

(en: device under test)

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

Szenario, welches sich aus GNSS-SIS-Daten und gegebenenfalls in Einsatzprüfungen erhobenen Sensordaten zusammensetzt, 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 Prüfszenarios sind Rohdaten, entweder HF-Signale von GNSS-Satelliten oder Rohdaten von anderen eingebetteten Sensoren.

Anmerkung 2 zum Begriff: Bei einem Prüfszenario 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 Prüfszenarien, die z. B. von einem „rein ländlichen“ Prüfszenario bis zu einem Prüfszenario „sämtliche Umgebungen“, das die 6 (sechs) verschiedenen Umgebungen abdeckt, reichen.

3.1.9

unitäres Prüfszenario

UTS

(en: unitary test scenario)

elementarer Baustein eines Prüfszenarios, der sich aus einer bestimmten Einsatzprüfung ergibt; mit anderen Worten: Ein Prüfszenario stellt eine Verknüpfung verschiedener unitärer Prüfszenarien 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; es 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

(en: GNSS-specialized test laboratory)

Laboratorium, das für die Erstellung von Prüfszenarien 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 Prüfszenarios zuständig ist

3.1.13

unitäres Bezugsgrößen-Prüfszenario

B-UTS

(en: benchmark unitary test scenario)

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

3.1.14

einheitlicher Bezugsgrößen-Umgebungsdatensatz

B-UEDS

(en: benchmark uniform environment data set)

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 (fr: <i>Comité Européen de Normalisation</i> , en: European Committee for Standardization)
CENELEC	<i>Europäisches Komitee für elektrotechnische Normung (fr: Comité Européen de Normalisation Électrotechnique,</i> 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
LNA	rauscharmer Verstärker (en: low noise amplifier)
Lab-A	auf GNSS spezialisiertes Prüflaboratorium (en: GNSS-specialized test laboratory)
Lab-B	universell aufgestelltes HF-Prüflaboratorium
MIR	Rate der irreführenden Informationen (en: misleading information rate)
NDS	nomineller Datensatz (en: nominal data set)

Abkürzung	Beschreibung
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)
RMS	Effektivwert (en: root mean square)
R&R	Aufzeichnung und Wiedergabe (en: Record & Replay)
SBAS	satellitengestütztes Erweiterungssystem (en: satellite based augmentation system)
SDR	softwaredefinierter Funk (en: software defined radio)
SIS	Signal-In-Space (Signal im Raum)
SNR	Signal-Rausch-Verhältnis (en: signal to noise ratio)
TCXO	temperaturstabilisierter Quarzoszillator (en: oven-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 Bewertung 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 prEN 16803-2:2018, 4.1.1 und 4.1.2, im Einzelnen erläutert.

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

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

Der R&R-Ansatz besteht in der Wiedergabe von GNSS-SIS-Daten und gegebenenfalls zusätzlichen Sensordaten oder Unterstützungs-/Korrekturdaten, die mit Hilfe eines speziellen Testfahrzeugs unter bestimmten Betriebsbedingungen aufgezeichnet wurden, in einer Laborumgebung. 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).

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 zwei verschiedene Ansätze für das Hinzufügen der Störsignale angewendet werden, die zu zwei verschiedenen Prüfarchitekturen führen. Diese Architekturen sind in den nächsten beiden Abschnitten beschrieben.

4.3 Prüfarchitektur für Störsendungen

Es gibt vorzugsweise 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 wiedergegeben 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 (en: privacy protection devices, PPDs). 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 diejenige, die in der vorliegenden Norm empfohlen wird. Dabei muss hervorgehoben werden, dass SDR-Störgeräten 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.

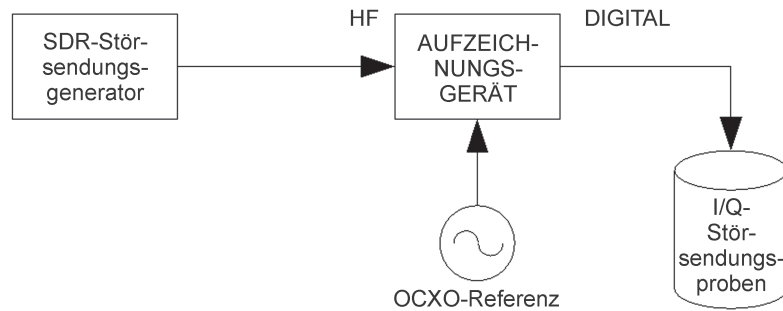


Bild 2 — Architektur der Aufzeichnung der Störsendung mit SDR-Störgenerator

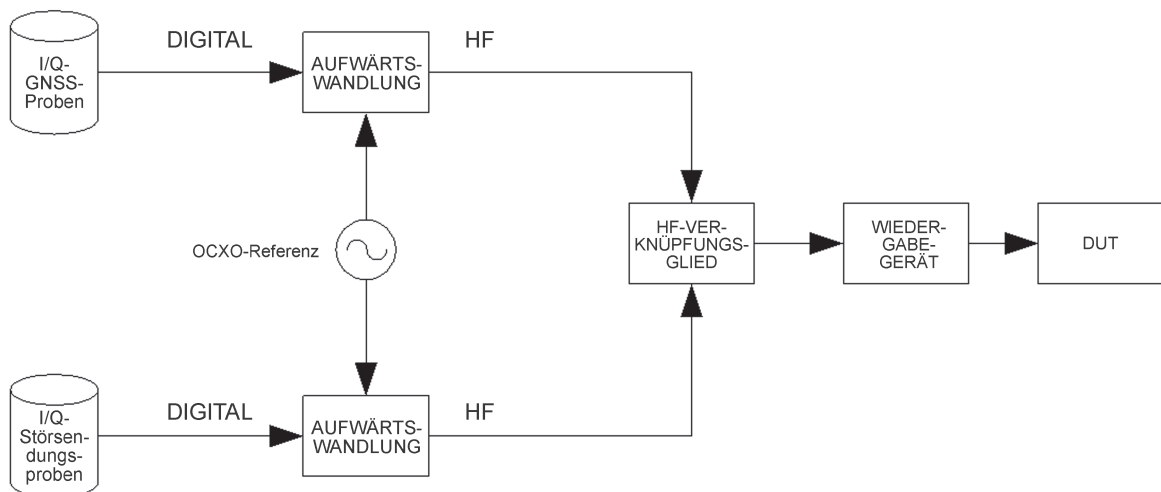


Bild 3 — Übergeordnete Architektur der Prüfung mit Störsendung

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 Prüf-szenarien 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.

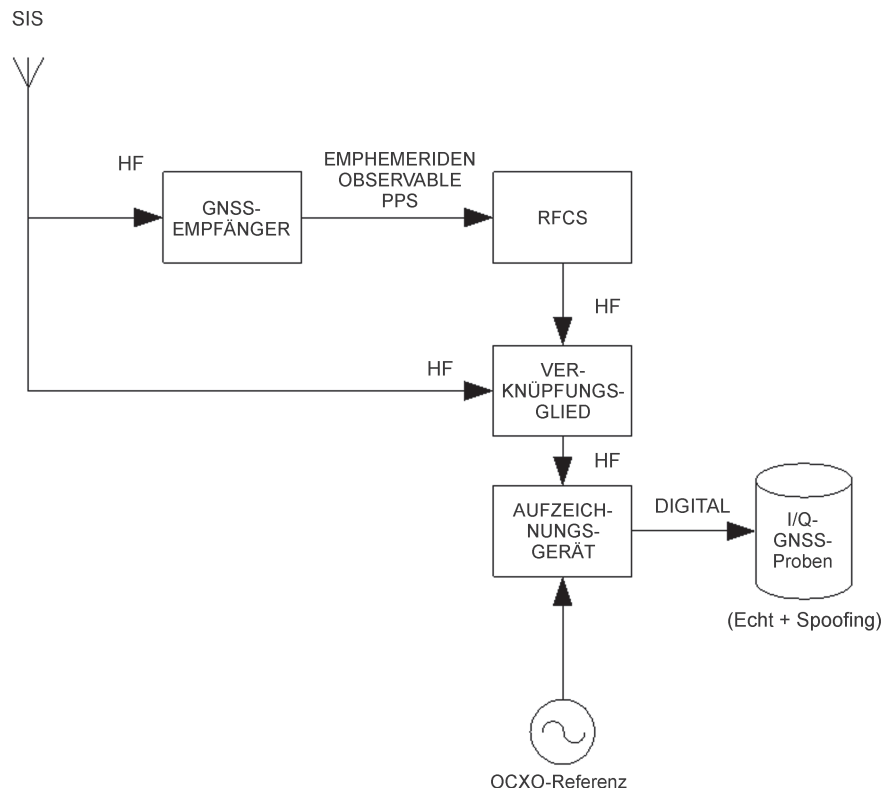


Bild 4 — Architektur der Spoofing-Aufzeichnung zur Durchführung von Live-Spoofing

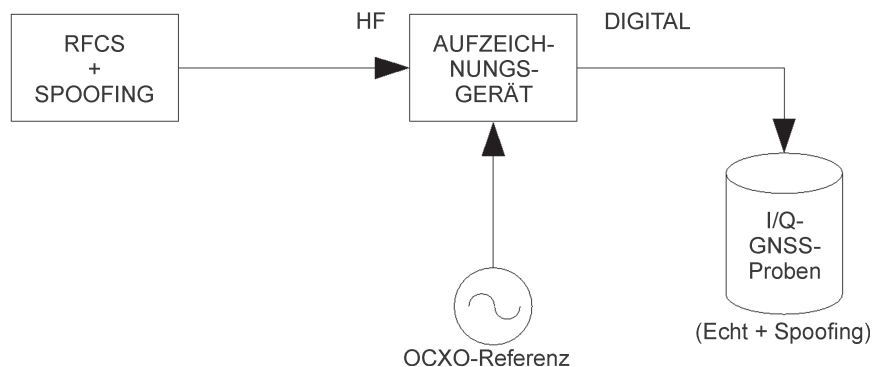


Bild 5 — Architektur der Spoofing-Aufzeichnung mit RFCS

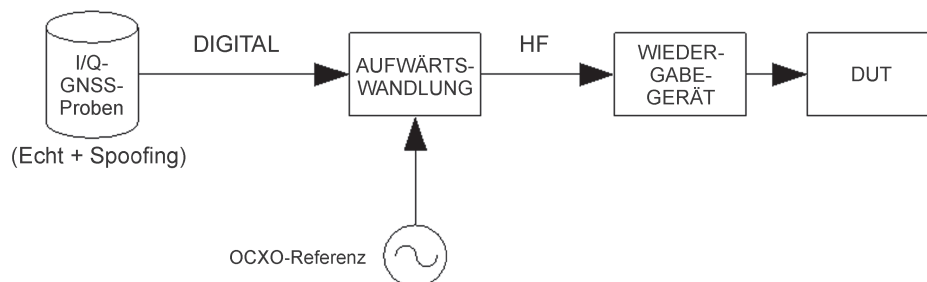


Bild 6 — Übergeordnete Architektur der Spoofing-Prüfung

Obwohl der erste Ansatz praxisnäher ist, 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 16603-3 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 ersten 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 des 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 Triplett, das sich aus den drei Minderungszahlen für das 50., 75. und 95. Fehler-Perzentil zusammensetzt, und zwar:

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

ANMERKUNG Diese Definition erfordert, dass alle drei nominellen Fehler-Perzentile δ_{50} , δ_{75} und δ_{95} anders als Null sind (und damit der Auslegung nach positiv, wie es EN 16803-2 entnommen werden kann). Dabei ist außerdem zu beachten, dass die Zahlen der Genauigkeitsminderung, 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 ausgeschlossen werden,

dass einige δ' -Werte besser sind als ihre entsprechenden δ -Werte, was als anomales Verhalten anzusehen ist und untersucht und entweder korrigiert oder angemessen begründet werden muss.

Bild 7 veranschaulicht die Minderung der Genauigkeitsmetrik. Die blaue Kurve entspricht der nominellen Genauigkeitsleistung, die mit dem zu prüfenden GBPT unter Nennbedingungen (d. h. ohne Angriffe) zu erzielen ist. Die rote Kurve gibt die Leistungsdaten wieder, die mit dem gleichen GBPT erzielt werden, wenn ein Angriff stattfindet. Die Prozentsätze der Minderung, die bei den betreffenden Perzentilen erzielt werden, sind angegeben.

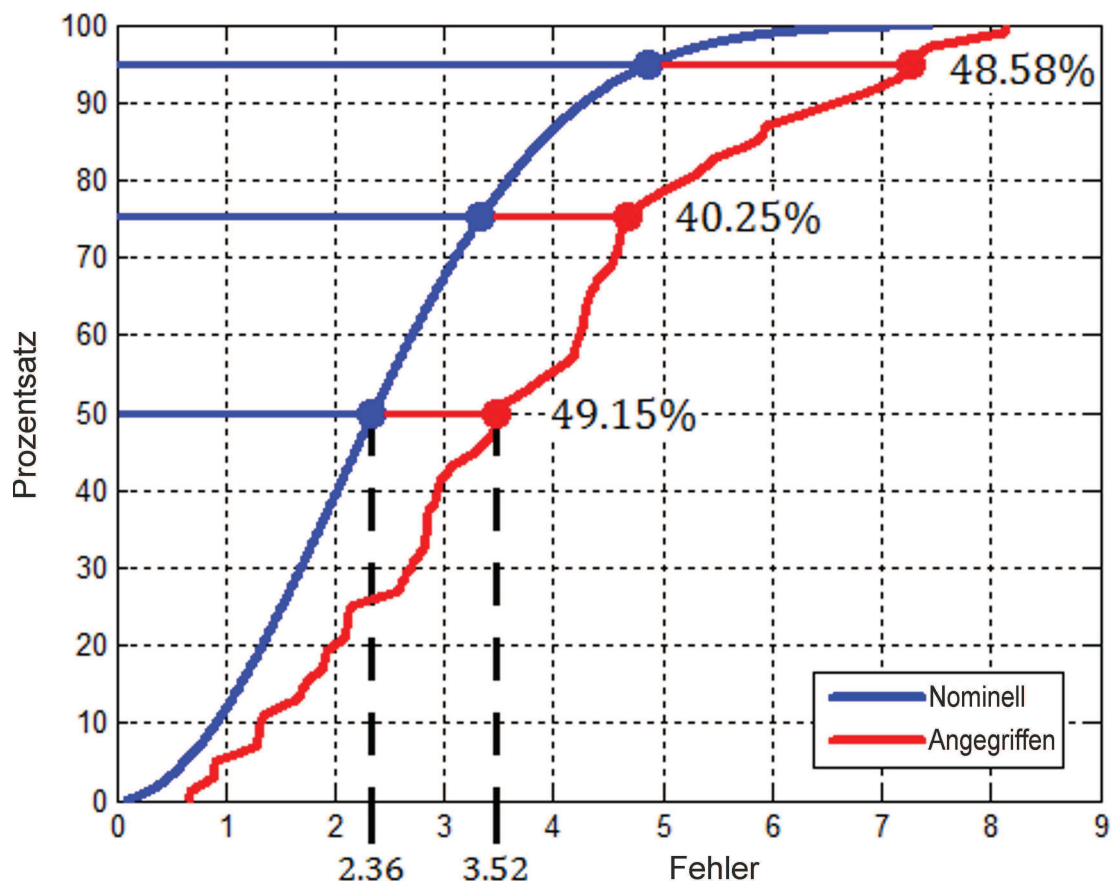


Bild 7 — Minderung der Genauigkeitsmetrik

5.3 Verfügbarkeits- und Stetigkeitsmetriken

X sei ein beliebiger interessierender Navigationsparameter (wie z. B. Position, Geschwindigkeit, Schnelligkeit, Bewegungsrichtung usw.). Angegeben als positive ganze Zahl T bezeichnen $A_X(T)$ und $C_X(T)$ die Zahlen für die Verfügbarkeit (T) bzw. die Stetigkeit (T) von X , die mit dem NDS erzielt werden und $A'_X(T)$ und $C'_X(T)$ bezeichnen die entsprechenden Werte, die mit dem ADS erzielt werden. Es wird daran erinnert, dass die genannten Zahlen in EN 16803-2 als Prozentsätze definiert sind.

Die Minderung der Verfügbarkeitsmetrik (T) für X wird als die folgende Differenz angegeben:

$$AvailDeg_X(T) = A_X(T) - A'_X(T)$$

Genauso wird die Minderung der Stetigkeitsmetrik (T) für X als die folgende Differenz angegeben:

$$ContDeg_X(T) = C_X(T) - C'_X(T)$$

ANMERKUNG Beide Werte $AvailDeg_X(T)$ und $ContDeg_X(T)$ müssen zwischen -100 und $+100$ liegen und es wird davon ausgegangen, dass sie beide positiv sind. Genau genommen kann nicht ausgeschlossen werden, dass einer der

beiden Werte negativ wird, diese Situation muss aber als anormal angesehen werden und untersucht und entweder korrigiert oder angemessen begründet werden.

5.4 Integritätsmetriken

5.4.1 Leistungsmetriken der Protection Levels

Mit X als PVT-Ausgabewert (z. B. die horizontale Position), deren zugehöriger Protection Level Y der Leistungsfähigkeit zu analysieren ist, sei X_G die Menge der gültigen GBPT-Ausgabewerte von X (was bedeutet, dass sie als gültig markiert sind und einen gültigen Protection Level besitzen) für den NDS und sei X'_G 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 Ausgangswerte von X betrachtet, für die im anderen Datensatz eine Entsprechung vorhanden ist). Y_C und Y'_C seien die entsprechenden Mengen von Protection Levels (verbunden mit den Navigationsausgabewerten X_C bzw. X'_C).

y_{50} , y_{75} und y_{95} bezeichnen das 50., 75. und 95. Perzentil von Y_C und y'_{50} , y'_{75} und y'_{95} bezeichnen das 50., 75. und 95. Perzentil von Y'_C . Die Minderung der Leistungsmetrik des Performance Levels für X wird angegeben als das Triplett, das sich aus den drei Minderungszahlen für das 50., 75. und 95. Perzentil zusammensetzt, und zwar:

$$PL_Deg_X = \left(100 \cdot \frac{y'_{50} - y_{50}}{y_{50}}, 100 \cdot \frac{y'_{75} - y_{75}}{y_{75}}, 100 \cdot \frac{y'_{95} - y_{95}}{y_{95}} \right)$$

ANMERKUNG Diese Definition erfordert, dass alle drei nominellen Perzentile y_{50} , y_{75} und y_{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 Zahlen der Leistungsminderung des Performance Levels, die als Prozentsätze des Leistungsverlustes bezogen auf die Nennleistung angegeben werden, grundsätzlich alle positiv sein sollten, da jeder y' -Wert schlechter sein sollte (also größer, da es sich um einen Fehlerwert handelt) als seine y -Entsprechung. Es kann jedoch nicht ausgeschlossen werden, dass einige y' -Werte besser sind als ihre entsprechenden y -Werte, was als anormales Verhalten anzusehen ist und untersucht und entweder korrigiert oder angemessen begründet werden muss.

5.4.2 Metrik der irreführenden Informationen

X sei ein Navigationsparameter (wie Position, Geschwindigkeit, Schnelligkeit, Bewegungsrichtung usw.), deren zugehöriges Integritätsrisiko zu messen ist. MIR_X und MIR'_X bezeichnen die Metrik der Rate der irreführenden Informationen (MIR) für X für den NDS bzw. den ADS. TIR_X sei das angestrebte Integritätsrisiko, d. h. das Integritätsrisiko, das nach den GBPT-Spezifikationen oder den dafür geltenden Anforderungen nicht zu überschreiten ist. Die Minderung der MIR-Metrik für X wird als das folgende Verhältnis angegeben:

$$MIR_Deg_X = \frac{MIR'_X - MIR_X}{TIR_X}$$

ANMERKUNG Es wird davon ausgegangen, dass MIR_Deg_X positiv ist, es kann jedoch nicht ausgeschlossen werden, dass die Größe negative Werte annimmt. Diese Situation muss jedoch als anormal angesehen werden und untersucht und entweder korrigiert oder angemessen begründet werden.

5.5 Zeitsteuerungsmetriken

5.5.1 Zeitstempelauflösung

Die Zeitstempelauflösung ist die numerische Auflösung der mit jeder GBPT-Ausgabe verbundenen Zeitmarke. Sie ist als die mindestens verstrichene Zeit definiert, die unterschiedliche aufeinander folgende Zeitstempel erzeugt, und kann als der Wert des jüngsten signifikanten Bits innerhalb des zur Kodierung des Zeitstempels im GBPT-Ausgabedatenstrom verwendeten Worts verstanden werden.

Die Zeitstempelauflösung wird als Bestandteil der Spezifikation der GBPT-Ausgabeschnittstelle bereitgestellt und benötigt, um den GBPT-Ausgabedatenstrom richtig zu entschlüsseln. Daher wird kein experimentelles Verfahren für die Bestimmung festgelegt, weder bei Nennbedingungen noch bei Sicherheitsangriffen.

5.5.2 Nominelle Ausgabelatenz

Die nominelle Ausgabelatenz ist die nominelle Zeitspanne zwischen dem Zeitstempel einer Ausgabe und der Zeit, zu dem diese bereitgestellt wird. Es handelt sich dabei um einen Wert, der als Bestandteil der Spezifikation der GBPT-Ausgabeschnittstelle bereitgestellt wird. Es wird kein experimentelles Verfahren für die Bestimmung festgelegt, weder bei Nennbedingungen noch bei Sicherheitsangriffen.

5.5.3 Nominelle Ausgabegeschwindigkeit

Die nominelle Ausgabegeschwindigkeit ist die nominelle Anzahl von Werten, die in einer Sekunde ausgegeben werden, oder der Kehrwert der zeitlichen Verzögerung zwischen aufeinander folgenden GBPT-Ausgaben. Es handelt sich dabei um einen Wert, der als Bestandteil der Spezifikation der GBPT-Ausgabeschnittstelle bereitgestellt wird. Es wird kein experimentelles Verfahren für die Bestimmung festgelegt, weder bei Nennbedingungen noch bei Sicherheitsangriffen. Für die Messung der Minderung der Ausgabegeschwindigkeit ist die zeitliche Verzögerung zwischen aufeinander folgenden Ausgaben zu messen, sodass das ein Zeitmaß erhalten wird und kein Frequenzmaß (oder Geschwindigkeitsmaß). Dieses Zeitmaß muss als *Ausgabeverzögerung* bezeichnet werden und sein Nennwert (Kehrwert der nominellen Ausgabegeschwindigkeit) muss als die *nominelle Ausgabeverzögerung* bezeichnet werden.

5.5.4 Stabilität der Ausgabelatenz

Anders als bei den Genauigkeitsmetriken und den Leistungsmetriken der Protection Levels, bei denen Vergleiche zwischen dem NDS und dem ADS nur in Epochen gezogen wurden, die beide Datensätze gemeinsam betreffen, wird bei der Stabilität der Ausgabelatenz von einer zufälligen Komponente ausgegangen, die die Beschränkung auf gemeinsame Epochen überflüssig macht. Deshalb werden die mit dem NDS und dem ADS erzielten Werte direkt und ohne vorherige Filterung oder Auswahl von Epochen verglichen.

δ_{50} , δ_{75} und δ_{95} bezeichnen das 50., 75. und 95. Perzentil der Stabilität der Ausgabelatenz, die nach den Festlegungen in EN 16803-2 für den NDS ermittelt werden, und δ'_{50} , δ'_{75} und δ'_{95} bezeichnen die entsprechenden Perzentile für den ADS. Die Minderung der Stabilität der Ausgabelatenz wird angegeben als das Triplet, das sich aus den drei Minderungszahlen für das 50., 75. und 95. Perzentil der Stabilität der Ausgabelatenz zusammensetzt, und zwar:

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

ANMERKUNG Diese Definition erfordert, dass alle drei Perzentile der Stabilität der Ausgabelatenz für den NDS δ_{50} , δ_{75} und δ_{95} anders als Null sind (und damit der Auslegung nach positiv, wie es EN 16803-2 entnommen werden kann).

Dabei ist außerdem zu beachten, dass die Minderungszahlen, 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 ausgeschlossen werden, dass einige δ' -Werte besser sind als ihre entsprechenden δ -Werte, was als anormales Verhalten anzusehen ist und untersucht und entweder korrigiert oder angemessen begründet werden muss.

5.5.5 Stabilität der Ausgabegeschwindigkeit

Wie bei der Stabilität der Ausgabelatenz wird davon ausgegangen, dass die Stabilität der Ausgabegeschwindigkeit Zufallseffekten unterliegt, die einen direkten Vergleich der mit dem NDS und dem ADS erzielten Werte ohne vorherige Filterung oder Auswahl von Epochen rechtfertigen.

δ_{50} , δ_{75} und δ_{95} bezeichnen das 50., 75. und 95. Perzentil der Stabilität der Ausgabegeschwindigkeit, die nach den Festlegungen in EN 16803-2 für das NDS ermittelt werden, und δ'_{50} , δ'_{75} und δ'_{95} bezeichnen die entsprechenden Perzentile für den ADS. Die Minderung der Stabilitätsmetrik der Ausgabegeschwindigkeit wird angegeben als das Triplet, das sich aus den drei Minderungszahlen für das 50., 75. und 95. Perzentil der Stabilität der Ausgabegeschwindigkeit zusammensetzt, und zwar:

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

ANMERKUNG Diese Definition erfordert, dass alle drei Perzentile der Stabilität der Ausgabegeschwindigkeit für den NDS δ_{50} , δ_{75} und δ_{95} anders als Null sind (und damit der Auslegung nach positiv, wie es EN 16803-2 entnommen werden kann). Dabei ist außerdem zu beachten, dass die Minderungszahlen, 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 ausgeschlossen werden, dass einige δ' -Werte besser sind als ihre entsprechenden δ -Werte, was als anormales Verhalten anzusehen ist und untersucht und entweder korrigiert oder angemessen begründet werden muss.

5.5.6 Time To First Fix

Die für die Bestimmung der TTFF verwendeten Datensätze dürfen für diesen Zweck speziell erstellt worden sein und sich von den für die anderen Metriken verwendeten Datensätzen unterscheiden, es wird aber hier davon ausgegangen, dass alle Datensätze (auch TTFF-spezifische) eine nominelle Entsprechung (NDS) und eine angegriffene Entsprechung (ADS) haben.

Die TTFF-Metriken werden berechnet als Stichprobenmittelwert und Standardabweichung von TTFF-Werten, die für eine Anzahl von GBPT-Anlaufversuchen unter verschiedenen Konfigurationen erhalten werden, bestimmt durch die Zeit, für die das GBPT vor dem Einschalten inaktiv war. Für jede der verschiedenen Inaktivitätsperioden wird ein Paar aus Mittelwert und Standardabweichung ermittelt (es müssen mindestens Inaktivitätsperioden von einer Minute, einem Tag und einer Woche betrachtet werden). Dieses Verfahren muss sowohl für den NDS als auch den ADS durchgeführt werden, sodass vergleichbare TTFF-Metriken (nach EN 16803-2) für jede einzelne der verschiedenen Inaktivitätsperioden erhalten werden.

$\hat{\mu}(T)$ und $s(T)$ seien der Mittelwert bzw. die Standardabweichung von TTFF, die mit dem NDS für eine bestimmte Inaktivitätsperiode T ermittelt werden, und $\hat{\mu}'(T)$ und $s'(T)$ sind die ADS-Entsprechungen. Die Minderung der TTFF-Metrik für eine Inaktivitätsperiode der Länge T wird mit dem folgenden Paar angegeben:

$$TTFF_Deg(T) = \left(100 \cdot \frac{\hat{\mu}'(T) - \hat{\mu}(T)}{\hat{\mu}(T)}, 100 \cdot \frac{s'(T) - s(T)}{s(T)} \right)$$

ANMERKUNG Diese Definition erfordert, dass sowohl $\hat{\mu}(T)$ als auch $s(T)$ 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 Nennwerte angegeben werden, grundsätzlich beide positiv sein sollten, da die ADS-TTFF-Werte schlechter sein sollten als die NDS-TTFF-Werte. Es kann

jedoch nicht ausgeschlossen werden, dass einige ADS-TTFF-Werte besser sind als ihre NDS-Entsprechungen, was als anomales Verhalten anzusehen ist und untersucht und entweder korrigiert oder angemessen begründet werden muss.

6 Beschreibung der Prüfverfahren und der Prüfeinrichtung

6.1 Anwendungsbereich

Wie bereits am Beginn von Abschnitt 5 eingeführt, müssen Bewertungsprüfungen für die Sicherheitsleistung durchgeführt werden durch:

- Wiedergabe des mit einem Angriffssignal speziell aufgezeichneten Datensatzes (nachfolgend als der angegriffene Datensatz oder ADS bezeichnet);
- Anwendung der betreffenden Metriken auf diesen ADS;
- Vergleich dieser Ergebnisse mit den Ergebnissen der gewählten Metriken, wenn diese auf den gleichen Datensatz ohne Angriffssignale (nachfolgend als der nominelle Datensatz oder NDS bezeichnet) angewendet werden, um die Leistungsminderung für die ausgewählten Metriken zu messen.

Der Wiedergabeprozess besteht in der HF-Übertragung der vorher aufgezeichneten Proben, um die Empfängerleistung zu überprüfen.

Der Aufzeichnungsprozess für die Störsendungs- und Spoofing-Prüfung wird in Anhang E kurz und in EN 16803-4 eingehend beschrieben.

Um die Wiederholpräzision des folgenden Wiedergabeverfahrens sicherzustellen, muss das Wiedergabegerät vor den Wiedergabeproofungen kalibriert werden. Ziel des Kalibrierverfahrens ist die Sicherstellung, dass das Wiedergabegerät einen vorgegebenen Leistungspegel für die HF-Übertragung abgibt.

Um diese Anforderung zu erfüllen, können verschiedene Ansätze mit verschiedenen Architekturen genutzt werden. Die folgenden Abschnitte 6.2.1 und 6.2.2 enthalten Informationsmaterial für diese Aspekte.

6.2 Aufstellung des Wiedergabeproofstandes

6.2.1 Kalibrieren des Wiedergabegeräts

Mit dem Kalibrieren des Wiedergabegeräts wird sichergestellt, dass die Ausgabewerte der HF-Übertragung einem vorgegebenen Leistungspegel entsprechen. Außerdem muss beachtet werden, dass der Leistungspegel eines wiedergegebenen Signals auch von den tatsächlichen Werten der aufgezeichneten I/Q-Proben abhängt. Deshalb ist ein Kalibrierverfahren erforderlich, weil das GNSS-Signal mit Nennleistung wiedergegeben werden muss, um die Wiederholpräzision des folgenden Wiedergabeverfahrens sicherzustellen. Wenn zwei getrennte HF-Signale überlagert werden müssen, wie es bei der Störsendung (siehe Bild 3) der Fall ist, ist darüber hinaus eine einwandfreie Kalibrierung für beide HF-Signale erforderlich, um das richtige und für die Prüfung erforderliche Störung-Signal-Verhältnis (J/S-Verhältnis) einzustellen.

Ein möglicher Weg der Umsetzung des Kalibrierprozesses sieht vor:

- die Beschreibung der GERÄTEVERSTÄRKUNG für die elektronischen Bauteile der Aufwärtswandlungskette;
- die Einstellung der richtigen ABSTIMMVERSTÄRKUNG zur Abbildung der digitalen Eingangsleistung auf genau eine angestrebte HF-Ausgangsleistung.

Um dieses Ziel zu erreichen, wird mit einem Leistungsmessgerät ein Kalibrierprofil definiert, das in einem Schema der Frequenz/Ausgangsleistung mit fester Beziehung besteht. Die empfohlene Signalprobe für die Kalibrierung kann ein einzelner Ton mit halber Amplitude bezogen auf den Vollbereich des Analog-Digital-Wandlers (ADC) sein, um Probleme bezüglich der Nichtlinearität durch Sättigung zu vermeiden. Für ein 16 Bit-Quantisierungsgerät beträgt der Vollbereich z. B. $2^{15}-1$ (0x7FFF) und der halbe Bereich 2^{14} (0x4000).

Es muss beachtet werden, dass ein Kalibrierverfahren, das auf die Übertragung einer bestimmten HF-Ausgangsleistung ausgerichtet ist, auf zwei verschiedenen Verstärkungsfaktoren beruhen kann, wie in Bild 7 dargestellt.

Die theoretische Leistung des digitalen Datenstroms kann berechnet werden als:

$$P_{D_{ref}} = \frac{\sum_{i=0}^N |s(i \cdot T)|^2}{N}$$

dabei ist N die Anzahl der Proben für die Gleichung, T ist die Abtastzeit und s ist das erzeugte Signal.

Dieses digitale Signal durchläuft während des Aufbereitungsprozesses des HF-Signals eine Anzahl analoger Komponenten wie Analog-Digital-Wandler, Mischer, Filter und Leistungsverstärker.

Der erste Verstärkungsbeitrag, und zwar die GERÄTEVERSTÄRKUNG, berücksichtigt die Differenz zwischen der Eingangsleistung des digitalen Kalibriersignals ($P_{D_{ref}}$) und der HF-Leistung ($P_{RF_{ref}}$), die am Ausgang des Aufwärtswandlers gemessen wird. Diese Verstärkung kann gewöhnlich in groben Schritten angepasst werden, da die Aufwärtswandlungskette einen einstellbaren Leistungsverstärker enthält. Dieser Verstärkungsbeitrag ist vom Gerät abhängig und kann nur über eine Messkampagne ermittelt werden.

Der zweite Beitrag, und zwar die ABSTIMMVERSTÄRKUNG, ist die Leistungsdifferenz zwischen der gewünschten HF-Leistung (P_{OUT}) und der gemessenen HF-Signalleistung des Kalibriersignals ($P_{RF_{ref}}$). Diese zweite Verstärkung wird gewöhnlich zur Feinabstimmung der Gesamtverstärkung der Erzeugungskette benutzt.

Die beiden Verstärkungsbeiträge werden addiert und das Ergebnis gibt den Verstärkungswert an, der für das HF-Gerät anzuwenden ist. In dem speziellen Fall, dass die endgültige Verstärkung positiv ist, muss für die Funkperipherie eine Verstärkung der Übertragung durchgeführt werden, ansonsten muss das Signal gedämpft werden. Bild 7 zeigt ein übergeordnetes Schema dieses Prozesses.

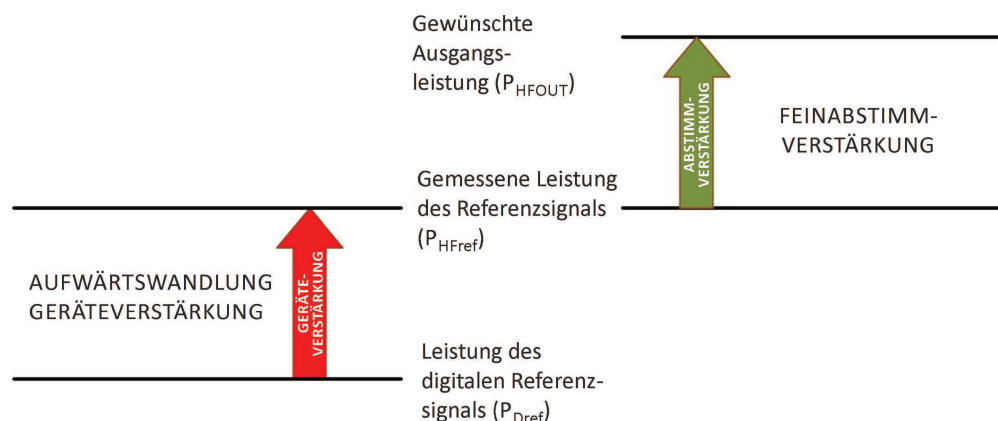


Bild 8 — Schema der Verstärkungsbeiträge für die Kalibrierung

Der Kalibrierprozess ist hinsichtlich der HF-Signalleistung für die Durchführung zuverlässiger Prüfungen notwendig, was bei Verwendung von typischen Funkgeräten nicht selbstverständlich ist.

Bild 8 zeigt ein Beispiel einer Architektur für den Aufbau des Kalibrierschemas. Die erforderlichen Elemente sind:

- zu kalibrierendes HF-Gerät;
- Kalibriersignalstapel;
- HF-Leistungsmessgerät.

Das Ergebnis des Prozesses ist das genannte Schema mit der Frequenz/Leistungs-Beziehung für den Referenzstapel.

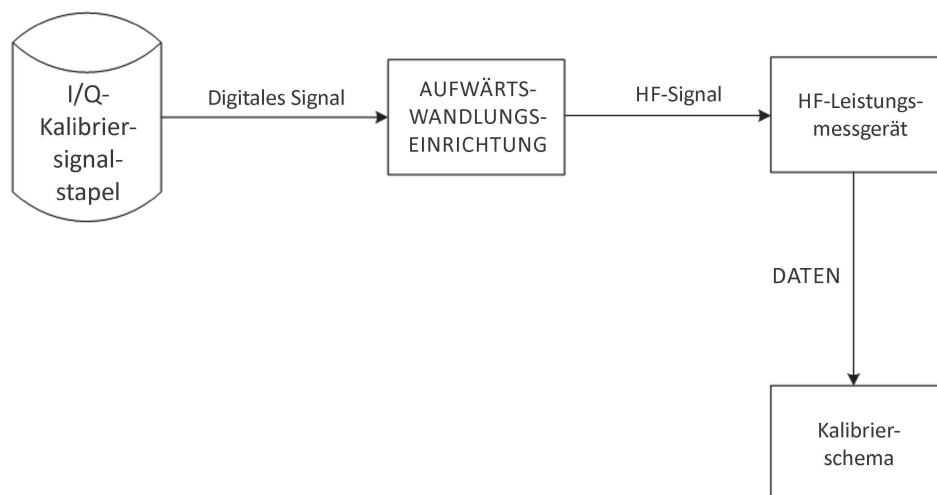


Bild 9 — Übergeordnete Architektur für den Aufbau des Kalibrierschemas zur Ermittlung der GERÄTEVERSTÄRKUNG

Der Kalibrierprozess sieht die folgenden Schritte vor, die automatisiert werden können:

- SCHÄTZUNG DER GERÄTEVERSTÄRKUNG;
 - Erzeugen eines digitalen Referenzsignals und Berechnen von dessen digitaler Leistung ($P_{D_{ref}}$);
- Erzeugen aller gewünschten Trägerfrequenzen des HF-Signals und Messen von dessen Leistung mit einem kalibrierten Leistungsmessgerät;
- Erzeugen eines Frequenz/Leistungs-Schemas für das Referenzsignal mit:
 - digitaler Leistung ($P_{D_{ref}}$);
 - Trägerfrequenz;
 - gemessener HF-Leistung ($P_{RF_{ref}}$);
 - GERÄTEVERSTÄRKUNG $G_D(f) = P_{RF_{ref}}(f) - P_{D_{ref}}(f)$;
- BERECHNUNG DER ABSTIMMVERSTÄRKUNG;
 - Holen der digitalen Signalprobe, die für das Prüfverfahren herangezogen wird, und Messen von dessen digitaler Leistung ($P_{D_{gen}}$); die Geräteverstärkung kann auch ermittelt werden nach $G_D = P_{RF_{gen}} - P_{D_{gen}}$;

- Nutzen der gewünschten HF-Signalleistung für die Simulation (P_{RFout}); die Abstimmverstärkung G_T die für die Funkperipherie angewendet werden muss, muss wie folgt berechnet werden (alle Leistungen sind im logarithmischen Maßstab angegeben) $G_T = P_{\text{RFout}} - P_{\text{RFgen}}$.

$$G_T = P_{\text{RFout}} - G_D - P_{\text{Dgen}}$$

Dabei ist P_{Dref} die digitale Leistung des Referenzsignals, P_{RFref} ist die HF-Leistung des Referenzsignals, P_{Dgen} ist die digitale Leistung des erzeugten Signals und P_{RFout} ist die angestrebte HF-Leistung.

Mit diesem Verfahren kann der Nutzer das HF-Signal mit einer spezifischen Ausgangsleistung übertragen. Es muss angemerkt werden, dass in einigen Fällen, wenn die in den vorangegangenen Schritten gemessene HF-Signalleistung den gewünschten Leistungspegel überschreitet, ein Dämpfungsglied in die Wiedergabearchitektur eingefügt werden kann, wie es auch im folgenden Abschnitt erläutert wird.

6.2.2 Architektur des Wiedergabe-Prüfstandes

Der Aufbau des Wiedergabe-Prüfstandes enthält hauptsächlich vier verschiedene Elemente:

- Steuer-PC für den Aufwärtswandler und die Überwachung des DUT;
- Funkperipheriegeräte für die HF-Übertragung (bei der Simulation einer Störsendung zwei);
- äußere OCXO-Referenz;
- Prüfling.

Bild 10 und Bild 11 zeigen den genauen Wiedergabeaufbau für die Prüfung mit Spoofing-/nominellen Signalen bzw. die Überprüfung mit Störsendung. Wie bereits erwähnt, ist ein zusätzliches HF-Übertragungsgerät erforderlich, da die Störsendung gesondert erzeugt wird.

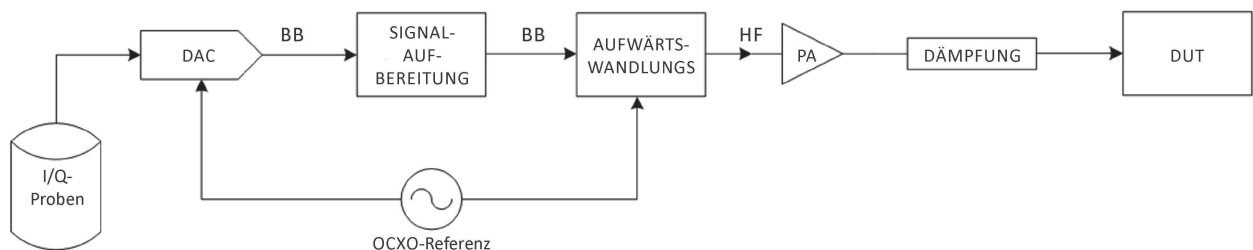


Bild 10 — Architektur des Wiedergabe-Prüfstandes mit Spoofing-/nominellen Signalen

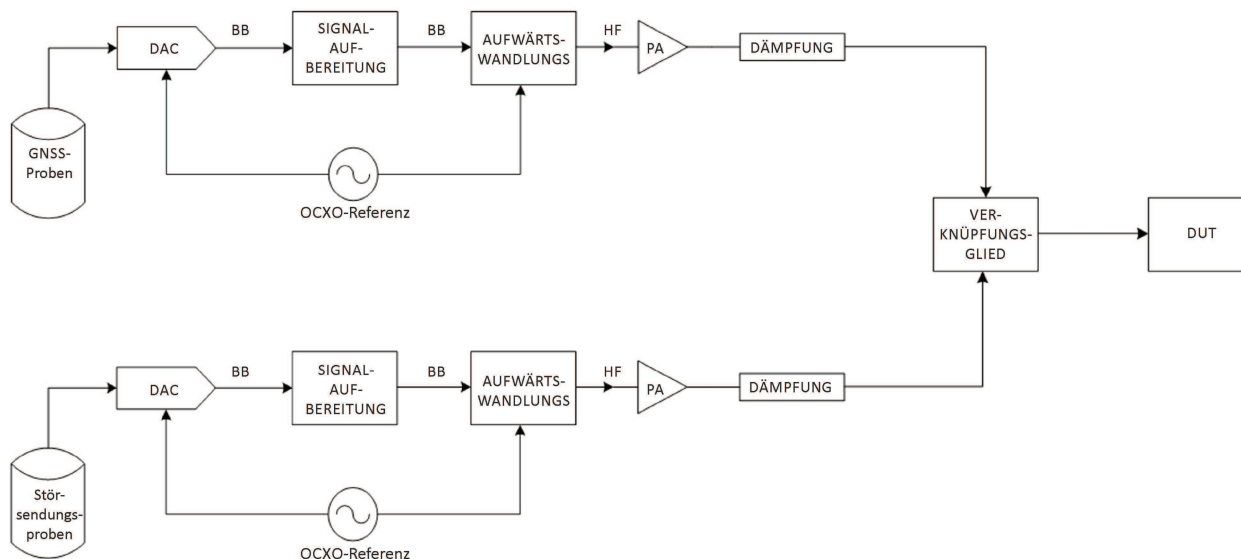


Bild 11 — Architektur des Wiedergabe-Prüfstandes mit Störsendung

Für die Prüfungen dürfen mehrere Dämpfungsglieder verwendet werden, weil die typischen HF-Geräte Übertragungsleistungspegel in der Größenordnung von 0 dBm haben können. Stattdessen liegt das GNSS-Signal unterhalb des thermischen Rauschpegels und deshalb ist die Signalleistung, die in diesen Arten von Systemen in Betracht gezogen wird, viel geringer. In diesem Fall muss mit dem im vorangegangenen Abschnitt beschriebenen Kalibrierverfahren der genaue Dämpfungswert abgeleitet werden und dann müssen in die Prüfarchitektur geeignete Dämpfungsglieder eingeführt werden, wie z. B. in Bild 10 und Bild 11 dargestellt.

6.3 Validierung der zur Datenverarbeitung verwendeten Hard- und Software durch das HF-Prüflaboratorium

Wie für die grundlegende Leistungsüberprüfung muss das Lab-B vor dem Wiedergabeszenario seinen eigenen Prozess validieren. Dies muss vor der Prüfung des GBPT erfolgen, um Vertrauen in das Endergebnis setzen zu können. Die vorliegende Norm empfiehlt zwei Arten des Nachweises:

- Softwarevalidierung: Das Lab-B muss mit seinen eigenen Softwarewerkzeugen aus den Ausgaben des Bezugsgrößenempfängers alle Metriken berechnen, die von Lab-A im Prüfszenario empfohlen werden, und mit den von Lab-A angegebenen Metriken („Bezugsgrößen-Metriken“) vergleichen. Die Software-Werkzeugkette wird für „betriebsbereit“ erklärt, wenn die Metriken abgeglichen sind. Ist dies nicht der Fall, so darf das Prüflaboratorium den Prozess nicht fortsetzen.
- Systemvalidierung: Lab-B muss die von Lab-A aufgezeichnete GNSS-I/Q-Probe desselben Bezugsgrößenempfängers wiedergeben. Es muss auch die Metriken mit seinem eigenen Softwarewerkzeug berechnen und mit den „Bezugsgrößenmetriken“ vergleichen. Dabei wird die gesamte Werkzeugkette verifiziert. Die gesamte Werkzeugkette (Hardware + Software) wird für „betriebsbereit“ erklärt, wenn die Metriken abgeglichen sind. Ist dies nicht der Fall, so darf das Prüflaboratorium den Prozess nicht fortsetzen.

Dieser Aspekt wird in prEN 16803-2:2018, Abschnitt 7, eingehend behandelt.

6.4 Wiedergabe der Daten

6.4.1 Allgemeines

Da der Gestaltungsprozess des Störsendungsszenarios und des Spoofing-Szenarios verschieden ist (siehe Abschnitt 4), ist auch das Überprüfungsverfahren anders. Es sind zwei verschiedene Fälle zu betrachten, die nachfolgend beschrieben werden.

6.4.2 Störsendungsszenario

Abhängig von den Umgebungen und von den Arten des Störsendungsangriffs, an deren Prüfung der Kunde interessiert ist, kann es verschiedene Störsendungsszenarien geben. Diese verschiedenen Störsendungsszenarien kombinieren die Wiedergabe der I/Q-GNSS-Proben, die einem vorgegebenen Prüfscenario entsprechen (wie in EN 16803-2 festgelegt), mit der Wiedergabe der I/Q-Störsendungsproben, die einem vorgegebenen Störsendungsangriff entsprechen, nach Bild 3.

Beispiele für die zutreffenden Störsendungsszenarien sind im informativen Anhang C angegeben.

Die Wiedergabe der GNSS-Proben ohne Störsendung erzeugt einen nominellen Datensatz (NDS), der bei grundlegenden Prüfungen in den Prüfling eingegeben wird, und die Überlagerung von GNSS-Proben mit Störsendungsproben erzeugt einen angegriffenen Datensatz (ADS), der bei Sicherheitsprüfungen in den Prüfling eingegeben wird, wie in Bild 12 dargestellt.

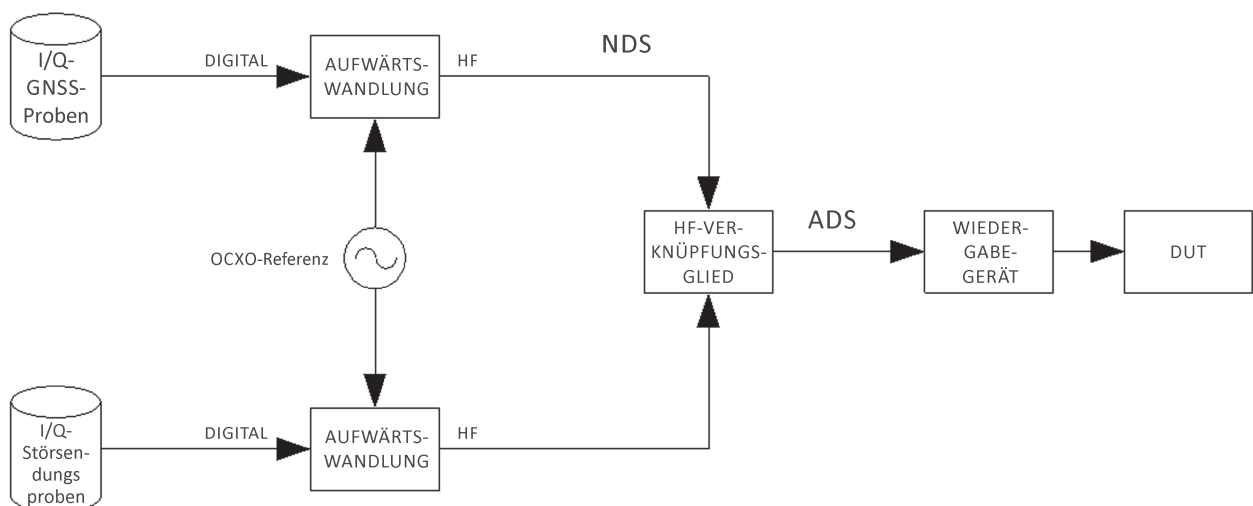


Bild 12 — Position von NDS und ADS in der Architektur der Prüfung mit Störsendung

Es wird davon ausgegangen, dass die Metriken für den NDS bereits nach EN 16803-2 berechnet worden sind, sodass nur der ADS wiedergegeben werden muss, um die Leistungsminderung zwischen NDS und ADS berechnen zu können.

6.4.3 Spoofing- und Meaconing-Szenarien

Spoofing-Szenarien werden von Lab-A in Form von I/Q-Proben bereitgestellt, die nominelle GNSS-Proben und simulierte GNSS-Proben mit Spoofing, die mit einem RFCS nach Bild 5 und Bild 6 erhalten werden, kombinieren.

Insofern ist der NDS, der den GNSS-Daten ohne Spoofing entspricht, noch nicht wiedergegeben worden. Um die Metriken und die Leistungsminderung berechnen zu können, müssen sowohl NDS als auch ADS von Lab-B wiedergegeben werden.

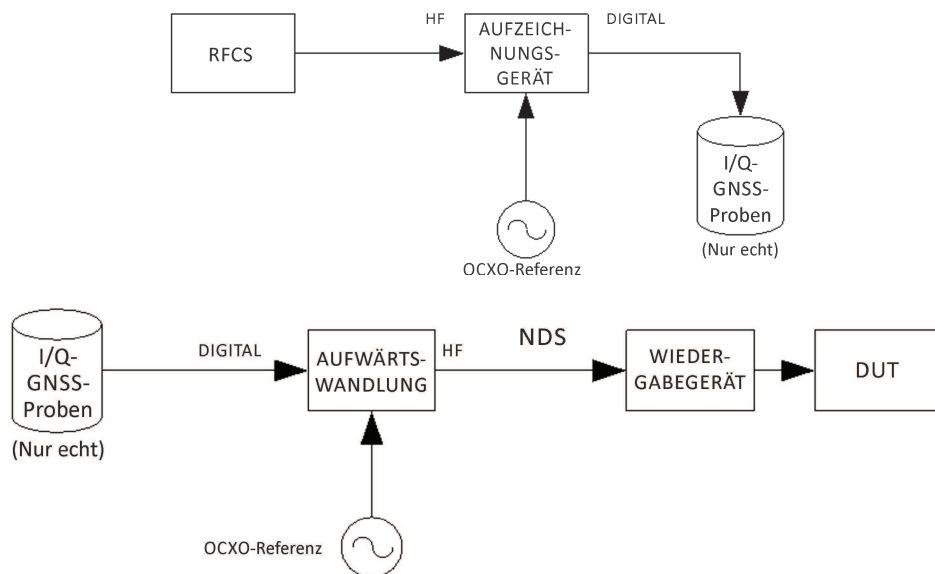


Bild 13 — Position des NDS in der Architektur mit Spoofing

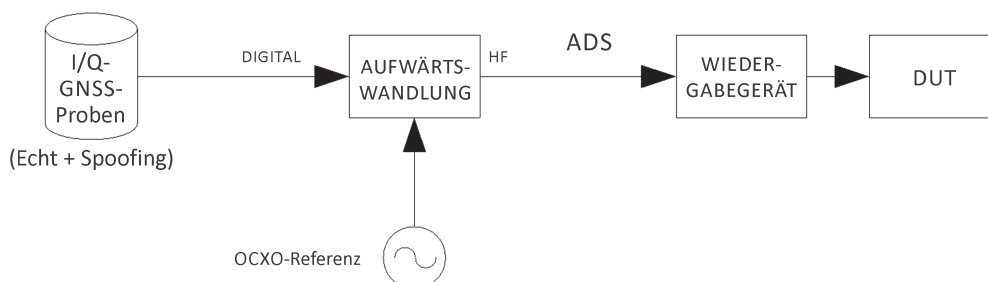


Bild 14 — Position des ADS in der Architektur mit Spoofing

ANMERKUNG Der Aufbau mit RFCS zur Erzeugung von authentischen GNSS-Signalen muss für ADS und NDS der gleiche sein.

Beispiele für die zutreffenden Spoofing- und Meaconing-Szenarien sind in Anhang C angegeben.

Wichtige Anmerkung: Aufgrund der Komplexität der Spoofing-Szenarien und der Verwendung des RFCS dürfen nur Bedingungen eines **klaren Himmels** herangezogen werden.

6.5 Berechnung der Minderung von Metriken

6.5.1 Allgemeines

Sobald die Wiedergabe erfolgt ist, müssen die Metriken, die sich aus dem ADS-Szenario mit Störsendung ergeben, berechnet werden, wie in EN 16803-2 beschrieben. Genauso müssen die Metriken, die sich aus dem NDS- und ADS-Szenario mit Spoofing ergeben, berechnet werden. Diese beiden Fälle, nämlich Störsendung und Spoofing, sind zu unterscheiden.

6.5.2 Störsendungsszenarien

Wie im Anwendungsbereich von EN 16802 festgelegt, sind die Prüfverfahren in der Normenreihe EN 16803 nur auf Verfügbarkeit, Stetigkeit, Genauigkeit, Integrität (ACAI) und Time To First Fix (TTFF) ausgerichtet. Da EN 16803-3 an die Berechnung der Minderung der Metriken nach EN 16803-2 gebunden ist, ist die Menge der Metriken die gleiche, und zwar ACAI und TTFF.

Die Minderung der ACAI- und TTFF-Metriken muss dann nach Abschnitt 5 berechnet werden unter Berücksichtigung von:

- NDS-Metriken aus der grundlegenden Leistungsüberprüfung und ADS-Metriken aus der aktuellen Überprüfung der Sicherheitsleistung für Störsendungsprüfungen;
- NDS- und ADS-Metriken aus aktuellen Überprüfungen der Sicherheitsleistung für Spoofing- und Meaconing-Prüfungen.

6.5.3 Spoofing- und Meaconing-Szenarien

Für den Spoofing-Teil muss die Minderung der ACAI-Metriken nach Abschnitt 5 berechnet werden, weil es sinnvoll ist, diese Metriken bei Spoofing-Angriffen zu überprüfen. Bei der Betrachtung der TTFF ist das nicht mehr notwendig. Die Überprüfung der Minderung der TTFF ist bei Spoofing-Angriffen unerheblich; die Normenreihe EN 16803 empfiehlt für das Spoofing-Szenario keine Überprüfung der Minderung der TTFF.

6.6 Erstellung des Abschlussberichts zur Prüfung

Sobald alle Prüfungen durchgeführt und alle Metriken berechnet worden sind, muss das Lab-B das Ergebnis in einem Prüfbericht angeben. In Abschnitt 8 ist eine Vorlage für diesen Prüfbericht beschrieben.

7 Validierungsverfahren

Wie für die Bewertungsprüfungen für die grundlegenden Leistungsmerkmale nach EN 16803-2 muss ein Validierungsverfahren angewendet werden, um nachzuweisen, dass die R&R-Prüfungen von Lab-B einwandfrei durchgeführt worden sind und die Prüfergebnisse vertrauenswürdig sind.

Einzelheiten siehe EN 16803-2.

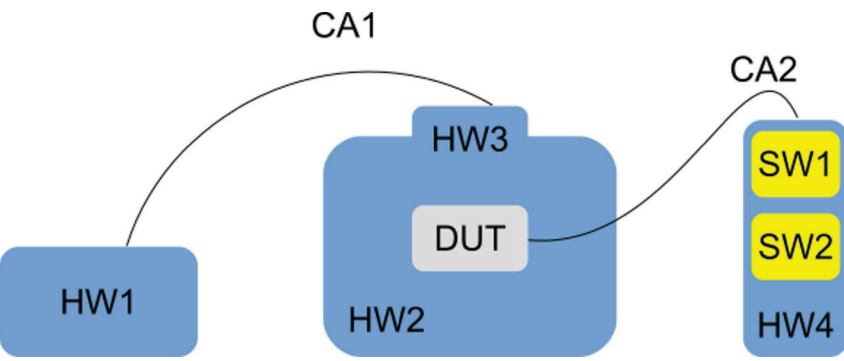
8 Definition des Syntheseberichts: Wie die Ergebnisse der Prüfungen im Bericht anzugeben sind

Um der vorliegenden Norm zu entsprechen, muss ein schriftlicher Bericht verfasst werden. Dieser muss mindestens die folgenden Teile umfassen:

- Laboratorium – Verwaltungsteil;
- Bezeichnung des DUT und Beschreibung;
- Beschreibung des Prüfstandes;
- Bezeichnung der Prüfreize;
- Bezeichnung der Ausgabedateien;
- überprüfte Metriken und verwendete DUT-Ausgabe;
- Zusammenfassung der Ergebnisse;
- Prüfbericht – Verwaltungsteil.

Alle diese Teile müssen festgelegt werden und die dazugehörigen Informationen nach der folgenden Vorlage enthalten (graue Teile sind nur Beispiele, die der Veranschaulichung dienen):

Laboratorium – Verwaltungsteil	
Name des Laboratoriums	AZERTY
Identifizierung des Laboratoriums	Anschrift/Codenummer/Logo
Laboratorium – Kontakt	E-Mail/Telefonnummer
Zertifizierungssymbole	ISO/IEC 17025, ISO 9001, ...
DUT-Beschreibung und Beschreibung	
Marke	NewGNSS Company
Modell	GBPT der neuen Generation
Seriennummer	XC54GFV3258
Firmware-Version	2.41
Konfigurationsversion	101.55: Galileo aktiviert/SBAS deaktiviert/IMU-Fusion deaktiviert/...
Stromversorgung	12 VDC erforderlich. Keine Batterie. Steckverbinder SUPERSEAL
GNSS-Antenne	Intern/extern falls extern: Anschlusstyp (SMA-Stecker/RP-SMA-Buchse/TNC männlich/...)
Der DUT ist bereit zur Überprüfung, wenn:	Die grüne LED auf der linken Seite mit 2 Hz blinkt.
Beschreibung des Prüfstandes	
Bezeichnung des Werkstoffs (HW 1):	StellaNGC GNSS Record & Playback
Typ:	Signalaufzeichnungs- und -wiedergabegerät
Marke:	M3-Systeme
Modell:	StellaNCG Platinum
Seriennummer:	54.1.25.41
Firmware-Version:	1.11
Konfigurationsversion:	Mehrkanal/Mehrfachkonstellation
Bezeichnung des Werkstoffs (HW 2):	Schallgedämmter Raum
Typ:	xxxx2
Marke:	yyyy2
Modell:	zzzz2
Seriennummer:	3214.235
Firmware-Version:	N/A
Konfigurationsversion:	N/A
Bezeichnung des Werkstoffs (HW 3):	Sendeantenne
Typ:	xxxx3

Marke:	yyyy3
Modell:	zzzz3
Seriennummer:	456
Firmware-Version:	N/A
Konfigurationsversion:	N/A
Bezeichnung des Werkstoffs (HW 4):	Arbeitsplatzrechner
Typ:	xxxx4
Marke:	yyyy4
Modell:	zzzz4
Seriennummer:	456.12378
Firmware-Version:	Betriebssystem: Windows10 Pro
Konfigurationsversion:	N/A
Name der Software (SW 1):	MetricsAnalyser
Typ:	Nachbearbeitung für die Berechnung der Metriken
Marke:	GUIDE
Version:	4.1
Konfiguration:	alle Metriken nach EN 16803-2
Name der Software (SW 2):	GBPT-Steuer- und Protokollierwerkzeug
Typ:	Nachbearbeitung für die Berechnung der Metriken
Marke:	NewGNSS Company
Version:	3.2
Kabel (CA 1)	Kabel, das zur Verbindung des GNSS-Wiedergabegeräts HW1 mit der Antenne HW3 verwendet wird
Kabel (CA 2)	Kabel, das zur Protokollierung der vom DUT ausgegebenen Daten auf dem Computer HW4 verwendet wird
Blockschaltbild des Prüfstandes:  <pre> graph LR HW1[HW1] -- CA1 --> HW3[HW3] subgraph HW2 [HW2] DUT[DUT] end DUT -- CA2 --> HW4[HW4] subgraph HW4_Box [HW4] SW1[SW1] SW2[SW2] end </pre>	
Wahl der Umgebung(en)	
Störsendung: Flache ländliche Umgebung (env1) / Europäisches Stadtrandgebiet (env4) Spoofing : klarer Himmel (Simulation)	

Bezeichnung der Prüfreize;	
Bezeichnung von Szenario A:	Sc456.1
Anbieter:	XLab
Ort der aufgezeichneten Daten:	Toulouse
Dauer:	3 h
Bezeichnung von Szenario B:	GL.65.12
Anbieter:	YLab
Ort der aufgezeichneten Daten:	Paris
Dauer:	1,5 h
Bezeichnung der Ausgabedateien	
UEDS env1	UEDS-env1A_DUT-24nov2017-run1.txt UEDS-env1A_DUT-24nov2017-run2.txt UEDS-env1A_DUT-24nov2017-run3.txt UEDS-env1A_DUT-24nov2017-run4.txt UEDS-env1A_DUT-24nov2017-run5.txt UEDS-env1A_DUT-24nov2017-run6.txt UEDS-env1B_DUT-24nov2017-run1.txt UEDS-env1B_DUT-24nov2017-run2.txt UEDS-env1B_DUT-24nov2017-run3.txt UEDS-env1B_DUT-24nov2017-run4.txt UEDS-env1B_DUT-24nov2017-run5.txt UEDS-env1B_DUT-24nov2017-run6.txt UEDS-env1I_DUT-24nov2017-run1.txt UEDS-env1I_DUT-24nov2017-run2.txt UEDS-env1I_DUT-24nov2017-run3.txt UEDS-env1I_DUT-24nov2017-run4.txt UEDS-env1I_DUT-24nov2017-run5.txt UEDS-env1I_DUT-24nov2017-run6.txt
UEDS env4	UEDS-env4A_DUT-24nov2017-run1.txt UEDS-env4A_DUT-24nov2017-run2.txt UEDS-env4A_DUT-24nov2017-run3.txt UEDS-env4A_DUT-24nov2017-run4.txt UEDS-env4A_DUT-24nov2017-run5.txt UEDS-env4A_DUT-24nov2017-run6.txt UEDS-env4A_DUT-25nov2017-run7.txt UEDS-env4A_DUT-25nov2017-run8.txt UEDS-env4A_DUT-25nov2017-run9.txt UEDS-env4A_DUT-25nov2017-run10.txt UEDS-env4A_DUT-25nov2017-run11.txt UEDS-env4A_DUT-25nov2017-run12.txt

	UEDS-env4D_DUT-25nov2017-run1.txt UEDS-env4D_DUT-25nov2017-run2.txt UEDS-env4D_DUT-25nov2017-run3.txt UEDS-env4D_DUT-25nov2017-run4.txt UEDS-env4D_DUT-25nov2017-run5.txt UEDS-env4D_DUT-25nov2017-run6.txt UEDS-env4D_DUT-25nov2017-run7.txt UEDS-env4D_DUT-25nov2017-run8.txt UEDS-env4D_DUT-25nov2017-run9.txt UEDS-env4D_DUT-25nov2017-run10.txt UEDS-env4D_DUT-25nov2017-run11.txt UEDS-env4D_DUT-25nov2017-run12.txt UEDS-env4E_DUT-25nov2017-run1.txt UEDS-env4E_DUT-25nov2017-run2.txt UEDS-env4E_DUT-25nov2017-run3.txt UEDS-env4E_DUT-25nov2017-run4.txt UEDS-env4E_DUT-25nov2017-run5.txt UEDS-env4E_DUT-25nov2017-run6.txt UEDS-env4E_DUT-25nov2017-run7.txt UEDS-env4E_DUT-25nov2017-run8.txt UEDS-env4E_DUT-25nov2017-run9.txt UEDS-env4E_DUT-25nov2017-run10.txt UEDS-env4E_DUT-25nov2017-run11.txt UEDS-env4E_DUT-25nov2017-run12.txt
	UEDS-env4G_DUT-25nov2017-run1.txt UEDS-env4G_DUT-25nov2017-run2.txt UEDS-env4G_DUT-25nov2017-run3.txt UEDS-env4G_DUT-25nov2017-run4.txt UEDS-env4G_DUT-25nov2017-run5.txt UEDS-env4G_DUT-25nov2017-run6.txt UEDS-env4G_DUT-25nov2017-run7.txt UEDS-env4G_DUT-25nov2017-run8.txt UEDS-env4G_DUT-25nov2017-run9.txt UEDS-env4G_DUT-25nov2017-run10.txt UEDS-env4G_DUT-25nov2017-run11.txt UEDS-env4G_DUT-25nov2017-run12.txt
Dateiformat:	Dateiformat: ASCII-Text Zeilenabschluss: <cr><lf> Protokoll: NMEA 0183 Version: 4.1 Sprecher-ID: GN Aktivierte Nachrichten-IDs: GGA, GSA, GSV, GRS, GBS, RMC, VTG, GNS usw.

Überprüfte Metriken		Verwendete DUT-Ausgabe				
Überprüfte Minderung der Genauigkeitsmetriken (nach EN 16803-3)	AccDeg _{Position – Horizontal}	\$GNGGA				
	AccDeg _{Position – Fahrtrichtung}	\$GNGGA				
	AccDeg _{Position – Querrichtung}	\$GNGGA				
	AccDeg _{Schnelligkeit – Horizontal}	\$GNVTG				
Überprüfte Minderung der Integritätsmetriken (nach EN 16803-3)	PL_Deg _{Position – Horizontal}	\$GNTBD ^a				
	PL_Deg _{Position – Fahrtrichtung}	\$GNTBD ^a				
	PL_Deg _{Position – Querrichtung}	\$GNTBD ^a				
	PL_Deg _{Geschwindigkeit – Horizontal}	\$GNTBD ^a				
Überprüfte Minderung der Verfügbarkeits- und Stetigkeitsmetriken (nach EN 16803)	AvailDeg _{Position – T-Fester von 1 s}	\$GNGGA				
	AvailDeg _{Position – T-Fenster von 60 s}	\$GNGGA				
Überprüfte Minderung der Zeitsteuerungssmetriken (nach EN 16803-3)	TTFF_Deg(T)	\$GNGGA				
Zusammenfassung der Ergebnisse für die Störsendung						
	Flache ländliche Umgebung	Straße mit Baum- bestand	Gebirge	Stadttrand gebiet	Euro- päisches Stadt- gebiet	Moderne Städte
AccDeg _{Position – Horizontal}	(20 %, 30 %, 40 %)	—	—	(50 %, 60 %, 70 %)	—	—
AccDeg _{Position – Fahrtrichtung}	(20 %, 30 %, 40 %)	—	—	(50 %, 60 %, 70 %)	—	—
AccDeg _{Position – Querrichtung}	(20 %, 30 %, 40 %)	—	—	(50 %, 60 %, 70 %)	—	—
AccDeg _{Schnelligkeit – Horizontal}	(30 %, 40 %, 50 %)	—	—	(60 %, 65 %, 70 %)	—	—
PL_Deg _{Position – Horizontal}	(45 %, 55 %, 65 %)	—	—	(60 %, 65 %, 70 %)	—	—
PL_Deg _{Position – Fahrtrichtung}	(45 %, 55 %, 65 %)	—	—	(60 %, 65 %, 70 %)	—	—
PL_Deg _{Position – Querrichtung}	(45 %, 55 %, 65 %)	—	—	(60 %, 65 %, 70 %)	—	—