DIN EN 16803-3:2021-07 (E)

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

Contents

Page

European foreword 4

Introduction 5

1 Scope 7

2 Normative references 7

3 Terms, definitions and acronyms 8
3.1 Terms and definitions 8
3.2 Acronyms 10

4 Description of the general logic of security tests 11
4.1 Record and Replay principle 11
4.2 Specificity of security tests based upon the R & R approach 12
4.3 Jamming testing Architecture 12
4.4 Spoofing/meaconing testing architecture 14

5 Definition of the metrics with respect to security performances 16
5.1 General 16
5.2 Accuracy metrics 16
5.3 Availability and continuity metrics 17
5.4 Integrity metrics 18
5.4.1 Protection Level performance metrics 18
5.4.2 Misleading Information metrics 19
5.5 Timing metrics 19
5.5.1 Timestamp resolution 19
5.5.2 Nominal output latency 19
5.5.3 Nominal output rate 19
5.5.4 Output latency stability 19
5.5.5 Output rate stability 20
5.5.6 Time to first fix 20

6 Description of the test procedures and the test equipment 21
6.1 Scope 21
6.2 Setting-up of the replay test-bench 21
6.2.1 Replay device calibration 21
6.2.2 Replay testbed architecture 24
6.3 Validation of the data processing HW and SW by the RF test laboratory 25
6.4 Replaying of the data 26
6.4.1 General 26
6.4.2 Jamming scenarios 26
6.4.3 Spoofing and meaconing scenarios 26
6.5 Computation of metrics degradation 27
6.5.1 General 27
6.5.2 Jamming scenarios 27
6.5.3 Spoofing and meaconing scenarios 28
6.6 Establishment of the final test report 28

7 Validation procedure 28

8 Definition of the synthesis report: how to report the results of the tests 28

Annex A (informative) Analysis of the GNSS attacks taxonomy 36

A.1 General 36
A.2 Categorization of GNSS attacks 36
A.3 GNSS attack models 37
A.3.1 General 37
A.3.2 Interference and jamming attacks 37
A.3.3 Meaconing attacks 38
A.3.4 Spoofing attacks 38

Annex B (informative) Security-specific metrics (authentication capabilities, spoofing and jamming detection flags, etc.) 40

Annex C (informative) Scenarios proposition 42

C.1 General 42
C.2 Jamming/interference proposed scenarios 42
C.3 Spoofing proposed scenario 43
C.4 Meaconing proposed scenarios 46

Annex D (informative) Spoofing insights 48

D.1 General 48
D.2 Range error impact 49
D.3 Oscillator error impact 49
D.4 Propagation channel 50

Annex E (informative) Data set record testbed 52

E.1 General 52
E.2 Jamming data generation 52
E.3 Spoofing data recording 56

Bibliography 57